Early Hints

Kazuho Oku
103 Early Hints

- notifies headers that are *likely* to appear in the final response

```
GET / HTTP/1.1
Host: example.com

HTTP/1.1 103 Early Hints
Link: </style.css>; rel=preload

HTTP/1.1 200 OK
Content-Type: text/html
Link: </style.css>; rel=preload

<!DOCTYPE HTML>
...
```
Changes since Seoul

• became WG draft
  – intended track: experimental
• reminder of cross-origin information leak
  – in security considerations
• forbid processing the header as part of the informational response itself
Cross-origin information leak

- a broken client may misinterpret a response as belonging to a different origin
  - if it doesn’t recognize 1xx response
  - and if it connects through a forward proxy

<table>
<thead>
<tr>
<th>Request</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET / HTTP/1.1 Host: example.com</td>
<td>HTTP/1.1 103 Early Hints Link: &lt;/style.css&gt;; rel=preload</td>
</tr>
<tr>
<td>GET / HTTP/1.1 Host: example.jp</td>
<td>HTTP/1.1 200 OK Content-type: text/plain</td>
</tr>
</tbody>
</table>

This response is for the first request, but...

HTTP/1.1 200 OK
...

Early Hints (IETF 98)
Cross-origin information leak

• non-issue for HTTPS
  – since no intermediaries exist
• non-issue for HTTP/2
  – since request-response relationship is retained by a stream ID
When to apply 103 headers

• Q. should the headers of 103 response processes as part of the informational response itself, as well as (speculatively) processing them as part of the final response?
  – asked by Vasiliy Faronov on the mailing list, using Warning header as an example
When to apply 103 headers

• RFC 7231:
  – (MUST) treat an unrecognized status code as being equivalent to the x00 status code of that class / the client can simply discard this interim response (for 100 continue)
  – a user agent MAY ignore unexpected 1xx responses

• RFC 6265:
  – MAY ignore Set-Cookie headers contained in responses with 100-level status codes
When to apply 103 headers

• available options:
  – leave it a MAY or be explicit in either way

• approach in -01: be explicit
  – “client MUST NOT process the headers included in the (103) response as if they belonged to the informational response.”
  – reasoning:
    • well-defined behavior will benefit us in the long-term
    • that’s what most clients do today (am I correct?)