Template-Driven HTTP CONNECT Proxying for TCP

Ben Schwartz, Meta Platforms Inc.
HTTPBIS @ IETF 117

Reminder: Template-driven TCP Transport Proxy (i.e. MASQUE for TCP)

Proxy is identified by a template:

```
https://proxy.example/tcp
{?target_host,tcp_port}
```

In HTTP/1.1:

```
GET /tcp?
    target_host=192.0.2.1&
    tcp_port=443 HTTP/1.1
Host: proxy.example:443
Connection: Upgrade
Upgrade: connect-tcp
```

In HTTP/2 & HTTP/3:

```
:method = CONNECT
:protocol = connect-tcp
:scheme = https
:authority = proxy.example:443
:path = /tcp?
        target_host=192.0.2.1&
        tcp_port=443
...
```

Status

- Discussion at IETF 117 related to request smuggling and HTTP Upgrade
  - See draft-schwartz-httpbis-optimistic-upgrade-00
- Text related to “optimistic” content and TLS 0-RTT has been improved (next slide)
- Technical content has not changed recently
- **Ready for WGLC**

New since IETF 117: s/false start/optimistic/ and other adjustments to §4.1 (Latency Optimizations)

When using this specification in HTTP/2 or HTTP/3, clients MAY start sending TCP stream content optimistically, subject to flow control limits ([RFC9113], Section 5.2)([RFC9000], Section 4.1). Proxies MUST buffer this "optimistic" content until the TCP stream becomes writable, and discard it if the TCP connection fails. (This "optimistic" behavior is not permitted in HTTP/1.1 because it would prevent reuse of the connection after an error response such as "407 (Proxy Authentication Required)".)

Servers that host a proxy under this specification MAY offer support for TLS early data in accordance with [RFC8470]. Clients MAY send "connect-tcp" requests in early data, and MAY include "optimistic" TCP content in early data (in HTTP/2 and HTTP/3). At the TLS layer, proxies MAY ignore, reject, or accept the early_data extension ([RFC8446], Section 4.2.10). At the HTTP layer, proxies MAY process the request immediately, return a "425 (Too Early)" response ([RFC8470], Section 5.2), or delay some or all processing of the request until the handshake completes. For example, a proxy with limited anti-replay defenses might choose to perform DNS resolution of the target_host when a request arrives in early data, but delay the TCP connection until the TLS handshake completes.