# HiNT and HELIUM for UDP (and IP?) tunnelling

## Presentation to HTTPbis WG at IETF 102

17th July 2018

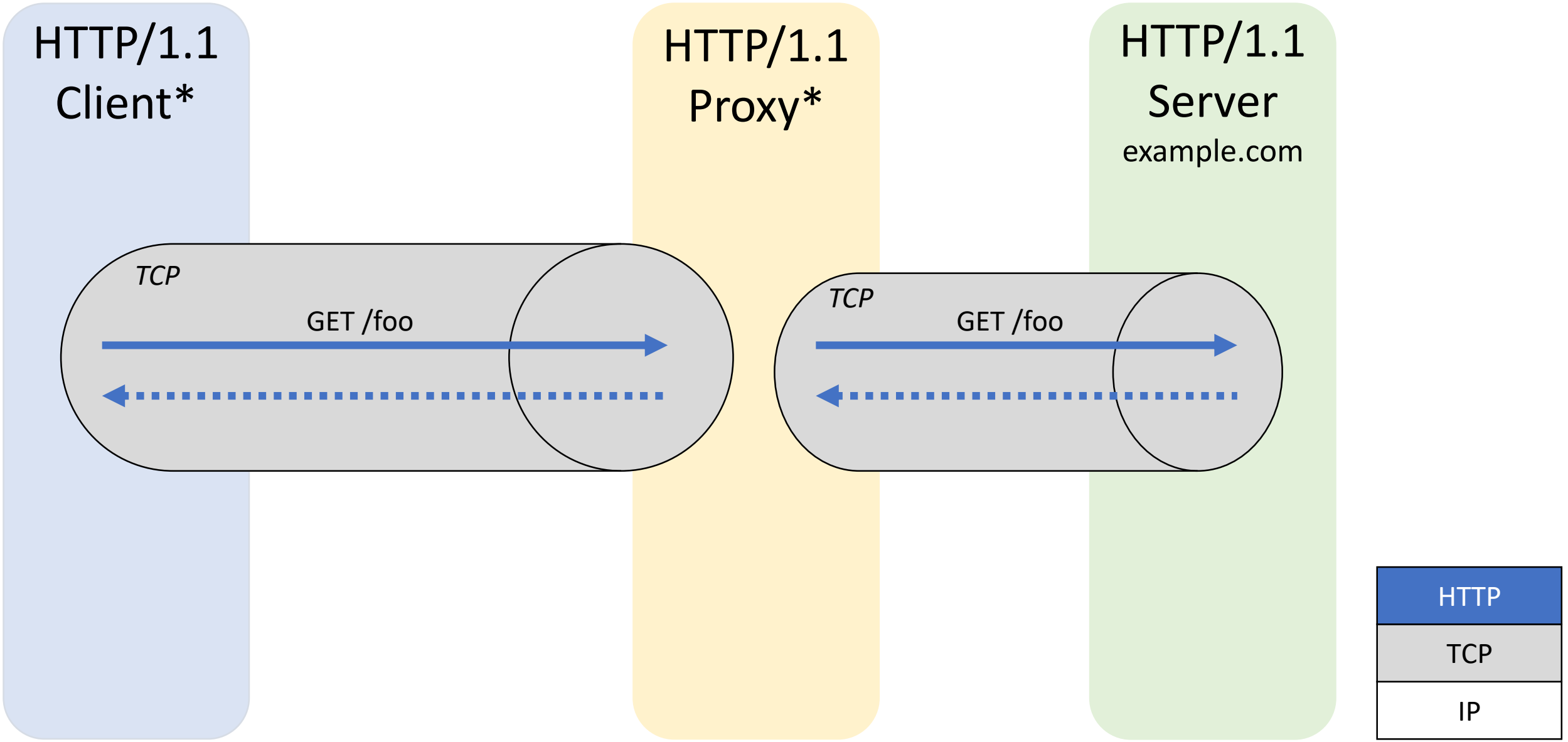
Lucas Pardue

BBC | Research & Development

# Internet-Drafts

- HiNT - HTTP-initiated Network Tunnelling
  - draft-pardue-httpbis-http-network-tunnelling-00
- HELIUM - Hybrid Encapsulation Layer for IP and UDP Messages
  - draft-schwartz-httpbis-helium-00
- Discussion is framed in terms of client-server proxying but tunnelling can be applied to other use cases.

# HTTP/1.1 via forward proxy

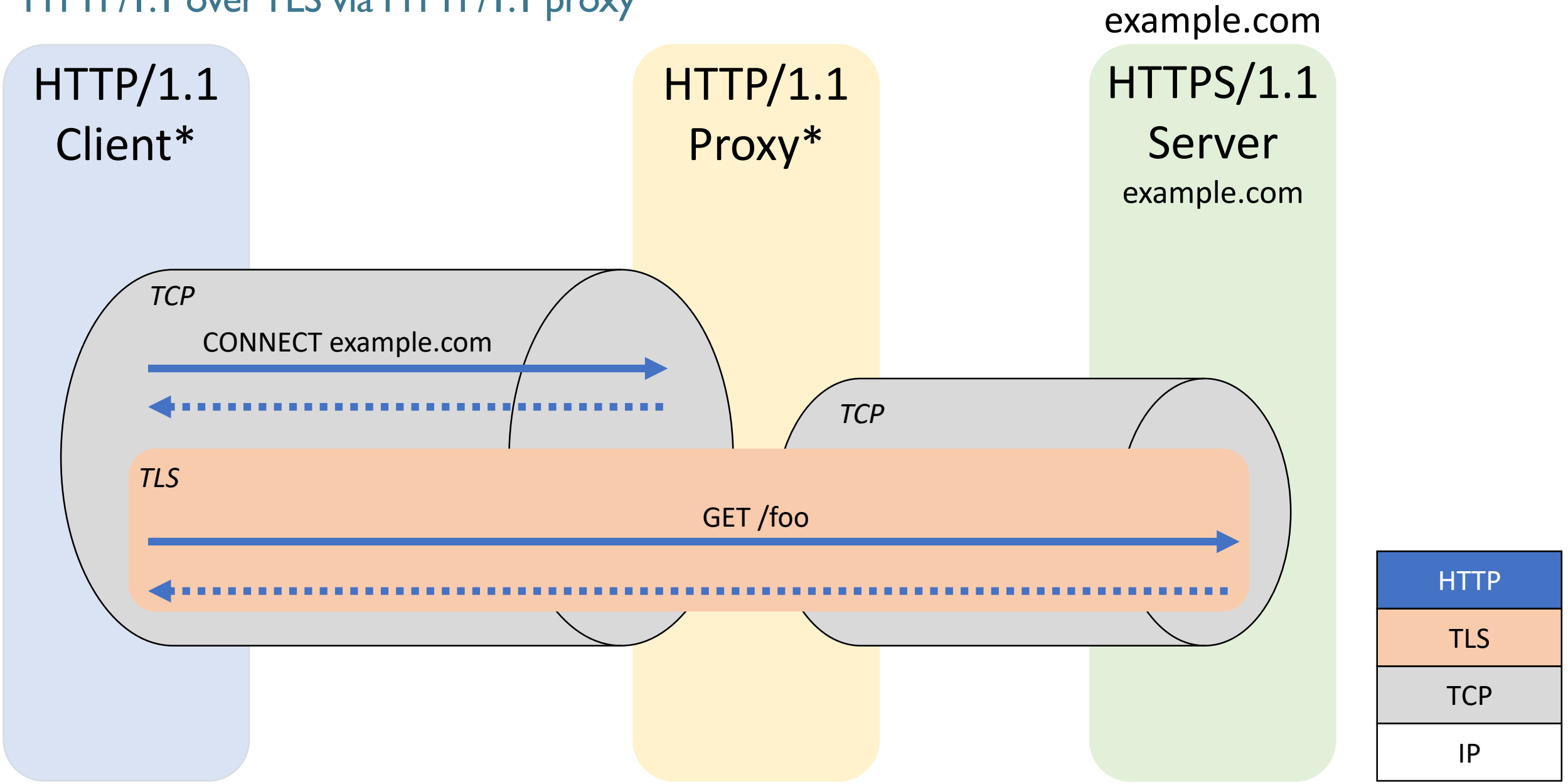



BBC | Research & Development



* Typically configured with http_proxy variable

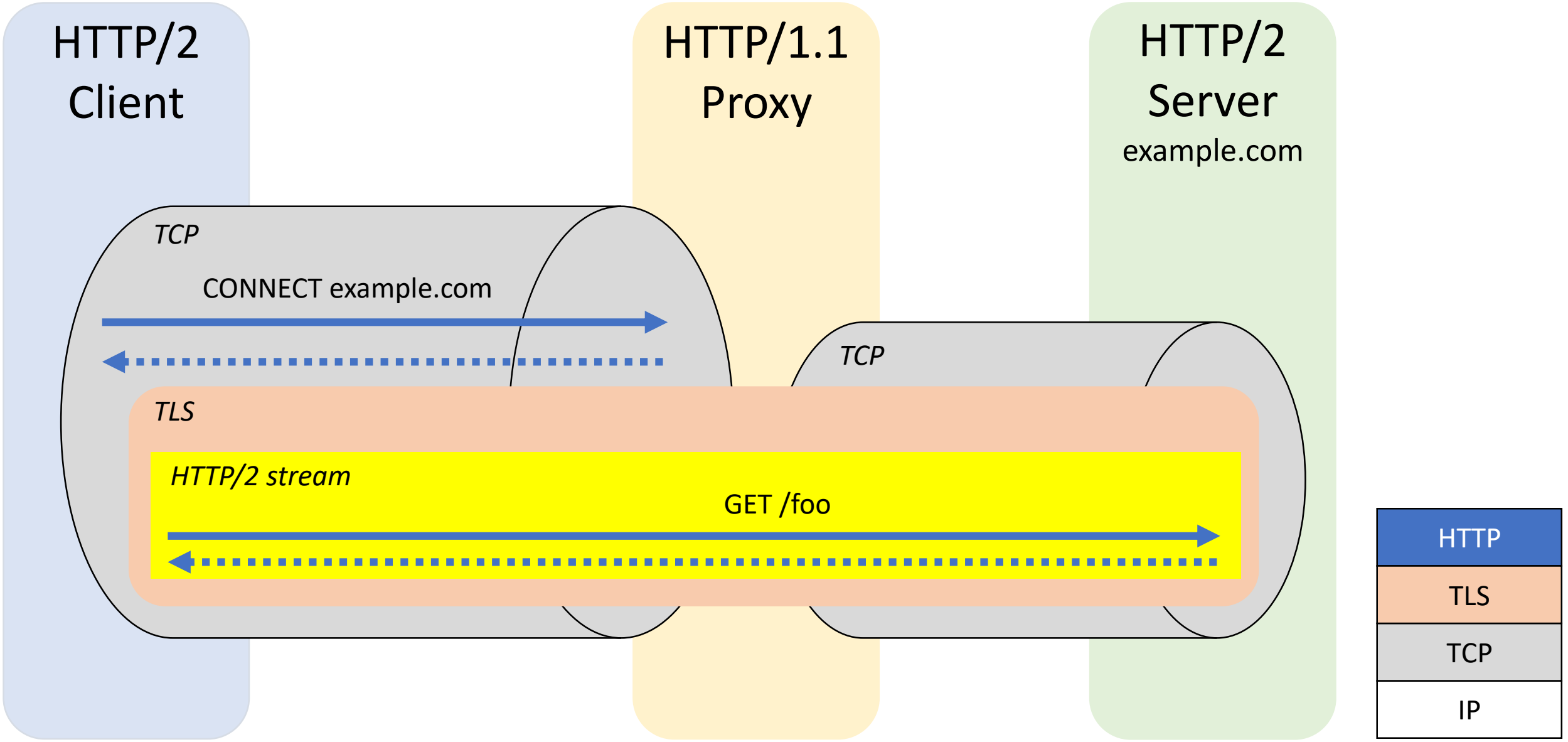
# HTTP/1.1 over TLS via HTTP/1.1 proxy



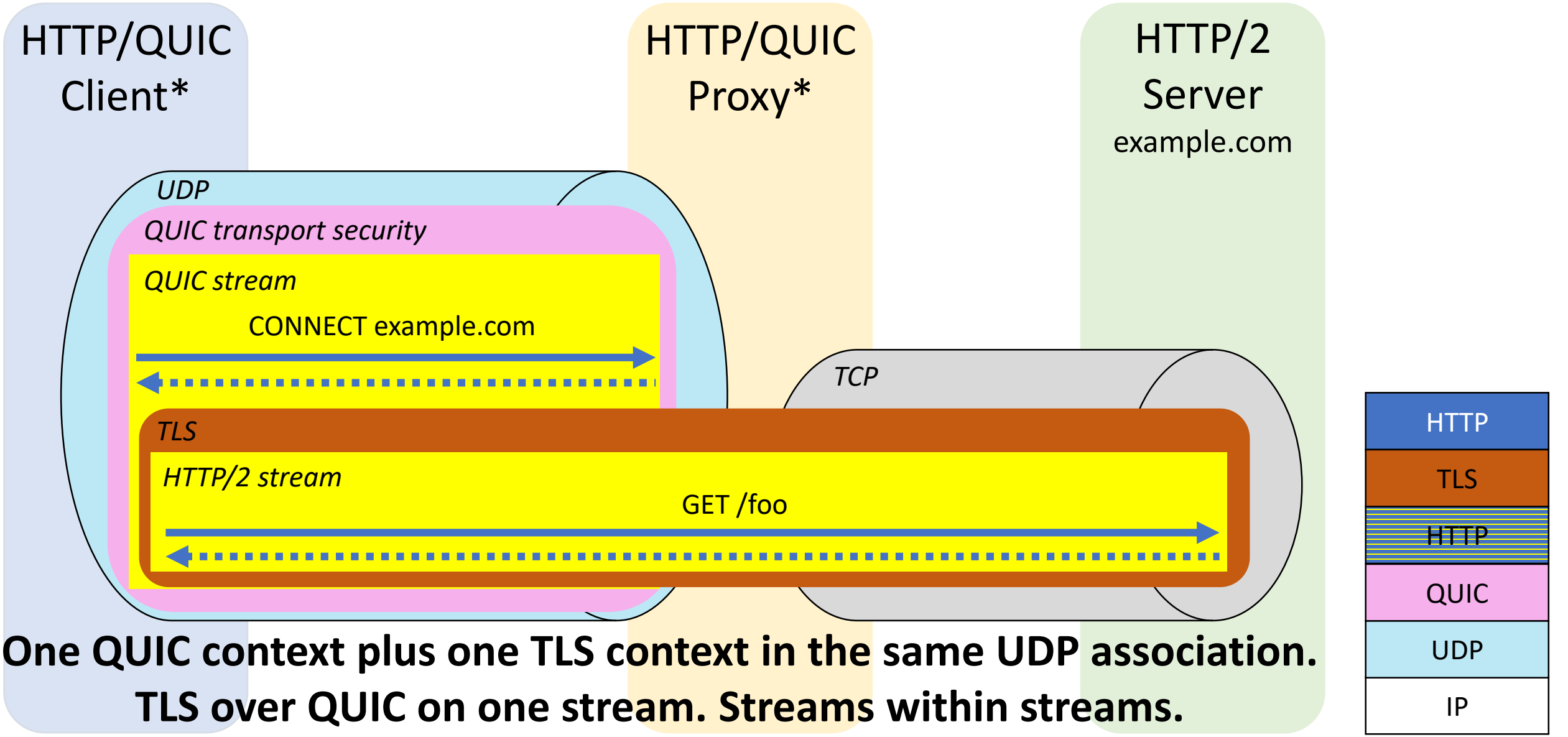



* Typically configured with https_proxy variable

# HTTP/2 over TLS via HTTP/1.1 forward proxy



# HTTP/2 over TLS via secure HTTP/QUIC forward proxy







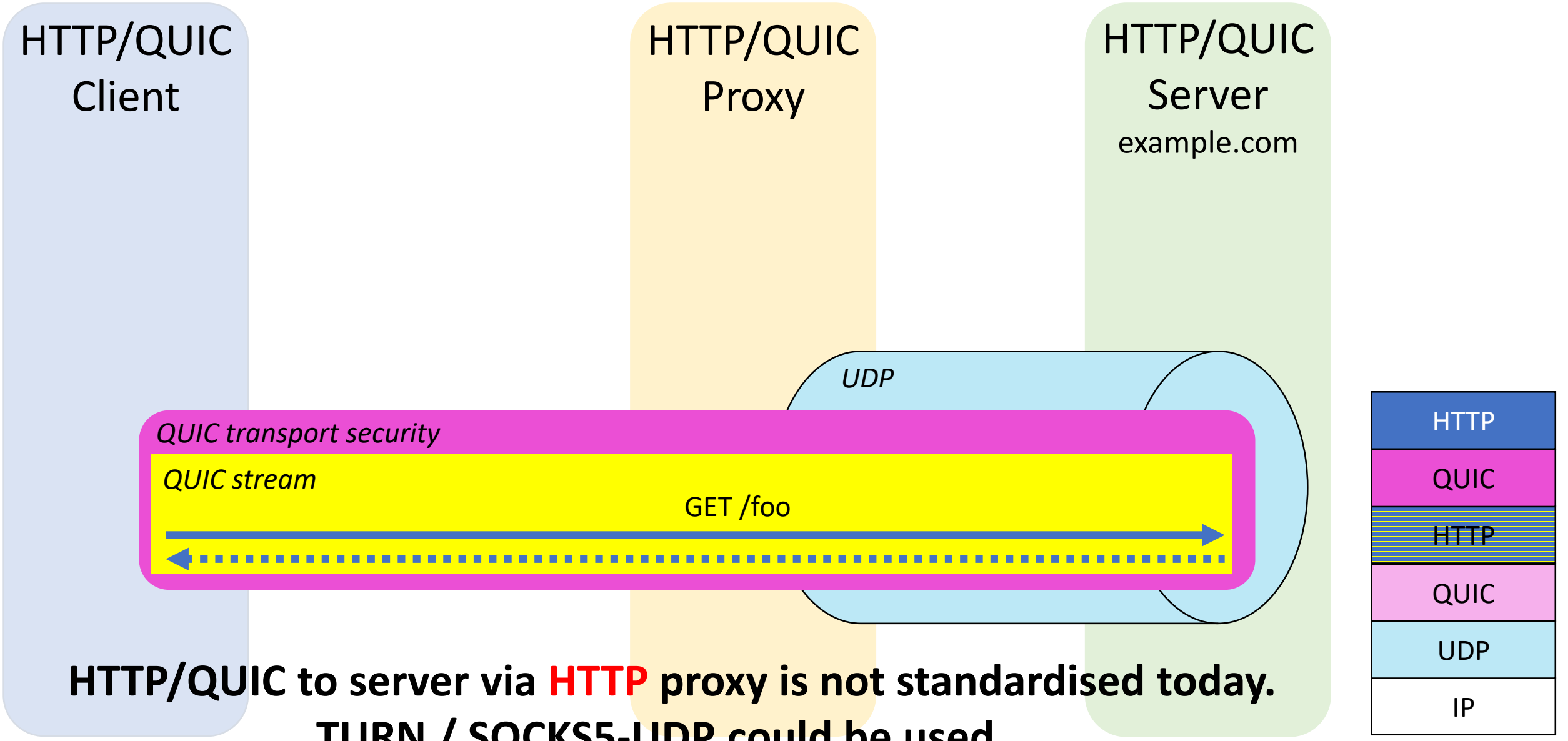
**One QUIC context plus one TLS context in the same UDP association.**

**TLS over QUIC on one stream. Streams within streams.**



* HTTP/QUIC advertised by the HTTP/QUIC proxy, or set up using prior knowledge (proxy.pac)

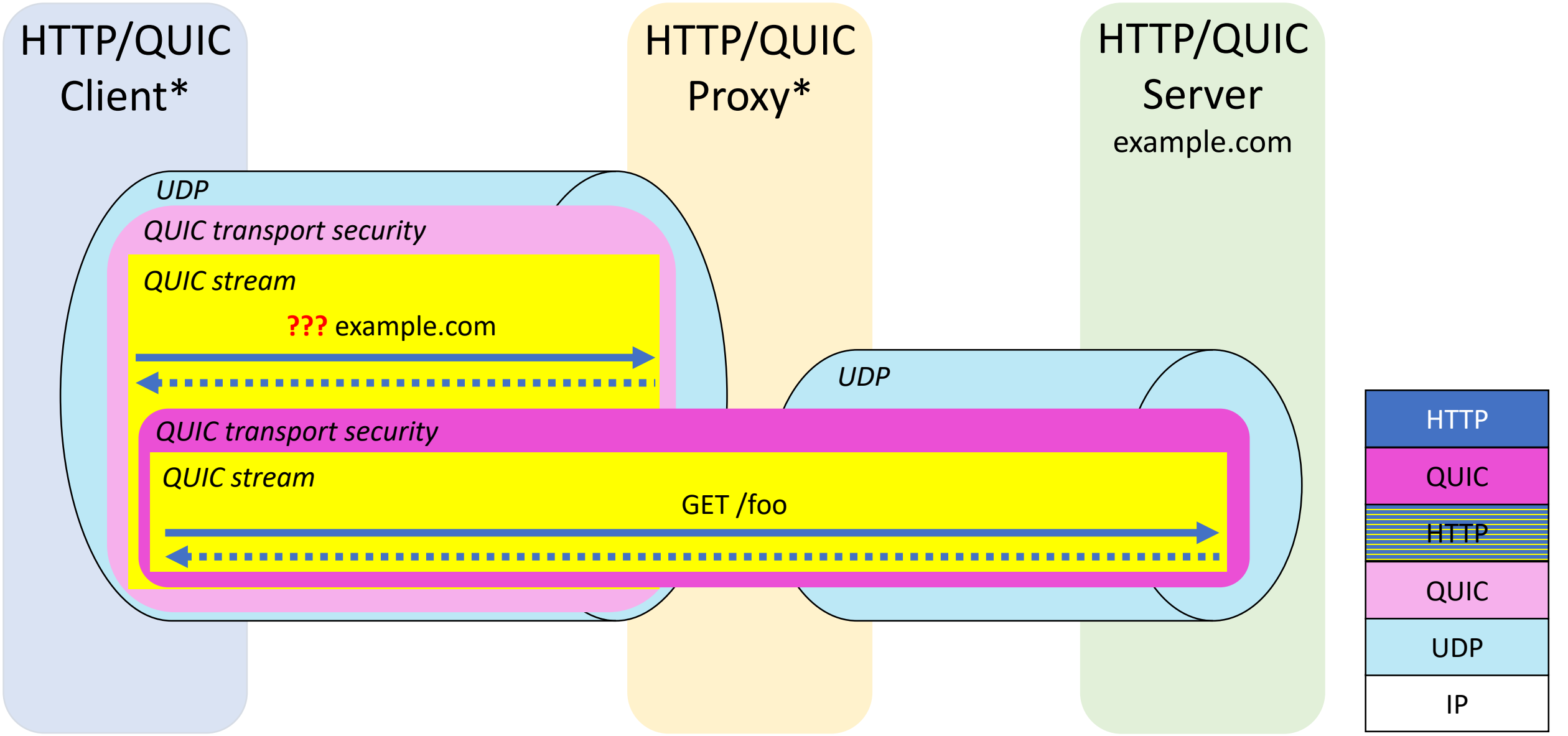
# HTTP over QUIC via forward proxy?




**HTTP/QUIC to server via HTTP proxy is not standardised today.**

**TURN / SOCKS5-UDP could be used…**

# Hypothetical: HTTP over QUIC via secure HTTP/QUIC forward proxy






* HTTP/QUIC advertised by the HTTP/QUIC proxy, or set up using prior knowledge (proxy.pac)

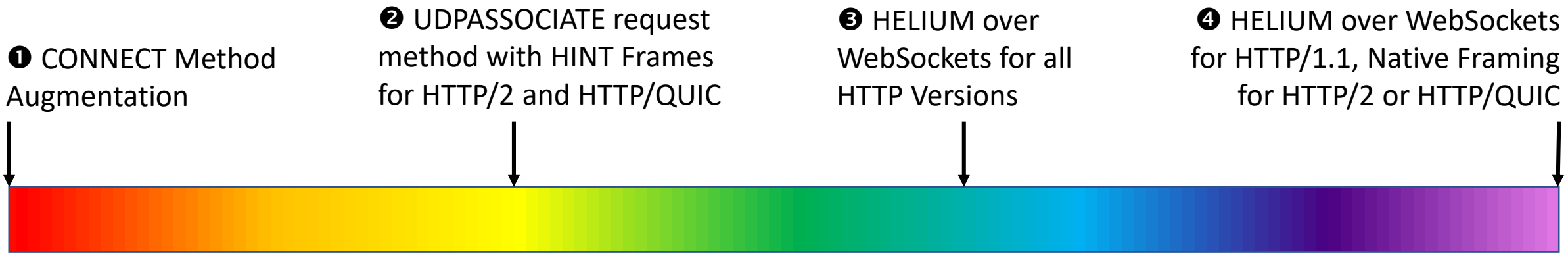
# HTTP-initiated Network Tunnelling (HiNT)

- Generalise the existing CONNECT-based tunnelling.
  - Conversion of an HTTP connection (in whole or in part) into a TCP, UDP or IP tunnel.
- Design considerations:
  - HTTP Version(s).
  - Tunnel proxy discovery and chaining.
  - Message destination agility.
  - Path MTU discovery.
  - Proxy's role in message passing - Blind forwarding vs. in-the-loop.
  - HoL blocking.
  - Padding for traffic obfuscation.
- I-D presents some options and weighs up pros and cons.

# HiNT proposed solution spectrum

- Initiation
  - Request method
  - HTTP/2 or HTTP/QUIC setting
- Message transfer
  - Framing of messages
  - Reservation of streams for particular tunnel

There are many permutations…



# HELIUM

- HELIUM: A lightweight, flexible proxy protocol based on IP.
- Designed to span many use cases:
  - Forwarding QUIC (c.f. SOCKS5-UDP)
  - WebRTC (c.f. TURN)
  - UDP proxy with ICMP support (e.g. traceroute, PMTUD)
  - VPN (c.f. OpenConnect, OpenVPN, L2TP)
- Currently uses CBOR, runs over a WebSocket (proposed solution ❸).
  - Possible to natively frame in HTTP/2 or HTTP/QUIC (proposed solution ❹).
- See detailed slides from DISPATCH.

# Closing

- There are already many ways to do UDP and IP network tunnelling
  - HTTP-based (-initiated) tunnelling has some unique benefits.
- There seems to be interest:
  - Is there enough interest in the community that warrants investing more time/effort?
- Input/guidance required:
  - Can/should we drive toward one solution?
    - Those presented or some new derivative.
  - Does this belong at a lower layer?
  - What is a suitable home in IETF for this work?

# Thank you

bbc.co.uk/rd

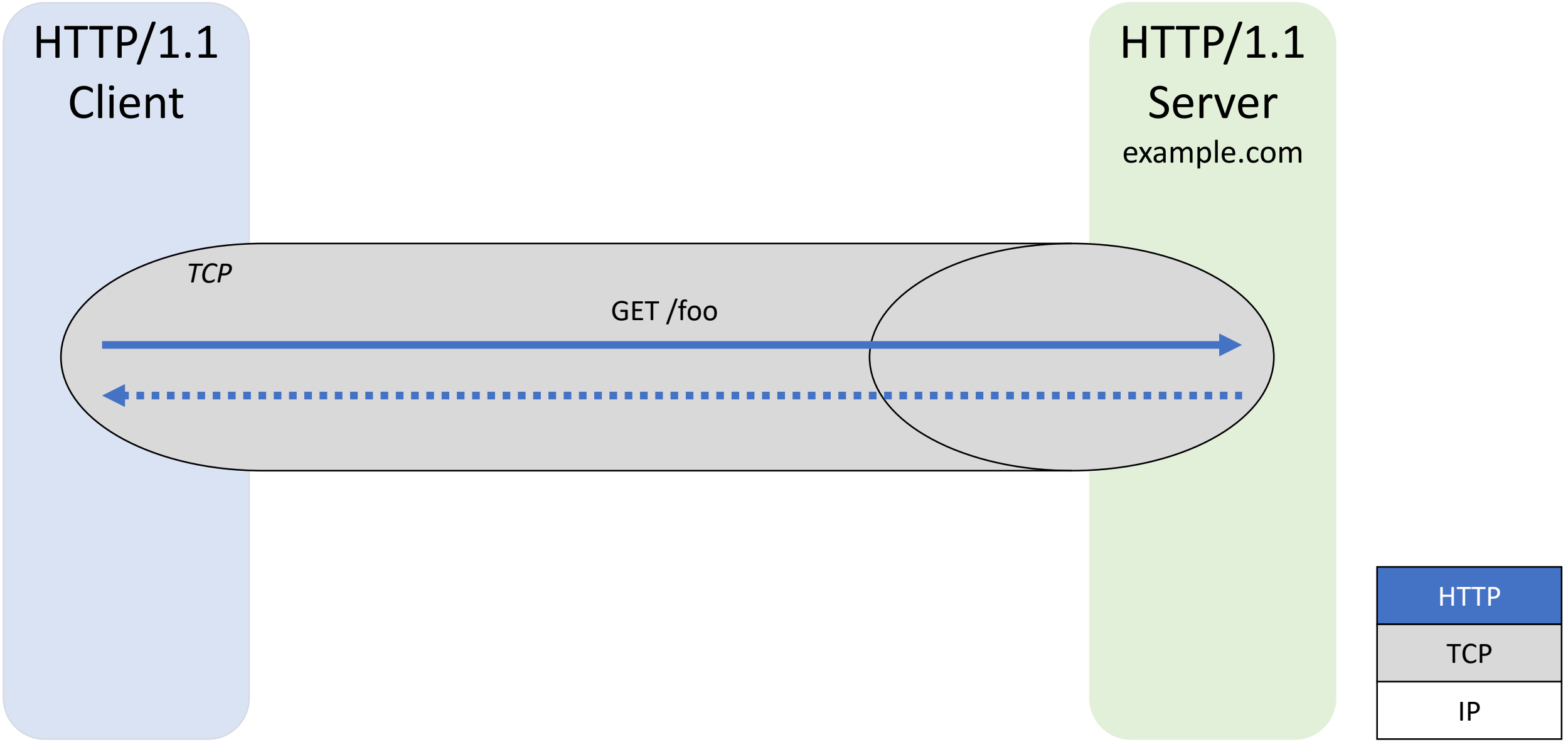
Email:

lucas.pardue@bbc.co.uk

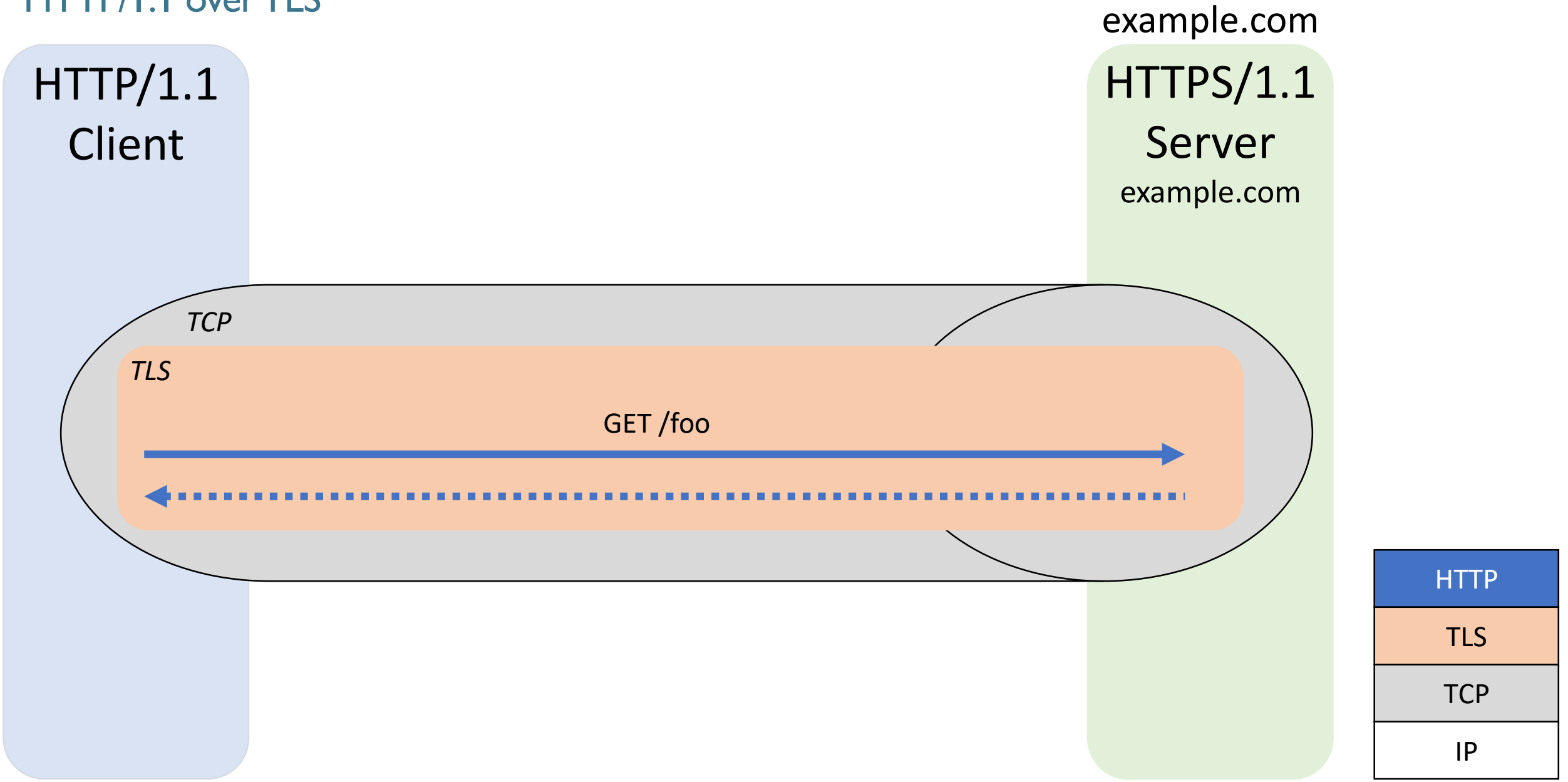
BBC | Research & Development

# Backup slides

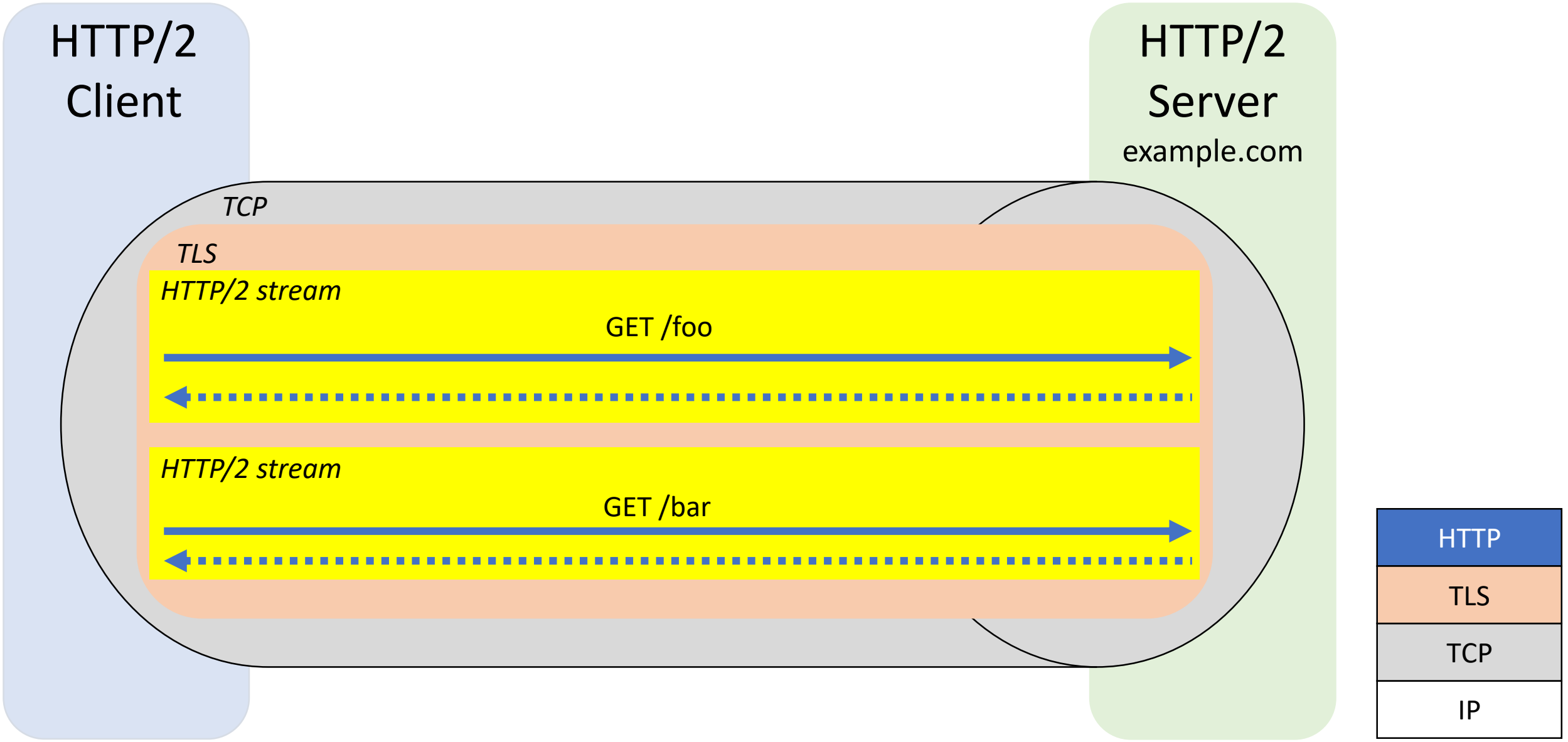
# HTTP/1.1 basic client-server interaction



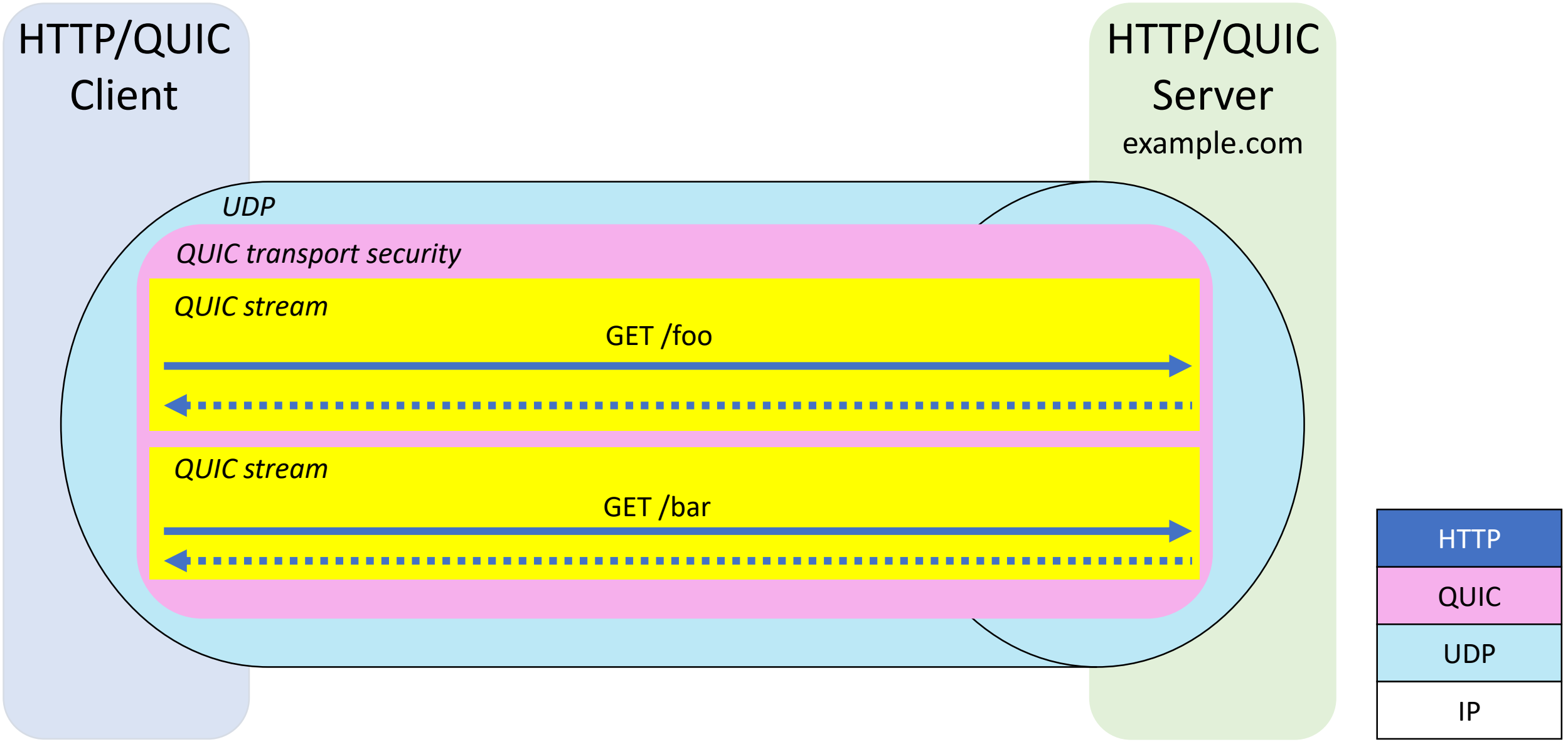
# HTTP/1.1 over TLS



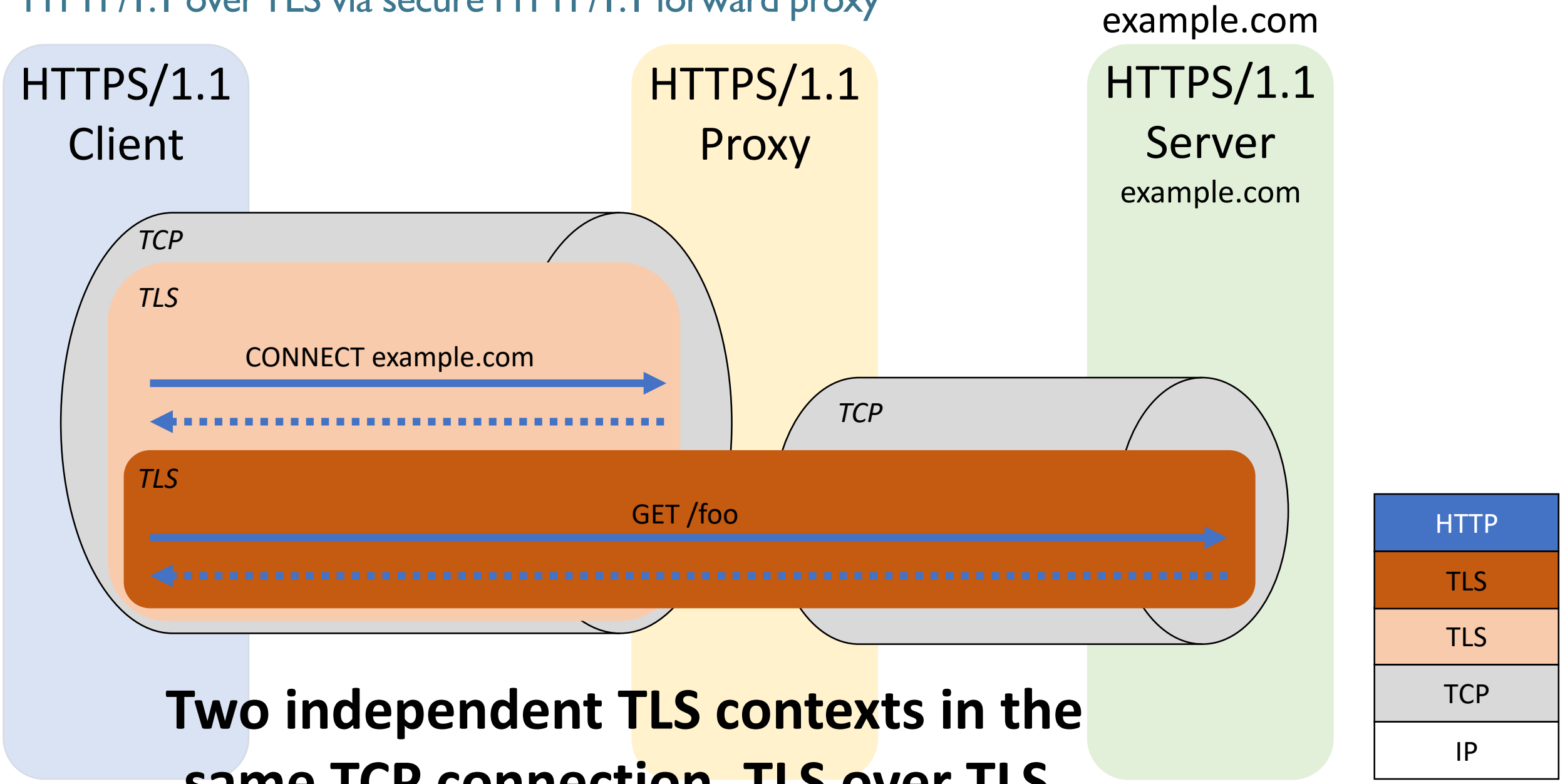
# HTTP/2 over TLS



# HTTP over QUIC

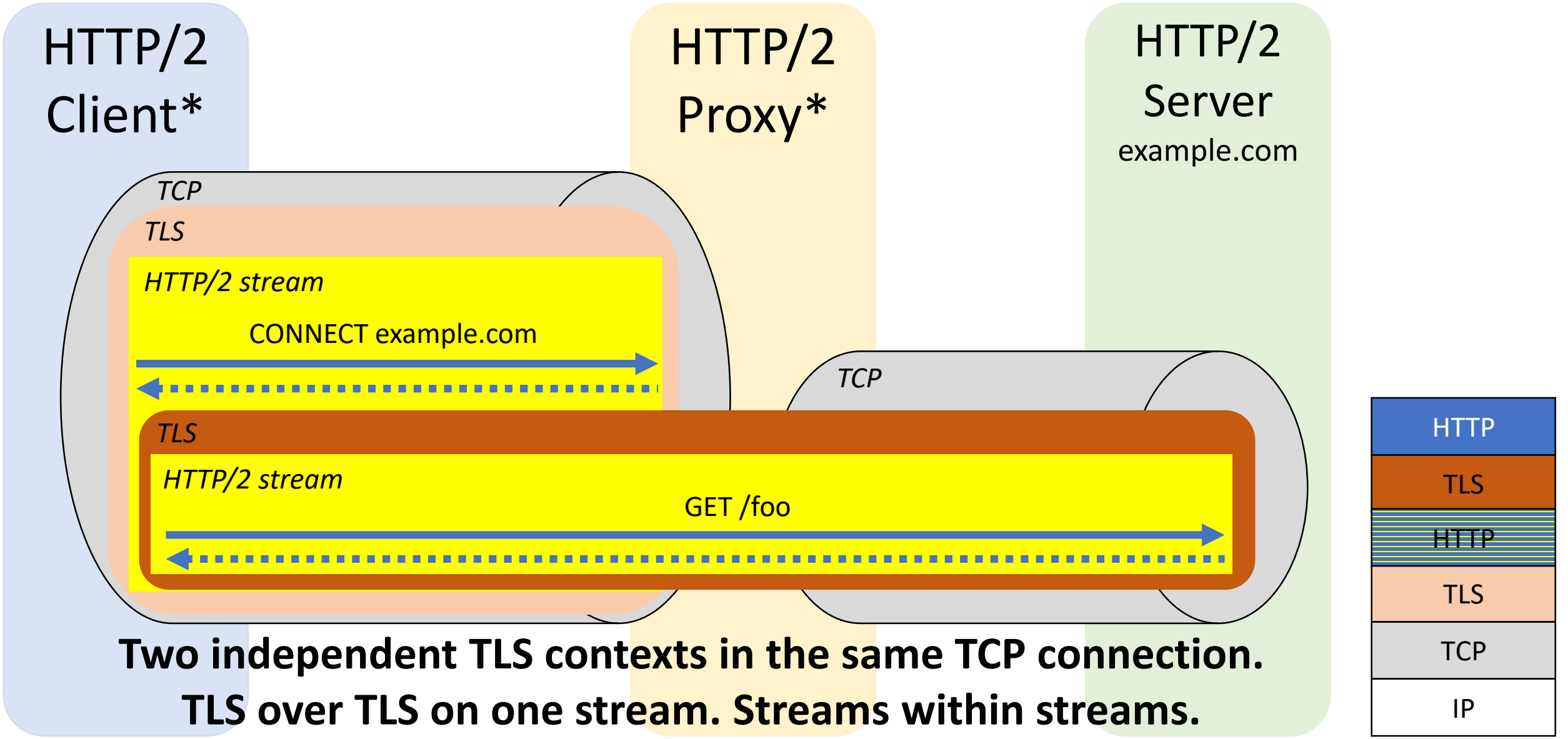


# HTTP/1.1 over TLS via secure HTTP/1.1 forward proxy




**Two independent TLS contexts in the same TCP connection. TLS over TLS.**

# HTTP/2 over TLS via secure HTTP/2 forward proxy




**Two independent TLS contexts in the same TCP connection.**
**TLS over TLS on one stream. Streams within streams.**



* HTTP/2 negotiated using ALPN

# HiNT framing

- Message transfer of proposed solution ❷.
- Client is unaware of UDP/IP in the tunnel: packetisation is done by the proxy.
- Frames sent on a stream contain payload for packetisation.
  - e.g. a QUIC packet.

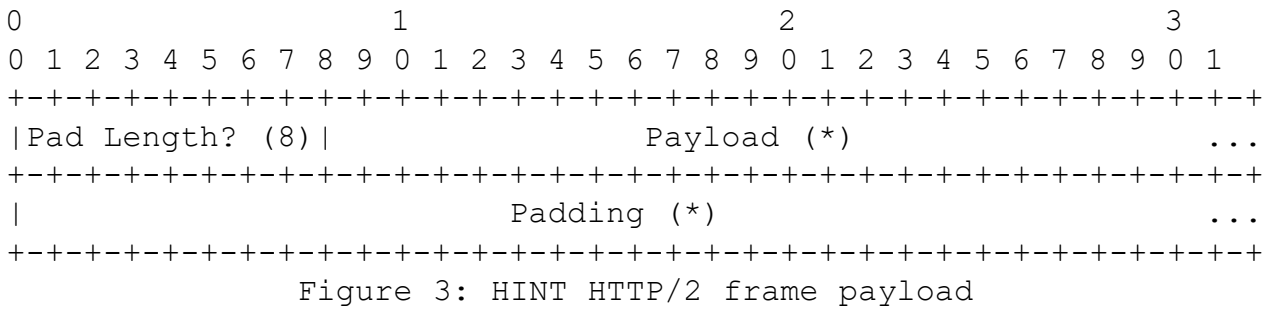



Figure 3: HINT HTTP/2 frame payload

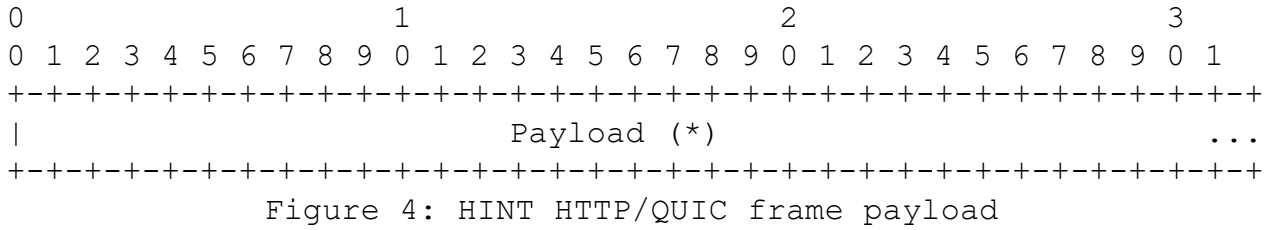
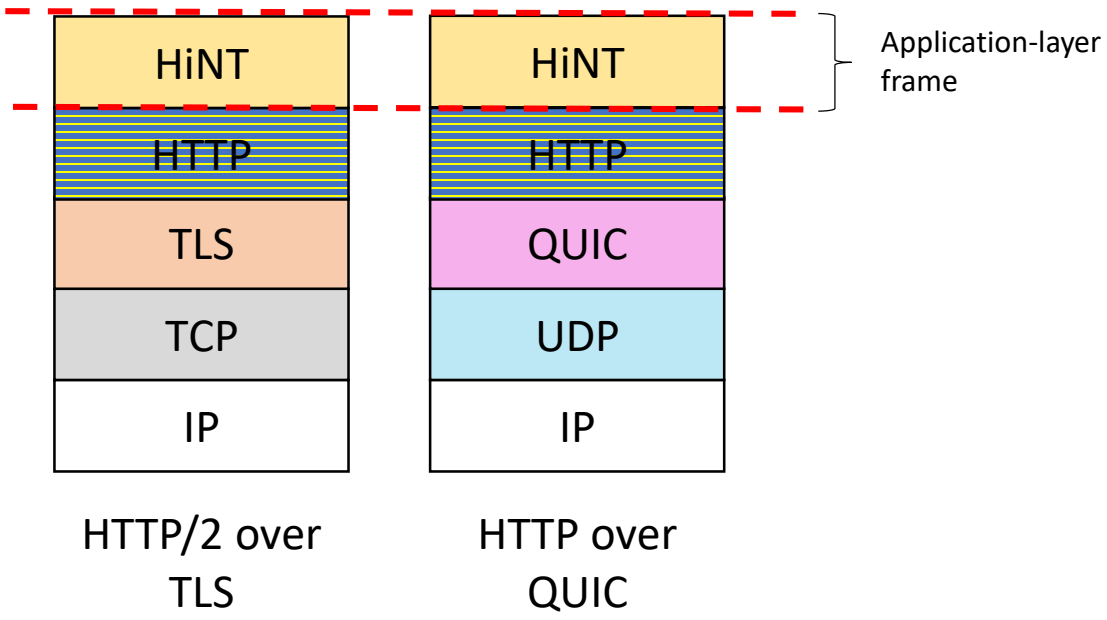


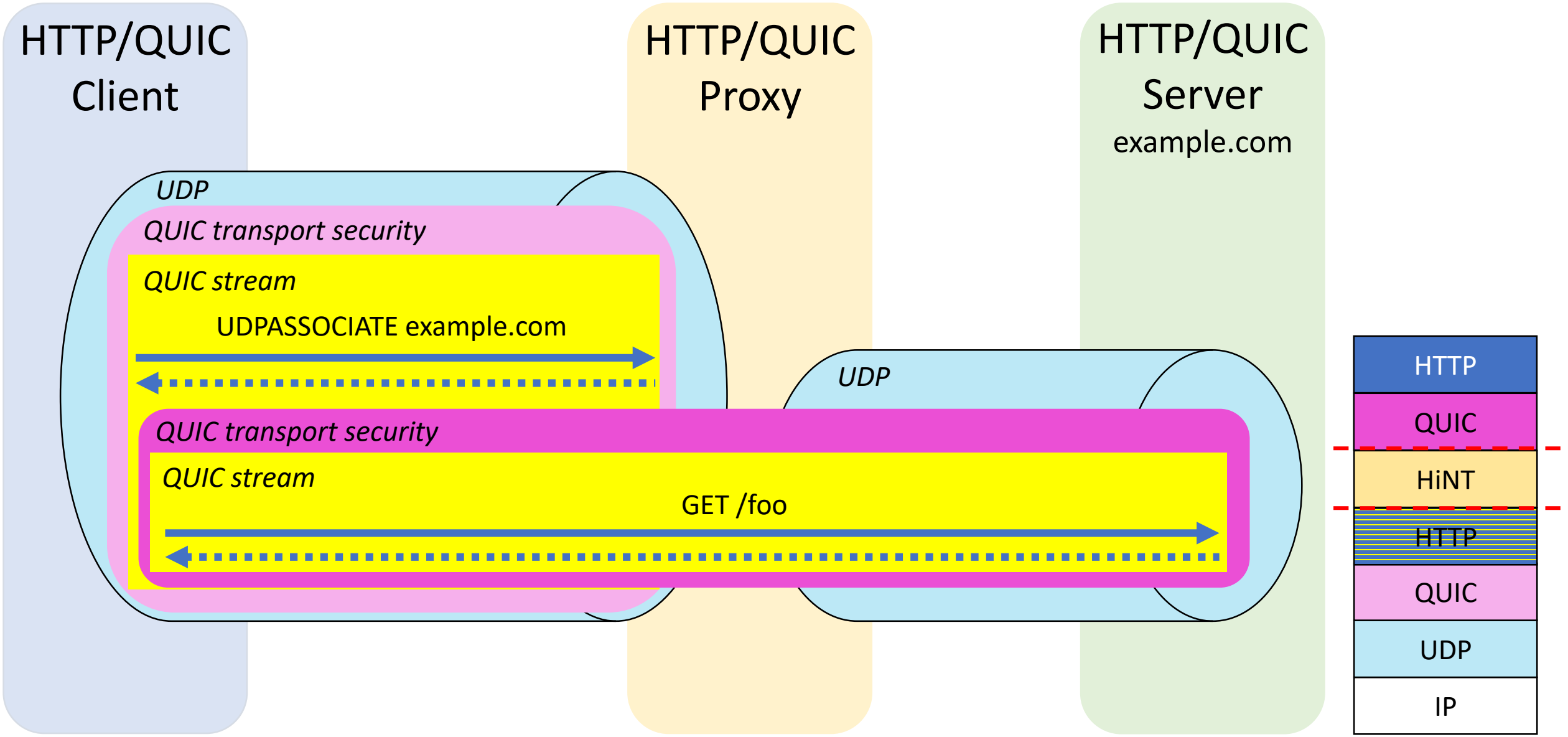

Figure 4: HINT HTTP/QUIC frame payload





Indicates a single reserved stream

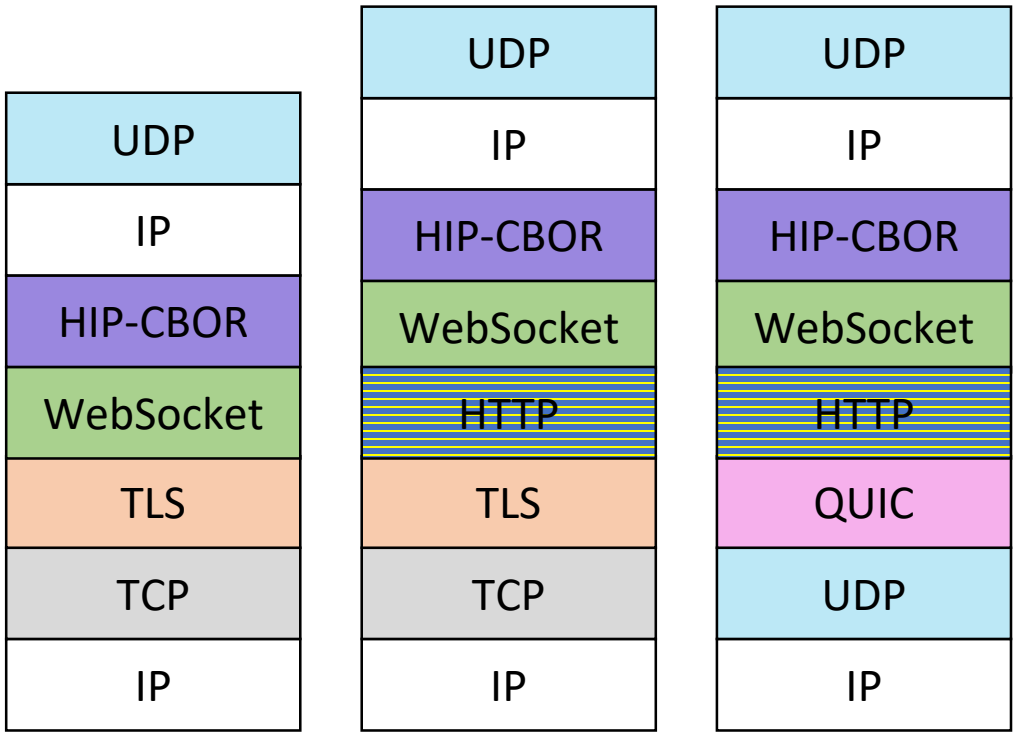
# UDPASSOCIATE and HiNT framing




 * HTTP/QUIC advertised by the HTTP/QUIC proxy, or set up using prior knowledge (proxy.pac)

# HELIUM over WebSockets and native framing

HELIUM over WebSocket



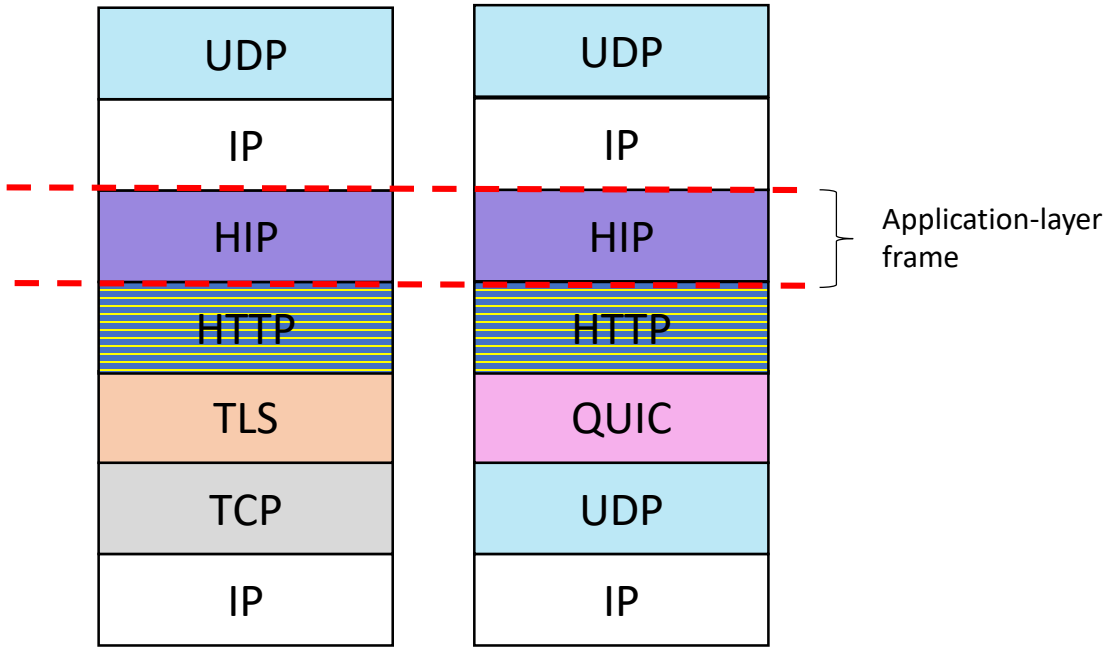

HTTP/1.1 over TLS

HTTP/2 over TLS

HTTP over QUIC*

*WebSockets over QUIC not defined (yet?)

HELIUM native framing (light or full)




HTTP/2 over TLS

HTTP over QUIC

HTTP — Indicates a single reserved stream