

Cache Digests for HTTP/2

Kazuho Oku
Fastly

Changes from draft-01

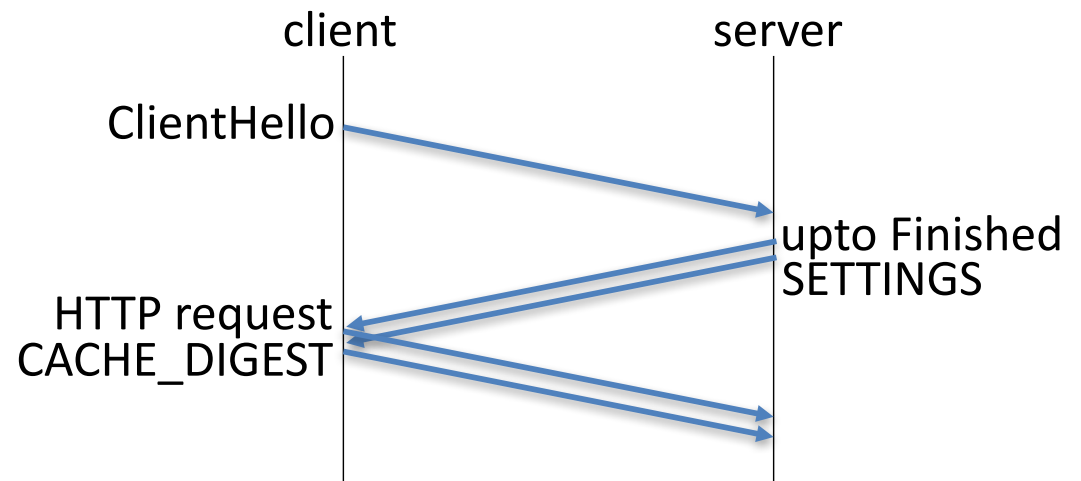
- added definition of the Cache-Digest header
- introduce `ACCEPT_CACHE_DIGEST_SETTINGS` parameter
- change intended status to Experimental

Cache-Digest header

- base64 digest value and flags
 - e.g., Cache-Digest: AfdA; complete
- document the format existing impls use
 - Apache, H2O, cache-digest-immutable (node)

ACCEPT_CACHE_DIGEST

- H2 SETTINGS parameter to indicate if the server supports cache digests
 - can be sent in 0.5 RTT in TLS 1.3 full handshake
 - no 0.5 RTT in case of 0-RTT resumption



Recommended client behavior

- send `CACHE_DIGEST` only when server sends `ACCEPT_CACHE_DIGEST`
- remember if the server accepts cache digest in the resumption cache, and use the value on resumption