

HTTP Working Group
Internet-Draft
Intended status: Experimental
Expires: April 7, 2017

I. Grigorik
Google
October 4, 2016

HTTP Client Hints
draft-ietf-httpbis-client-hints-02

Abstract

An increasing diversity of Web-connected devices and software capabilities has created a need to deliver optimized content for each device.

This specification defines a set of HTTP request header fields, colloquially known as Client Hints, to address this. They are intended to be used as input to proactive content negotiation; just as the Accept header field allows clients to indicate what formats they prefer, Client Hints allow clients to indicate a list of device and agent specific preferences.

Note to Readers

Discussion of this draft takes place on the HTTP working group mailing list (ietf-http-wg@w3.org), which is archived at <https://lists.w3.org/Archives/Public/ietf-http-wg/> .

Working Group information can be found at <http://httpwg.github.io/> ; source code and issues list for this draft can be found at <https://github.com/httpwg/http-extensions/labels/client-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 <http://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 April 7, 2017.

Internet-Draft

HTTP Client Hints

October 2016

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
1.1.	Notational Conventions	3
2.	Client Hint Request Header Fields	4
2.1.	Sending Client Hints	4
2.2.	Server Processing of Client Hints	4
2.2.1.	Advertising Support for Client Hints	4
2.2.2.	Interaction with Caches	5
3.	The DPR Client Hint	6
3.1.	Confirming Selected DPR	6
4.	The Width Client Hint	7
5.	The Viewport-Width Client Hint	7
6.	The Downlink Client Hint	7
7.	The Save-Data Client Hint	8
8.	Examples	8
9.	Security Considerations	9
10.	IANA Considerations	9
10.1.	Accept-CH	10
10.2.	Content-DPR	10
10.3.	Downlink	10
10.4.	DPR	10
10.5.	Save-Data	10
10.6.	Viewport-Width	11
10.7.	Width	11
11.	References	11
11.1.	Normative References	11
11.2.	Informative References	12

Appendix A. Changes	12
A.1. Since -00	12
A.2. Since -01	12
A.3. Since -02	13
Author's Address	13

[1.](#) Introduction

There are thousands of different devices accessing the web, each with different device capabilities and preference information. These device capabilities include hardware and software characteristics, as well as dynamic user and client preferences.

One way to infer some of these capabilities is through User-Agent (UA; [Section 5.5.3 of \[RFC7231\]](#)) detection against an established database of client signatures. However, this technique requires acquiring such a database, integrating it into the serving path, and keeping it up to date. However, even once this infrastructure is deployed, UA sniffing has numerous limitations:

- o UA detection cannot reliably identify all static variables
- o UA detection cannot infer any dynamic client preferences
- o UA detection requires an external device database
- o UA detection is not cache friendly

A popular alternative strategy is to use HTTP cookies ([\[RFC6265\]](#)) to communicate some information about the client. However, this approach is also not cache friendly, bound by same origin policy, and imposes additional client-side latency by requiring JavaScript execution to create and manage HTTP cookies.

This document defines a set of new request header fields that allow the client to perform proactive content negotiation ([Section 3.4.1 of \[RFC7231\]](#)) by indicating a list of device and agent specific preferences, through a mechanism similar to the Accept header field which is used to indicate preferred response formats.

Client Hints does not supersede or replace the User-Agent header field. Existing device detection mechanisms can continue to use both mechanisms if necessary. By advertising its capabilities within a request header field, Client Hints allows for cache friendly and proactive content negotiation.

[1.1.](#) Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

This document uses the Augmented Backus-Naur Form (ABNF) notation of [[RFC5234](#)] with the list rule extension defined in [[RFC7230](#)], [Appendix B](#). It includes by reference the DIGIT rule from [[RFC5234](#)] and the OWS and field-name rules from [[RFC7230](#)].

[2.](#) Client Hint Request Header Fields

A Client Hint request header field is a HTTP header field that is used by HTTP clients to indicate configuration data that can be used by the server to select an appropriate response. Each one conveys a list of client preferences that the server can use to adapt and optimize the response.

[2.1.](#) Sending Client Hints

Clients control which Client Hint headers and their respective header fields are communicated, based on their default settings, user configuration and/or preferences. The user can be given the choice to enable, disable, or override specific hints.

The client and server, or an intermediate proxy, can use an opt-in mechanism to negotiate which fields should be reported to allow for efficient content adaptation.

[2.2.](#) Server Processing of Client Hints

Servers respond with an optimized response based on one or more received hints from the client. When doing so, and if the resource is cacheable, the server MUST also emit a Vary response header field ([Section 7.1.4 of \[RFC7231\]](#)), and optionally Key ([\[I-D.ietf-httpbis-key\]](#)), to indicate which hints can affect the selected response and whether the selected response is appropriate for a later request.

Further, depending on the used hint, the server can emit additional response header fields to confirm the property of the response, such that the client can adjust its processing. For example, this specification defines "Content-DPR" response header field that needs to be returned by the server when the "DPR" hint is used to select the response.

2.2.1. Advertising Support for Client Hints

Servers can advertise support for Client Hints using the Accept-CH header field or an equivalent HTML meta element with http-equiv attribute ([\[W3C.REC-html5-20141028\]](#)).

Accept-CH = #field-name

For example:

Grigorik

Expires April 7, 2017

[Page 4]

Internet-Draft

HTTP Client Hints

October 2016

Accept-CH: DPR, Width, Viewport-Width, Dwnlink

When a client receives Accept-CH, or if it is capable of processing the HTML response and finds an equivalent HTML meta element, it SHOULD append the Client-Hint header fields that match the advertised field-values to the header list of all subsequent requests. For example, based on Accept-CH example above, a user agent could append DPR, Width, Viewport-Width, and Dwnlink header fields to all subresource requests initiated by the page constructed from the response. Alternatively, a client can treat advertised support as a persistent origin preference and append same header fields on all future requests initiated to and by the resources associated with that origin.

2.2.2. Interaction with Caches

When selecting an optimized response based on one or more Client Hints, and if the resource is cacheable, the server needs to emit a Vary response header field ([\[RFC7234\]](#)) to indicate which hints can affect the selected response and whether the selected response is appropriate for a later request.

Vary: DPR

Above example indicates that the cache key needs to include the DPR header field.

Vary: DPR, Width, Downlink

Above example indicates that the cache key needs to include the DPR, Width, and Downlink header fields.

Client Hints MAY be combined with Key ([\[I-D.ietf-httpbis-key\]](#)) to enable fine-grained control of the cache key for improved cache efficiency. For example, the server can return the following set of instructions:

Key: DPR;partition=1.5:2.5:4.0

Above example indicates that the cache key needs to include the value of the DPR header field with three segments: less than 1.5, 1.5 to less than 2.5, and 4.0 or greater.

Key: Width;div=320

Above example indicates that the cache key needs to include the value of the Width header field and be partitioned into groups of 320: 0-320, 320-640, and so on.

Key: Downlink;partition=0.5:1.0:3.0:5.0:10

Above example indicates that the cache key needs to include the (Mbps) value of the Downlink header field with six segments: less than 0.5, 0.5 to less than 1.0, 1.0 to less than 3.0, 3.0 to less than 5.0, 5.0 to less than 10; 10 or higher.

[3.](#) The DPR Client Hint

The "DPR" request header field is a number that indicates the

client's current Device Pixel Ratio (DPR), which is the ratio of physical pixels over CSS px (Section 5.2 of [[W3C.CR-css-values-3-20150611](#)]) of the layout viewport ([Section 9.1.1](#) of [[CSS2](#)]) on the device.

DPR = 1*DIGIT ["." 1*DIGIT]

If DPR occurs in a message more than once, the last value overrides all previous occurrences.

[3.1.](#) Confirming Selected DPR

The "Content-DPR" response header field is a number that indicates the ratio between physical pixels over CSS px of the selected image response.

Content-DPR = 1*DIGIT ["." 1*DIGIT]

DPR ratio affects the calculation of intrinsic size of image resources on the client - i.e. typically, the client automatically scales the natural size of the image by the DPR ratio to derive its display dimensions. As a result, the server MUST explicitly indicate the DPR of the selected image response whenever the DPR hint is used, and the client MUST use the DPR value returned by the server to perform its calculations. In case the server returned Content-DPR value contradicts previous client-side DPR indication, the server returned value MUST take precedence.

Note that DPR confirmation is only required for image responses, and the server does not need to confirm the resource width as this value

can be derived from the resource itself once it is decoded by the client.

If Content-DPR occurs in a message more than once, the last value overrides all previous occurrences.

[4.](#) The Width Client Hint

The "Width" request header field is a number that indicates the desired resource width in physical px (i.e. intrinsic size of an image). The provided physical px value is a number rounded to the smallest following integer (i.e. ceiling value).

Width = 1*DIGIT

If the desired resource width is not known at the time of the request or the resource does not have a display width, the Width header field can be omitted. If Width occurs in a message more than once, the last value overrides all previous occurrences.

5. The Viewport-Width Client Hint

The "Viewport-Width" request header field is a number that indicates the layout viewport width in CSS px. The provided CSS px value is a number rounded to the smallest following integer (i.e. ceiling value).

Viewport-Width = 1*DIGIT

If Viewport-Width occurs in a message more than once, the last value overrides all previous occurrences.

6. The Downlink Client Hint

The "Downlink" request header field is a number that indicates the client's maximum downlink speed in megabits per second (Mbps), as defined by the "downlinkMax" attribute in the W3C Network Information API ([\[NETINFO\]](#)).

Downlink = 1*DIGIT ["." 1*DIGIT]

If Downlink occurs in a message more than once, the minimum value should be used to override other occurrences.

7. The Save-Data Client Hint

The "Save-Data" request header field consists of one or more tokens that indicate client's preference for reduced data usage, due to high transfer costs, slow connection speeds, or other reasons.

```
Save-Data = sd-token *( OWS ";" OWS [sd-token] )  
sd-token = token
```

This document defines the "on" sd-token value, which is used as a signal indicating explicit user opt-in into a reduced data usage mode on the client, and when communicated to origins allows them to deliver alternate content honoring such preference - e.g. smaller image and video resources, alternate markup, and so on. New token and extension token values can only be defined by revisions of this specification.

[8.](#) Examples

For example, given the following request header fields:

```
DPR: 2.0  
Width: 320  
Viewport-Width: 320
```

The server knows that the device pixel ratio is 2.0, that the intended display width of the requested resource is 160 CSS px (320 physical pixels at 2x resolution), and that the viewport width is 320 CSS px.

If the server uses above hints to perform resource selection for an image asset, it must confirm its selection via the Content-DPR response header to allow the client to calculate the appropriate intrinsic size of the image response. The server does not need to confirm resource width, only the ratio between physical pixels and CSS px of the selected image resource:

```
Content-DPR: 1.0
```

The Content-DPR response header field indicates to the client that the server has selected resource with DPR ratio of 1.0. The client can use this information to perform additional processing on the resource - for example, calculate the appropriate intrinsic size of the image resource such that it is displayed at the correct resolution.

Alternatively, the server could select an alternate resource based on the maximum downlink speed advertised in the request header fields:

Downlink: 0.384

The server knows that the client's maximum downlink speed is 0.384Mbps (GPRS EDGE), and it can use this information to select an optimized resource - for example, an alternate image asset, stylesheet, HTML document, media stream, and so on.

9. Security Considerations

Client Hints defined in this specification do not expose new information about the user's environment beyond what is already available to, and can be communicated by, the application at runtime via JavaScript and CSS. For example, the application can obtain viewport width, image display width, and device pixel ratio via JavaScript, or through the use of CSS media queries and unique resource URLs even if JavaScript is disabled. However, implementors should consider the privacy implications of various methods to enable delivery of Client Hints - see "Sending Client Hints" section.

For example, sending Client Hints on all requests can make information about the user's environment available to origins that otherwise did not have access to this data, which may or may not be the desired outcome - e.g. this may enable an image optimization service to deliver a tailored asset, and it may reveal some information about the user to other origins that may not have had access to it before. Similarly, sending highly granular data, such as image and viewport width may help identify users across multiple requests. Restricting such field values to an enumerated range, where the user agent advertises a threshold value that is close but is not an exact representation of the current value, might reduce such fingerprinting risks.

The implementers can provide mechanisms and policies to control how and when such hints are advertised: require origin opt-in and restrict delivery to same origin subrequests; limit delivery to requests that already carry indentifying information (e.g. cookies); modify delivery policy when in an "incognito" or a similar privacy mode; enable user configuration and opt in, and so on.

10. IANA Considerations

This document defines the "Accept-CH", "DPR", "Width", and "Downlink"

HTTP request fields, "Content-DPR" HTTP response field, and registers them in the Permanent Message Header Fields registry.

[10.1.](#) Accept-CH

- o Header field name: Accept-CH
- o Applicable protocol: HTTP
- o Status: standard
- o Author/Change controller: IETF
- o Specification document(s): [Section 2.2.1](#)
- o Related information: for Client Hints

[10.2.](#) Content-DPR

- o Header field name: Content-DPR
- o Applicable protocol: HTTP
- o Status: standard
- o Author/Change controller: IETF
- o Specification document(s): [Section 3.1](#) of this document
- o Related information: for Client Hints

[10.3.](#) Downlink

- o Header field name: Downlink
- o Applicable protocol: HTTP
- o Status: standard
- o Author/Change controller: IETF
- o Specification document(s): [Section 6](#) of this document
- o Related information: for Client Hints

[10.4.](#) DPR

- o Header field name: DPR
- o Applicable protocol: HTTP
- o Status: standard
- o Author/Change controller: IETF
- o Specification document(s): [Section 3](#) of this document
- o Related information: for Client Hints

[10.5.](#) Save-Data

- o Header field name: Save-Data

- o Applicable protocol: HTTP
- o Status: standard
- o Author/Change controller: IETF
- o Specification document(s): [Section 7](#) of this document
- o Related information: for Client Hints

[10.6.](#) Viewport-Width

- o Header field name: Viewport-Width
- o Applicable protocol: HTTP
- o Status: standard
- o Author/Change controller: IETF
- o Specification document(s): [Section 5](#) of this document
- o Related information: for Client Hints

[10.7.](#) Width

- o Header field name: Width
- o Applicable protocol: HTTP
- o Status: standard
- o Author/Change controller: IETF
- o Specification document(s): [Section 4](#) of this document
- o Related information: for Client Hints

[11.](#) References

[11.1.](#) Normative References

- [CSS2] Bos, B., Celic, T., Hickson, I., and H. Lie, "Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification", W3C Recommendation REC-CSS2-20110607, June 2011, <<http://www.w3.org/TR/2011/REC-CSS2-20110607>>.
- [NETINFO] Caceres, M., Moreno, F., and I. Grigorik, "Network Information API", December 2015, <<https://w3c.github.io/netinfo/>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

Requirement Levels", [BCP 14](#), [RFC 2119](#),
DOI 10.17487/RFC2119, March 1997,
<<http://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,
<<http://www.rfc-editor.org/info/rfc5234>>.
- [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,
<<http://www.rfc-editor.org/info/rfc7230>>.

Grigorik

Expires April 7, 2017

[Page 11]

Internet-Draft

HTTP Client Hints

October 2016

- [RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", [RFC 7231](#),
DOI 10.17487/RFC7231, June 2014,
<<http://www.rfc-editor.org/info/rfc7231>>.
- [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,
<<http://www.rfc-editor.org/info/rfc7234>>.
- [W3C.CR-css-values-3-20150611]
Atkins, T. and E. Etemad, "CSS Values and Units Module Level 3", World Wide Web Consortium CR CR-css-values-3-20150611, June 2015,
<<http://www.w3.org/TR/2015/CR-css-values-3-20150611>>.
- [W3C.REC-html5-20141028]
Hickson, I., Berjon, R., Faulkner, S., Leithead, T., Navara, E., O'Connor, T., and S. Pfeiffer, "HTML5", World Wide Web Consortium Recommendation REC-html5-20141028, October 2014,
<<http://www.w3.org/TR/2014/REC-html5-20141028>>.

[11.2](#). Informative References

[I-D.ietf-httpbis-key]

Fielding, R. and M. Nottingham, "The Key HTTP Response Header Field", [draft-ietf-httpbis-key-01](#) (work in progress), March 2016.

[RFC6265] Barth, A., "HTTP State Management Mechanism", [RFC 6265](#), DOI 10.17487/RFC6265, April 2011, <<http://www.rfc-editor.org/info/rfc6265>>.

[Appendix A](#). Changes

[A.1](#). Since -00

- o Issue 168 (make Save-Data extensible) updated ABNF.
- o Issue 163 (CH review feedback) editorial feedback from httpwg list.
- o Issue 153 (NetInfo API citation) added normative reference.

[A.2](#). Since -01

- o Issue 200: Moved Key reference to informative.
- o Issue 215: Extended passive fingerprinting and mitigation considerations.

Grigorik

Expires April 7, 2017

[Page 12]

Internet-Draft

HTTP Client Hints

October 2016

- o Changed document status to experimental.

[A.3](#). Since -02

None yet.

Author's Address

Ilya Grigorik
Google

Email: ilya@igvita.com

URI: <https://www.igvita.com/>

