MoQT Toronto: 0-RTT

Why do we care?

With no 0-RTT or resumption, establishing a session over H2 WebTransport is:

- TCP handshake
- TLS 1.3 handshake
- WebTransport handshake
- MoQ handshake
- Profit! (real MoQ happens now)

Constraints

FYI: WebTransport doesn’t have 0-RTT session establishment today

> *“Clients cannot initiate WebTransport in 0-RTT packets, as the CONNECT method is not considered safe”*

From RFC9000:

> *“if Early Data is supported, embed application-controlled data in the TLS resumption ticket sent to the client; and*
>
> *if Early Data is supported, retrieve application-controlled data from the client's resumption ticket and accept or reject Early Data based on that information.”*

So let’s initially focus on raw QUIC

Client needs to save:

- QUIC Source Address Token
- Some QUIC Transport Params (RFC9000 7.4.1)
- TLS resumption and 0-RTT credentials
- Any MoQ SETUP parameters that can’t change
  - AUTHORITY
  - PATH (?)
  - MAX_REQUEST_ID
  - MAX_AUTH_TOKEN_CACHE_SIZE - If we want to use that during SETUP

HTTP/3 with WebTransport (1-RTT)

Client needs to save:

- QUIC Source Address Token
- Some QUIC Transport Params (RFC9000 7.4.1)
- TLS resumption and 0-RTT credentials
- Any MoQ SETUP parameters that can't change
  - ~~**AUTHORITY**~~
  - ~~**PATH (?)**~~
  - MAX_REQUEST_ID
  - MAX_AUTH_TOKEN_CACHE_SIZE - If we want to use that during SETUP
- **HTTP/3 (QPACK SETTINGS)**