

Cache Digests for HTTP/2

Kazuho Oku
Fastly

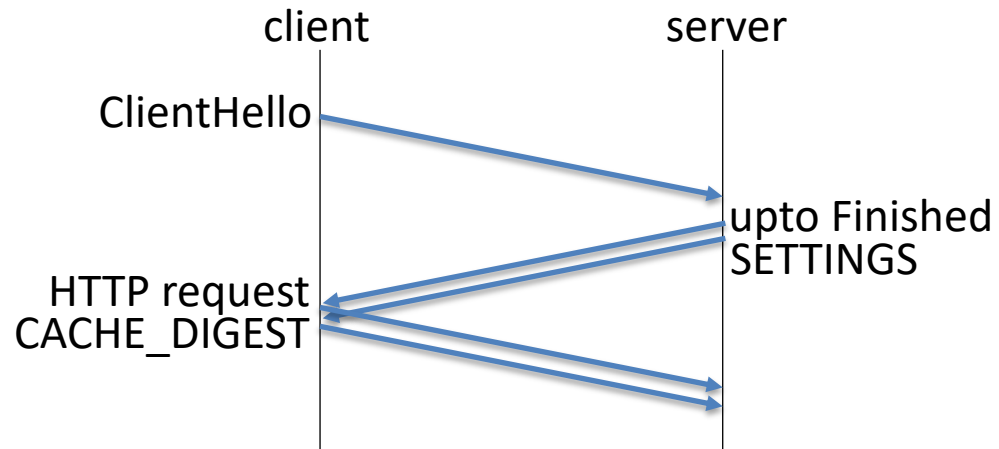
Changes from draft-02

- switch to Cuckoo Hash
- open issues:
 - negotiating the use #410
 - remove etag / stale support #516

Negotiating the Use #410

Current approach: use SETTINGS

- **SENDING_CACHE_DIGEST:**
 - indicates client-support
- **ACCEPT_CACHE_DIGEST:**
 - indicates server-support
 - sent in 0.5 RTT in TLS 1.3 full handshake
 - client can remember



Current approach: issues

- server's indication is per-connection
 - need to be per-origin?
 - use ORIGIN frame?
- require clients to cache the info?
 - currently it's a MAY

remove etag / stale support #516

Current approach: four types of digests

digest key / cache state	server's strategy	
	match found	match not found
SHA(URL) / fresh	do not push	push
SHA(URL) / stale	push Etag only**	push
SHA(URL + Etag)* / fresh	do not push	push***
SHA(URL + Etag)* / stale	push Etag only**	push

*: hard to use unless h2 endpoint and cache (that store's the Etag value) exist on a single machine

**: up-to-date value of the Etag needs to be transferred, but how?

***: existing clients do not adopt the pushed response if it has a fresh cache

Proposal: remove etag / stale support

- i.e. concentrate on *SHA(URL) / fresh* case
 - since majority of the resources that block rendering are long-term cacheable
 - see <http://bit.ly/crit-res-cacheability> by Yoav

