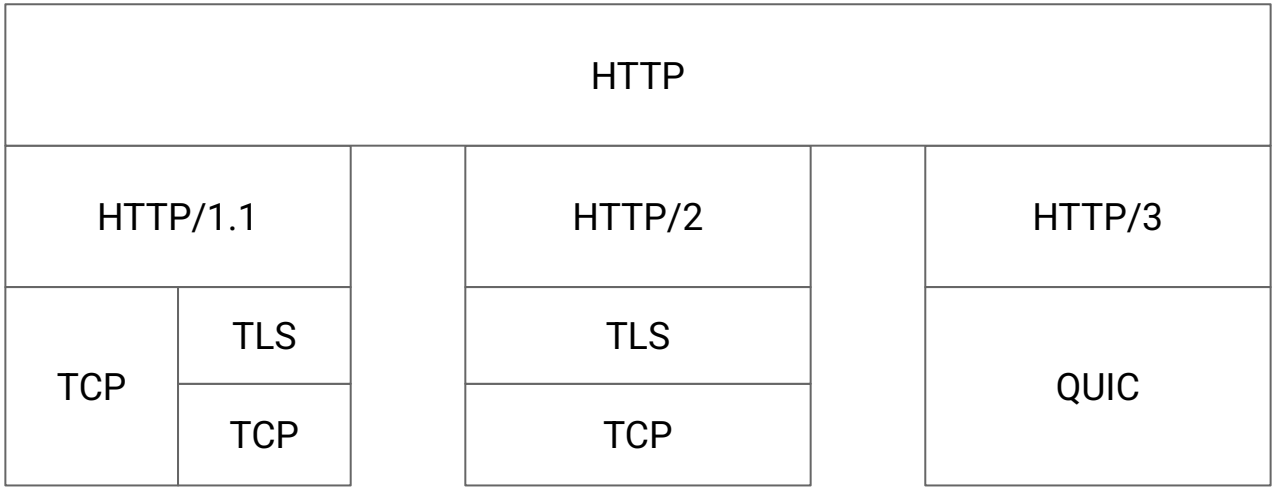
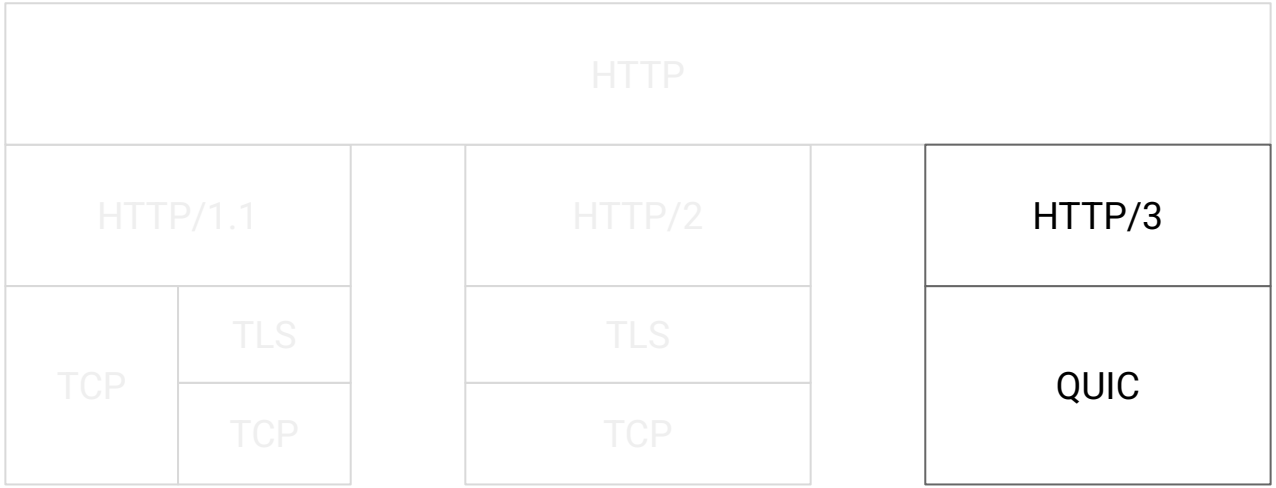
Forward and Reverse HTTP/3 over WebTransport

Ben Schwartz, Meta
Yaroslav Rosomakho, Zscaler

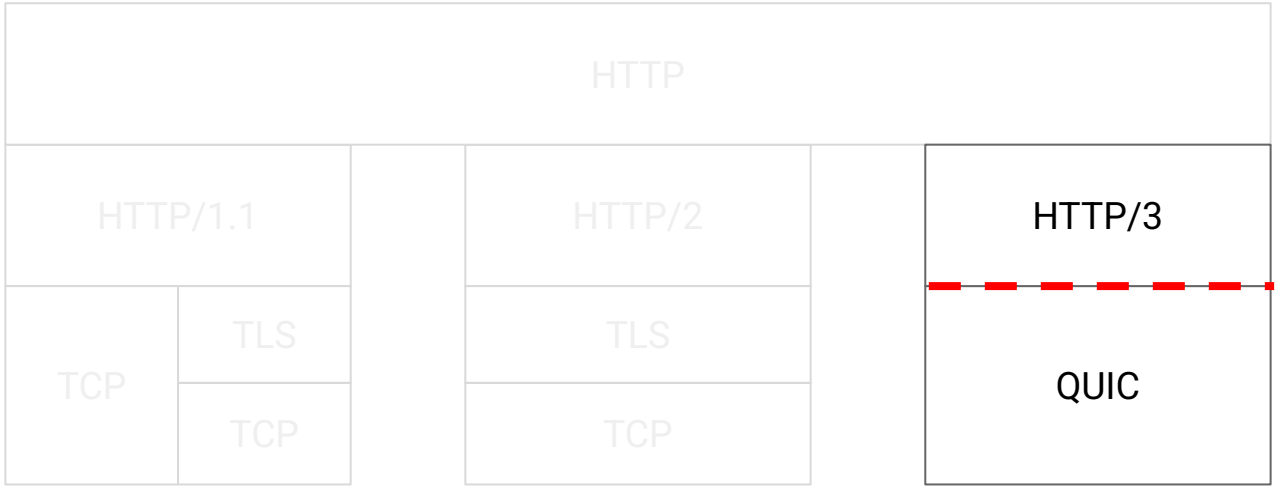
WEBTRANS @ IETF 122, March 2025



Background: The HTTP Stacks



Zoom In: HTTP/3

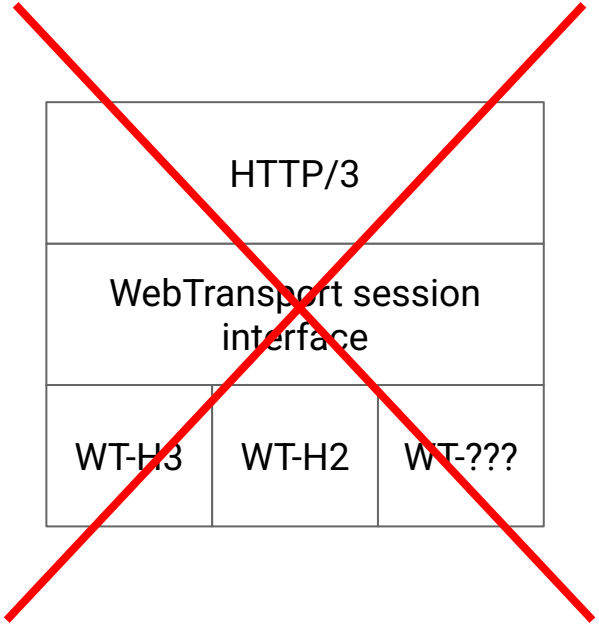


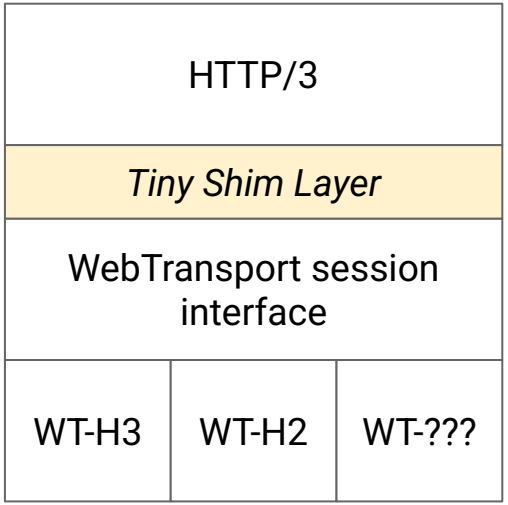
Zoom In: HTTP/3's Interface with QUIC

How does HTTP/3 interface with QUIC?

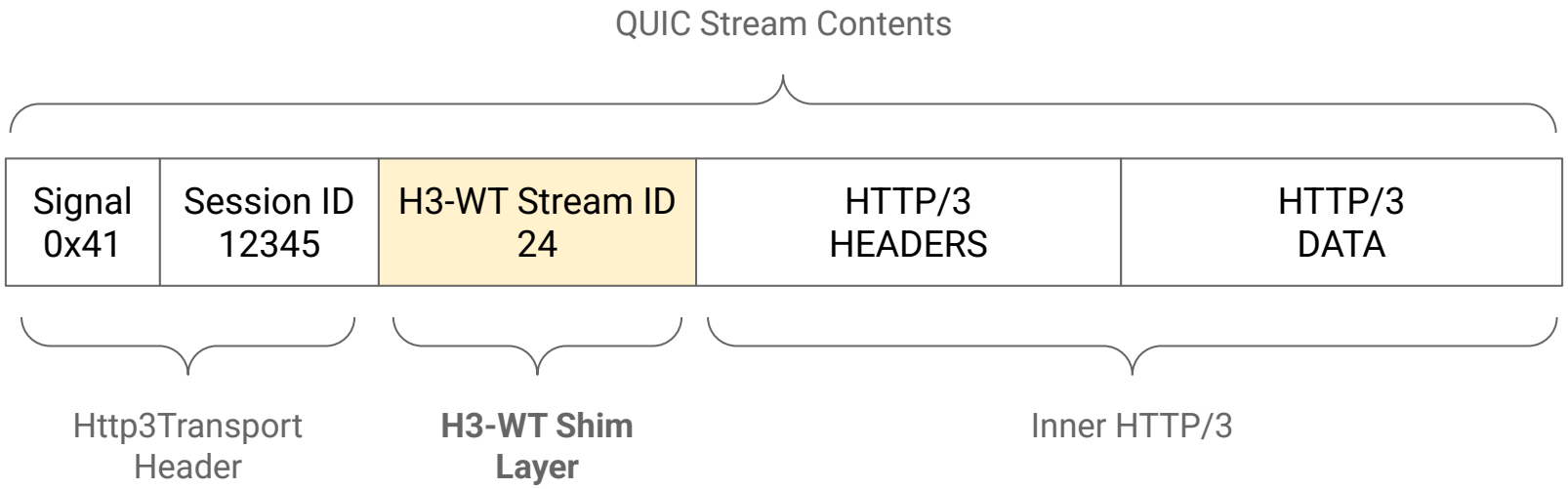
- Connect
- Create a Stream
  - By Client / By Server
  - Unidirectional / Bidirectional
- Use a stream
  - Read data / Write data
- Close a stream
  - Cleanly / With error code
- Close a connection
  - Cleanly / With error code
- Datagram (optional)
  - Send / Receive
  - Associated with the connection

This is the WebTransport session interface!





Architecture of HTTP/3 over WebTransport (H3-WT)



Tiny Shim Layer Restores End-to-End Stream IDs for GOAWAY and DATAGRAM

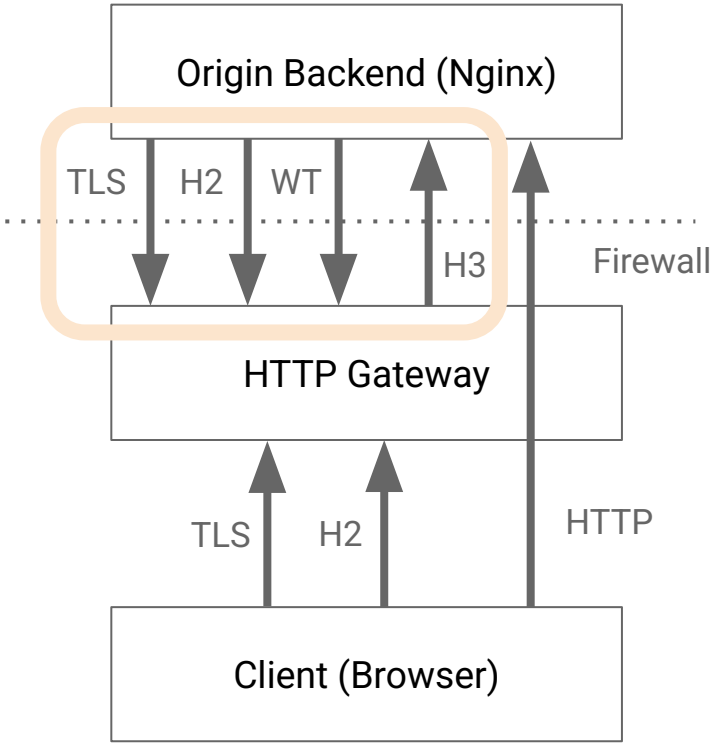
WebTransport is Symmetrical, so the roles can be reversed

- WebTransport roles:
  “**Dialer**” + “**Listener**”
- (Inner) HTTP roles:
  Server + Client

Dialer == Client ⇒ *Forward* H3-WT

Dialer == Server ⇒ *Reverse* H3-WT

Why?




```
nginx.conf:

server {
  server_name  bobs-backend.example;

  listen  443 ssl;

  listen_reverse {
    url  https://gateway.example/reverse/bob;
    auth {
      bearer YSBiZWFyZXIgdG9rZW4=;
  }

  location / {
    root   html;
    index  index.html;
  }
}
```

Example Use Case - Serving HTTP from a hidden backend

Other Use Cases

- Forward H3-WT
  - HTTP/3 over TCP (by private arrangement)
    - c.f. “QUIC on Streams”
  - Improved HTTP request proxy
    - Virtual-hosting
    - Distinguish proxy services by path
- Reverse H3-WT
  - Running an origin backend behind a firewall
    - Proprietary solutions available
  - Using a proxy to run a TCP server
    - c.f. SOCKS5 BIND (RFC 1928) or TURN-TCP (RFC 6062)
    - The proxy sends an HTTP CONNECT request to forward each incoming TCP connection.
  - Exposing controlled access to firewalled local databases and other resources.
    - Proprietary solutions available

Many Details - *Can be adjusted*

- MUST accept 3 unidirectional streams
- SHOULD accept 100 bidirectional streams
- Servers SHOULD send an ORIGIN frame
  - Unless it's irrelevant (e.g. for a request proxy) or clear from context.
- Authentication is by private arrangement.
- No .well-known/
- No reserved WT-Protocol value
- No ALPN

- Some optional features depend on the transport.
  - Authentication options for the connection vary between transports.
  - Secondary Certificate Authentication and Concealed Authentication inside the tunnel are possible, but only on transports that expose a TLS Exported Authenticator.
- Some do not!
  - HTTP/3 Datagrams can be negotiated even when running H3-WT over TCP.

Now Seeking

- More use cases
- Developer interest
- Technical review
- Adoption!
  - HTTPBIS or WEBTRANS?