

Measuring Trends in Server Support for Post-Quantum TLS

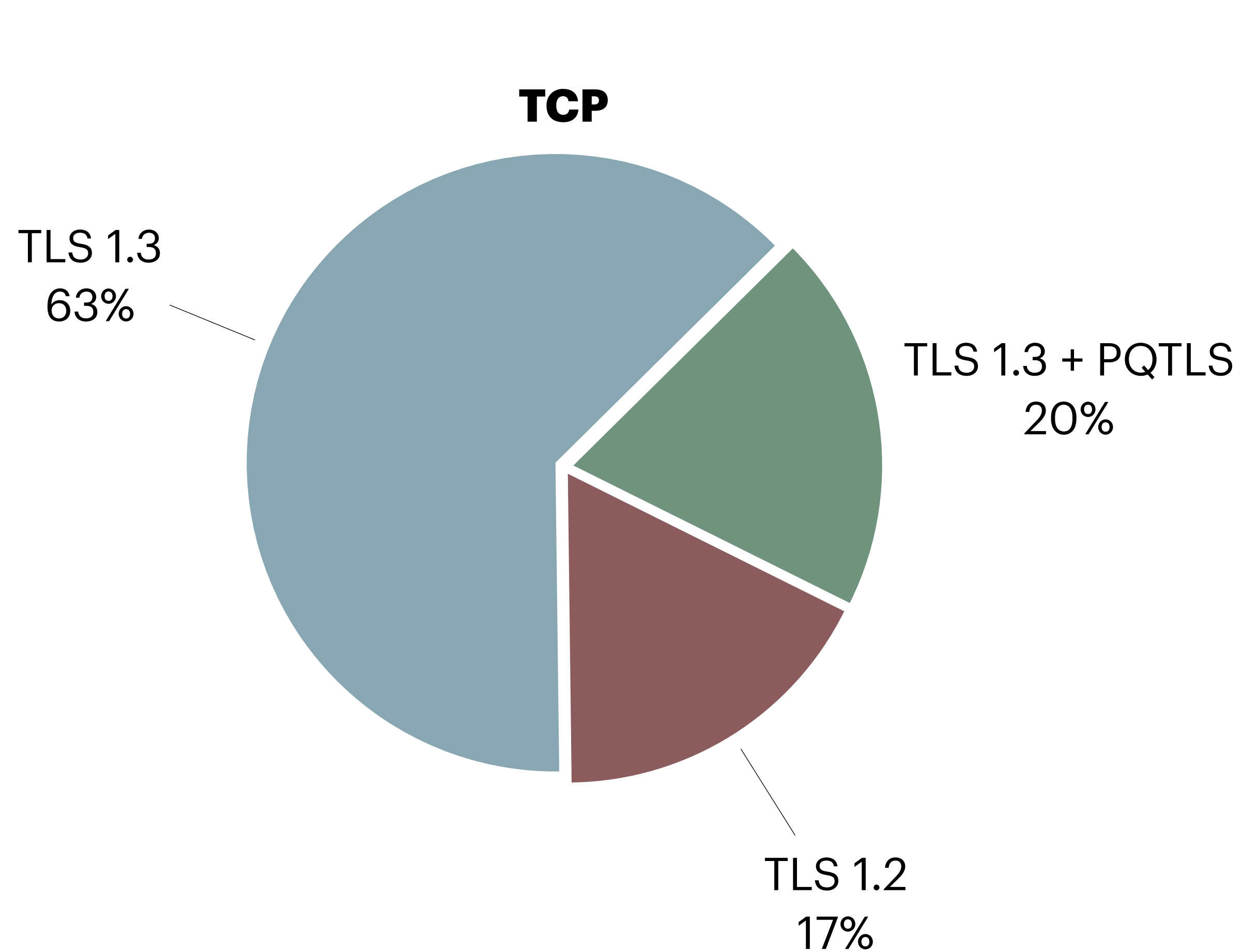
A view from client measurements

Context

- In previous MAPRG sessions, we've looked at server protocol adoption as seen by client connection establishment rates (using Happy Eyeballs, etc)
 - IPv6 / IPv4 support
 - TLS 1.3 support
 - HTTP/2 support
- Today will be an updated look, correlating the support for Post-Quantum key exchange in TLS with support for QUIC and support for IPv6
 - Specifically PQTLS is about supporting "X25519MLKEM768" for key exchange; this requires TLS 1.3 support

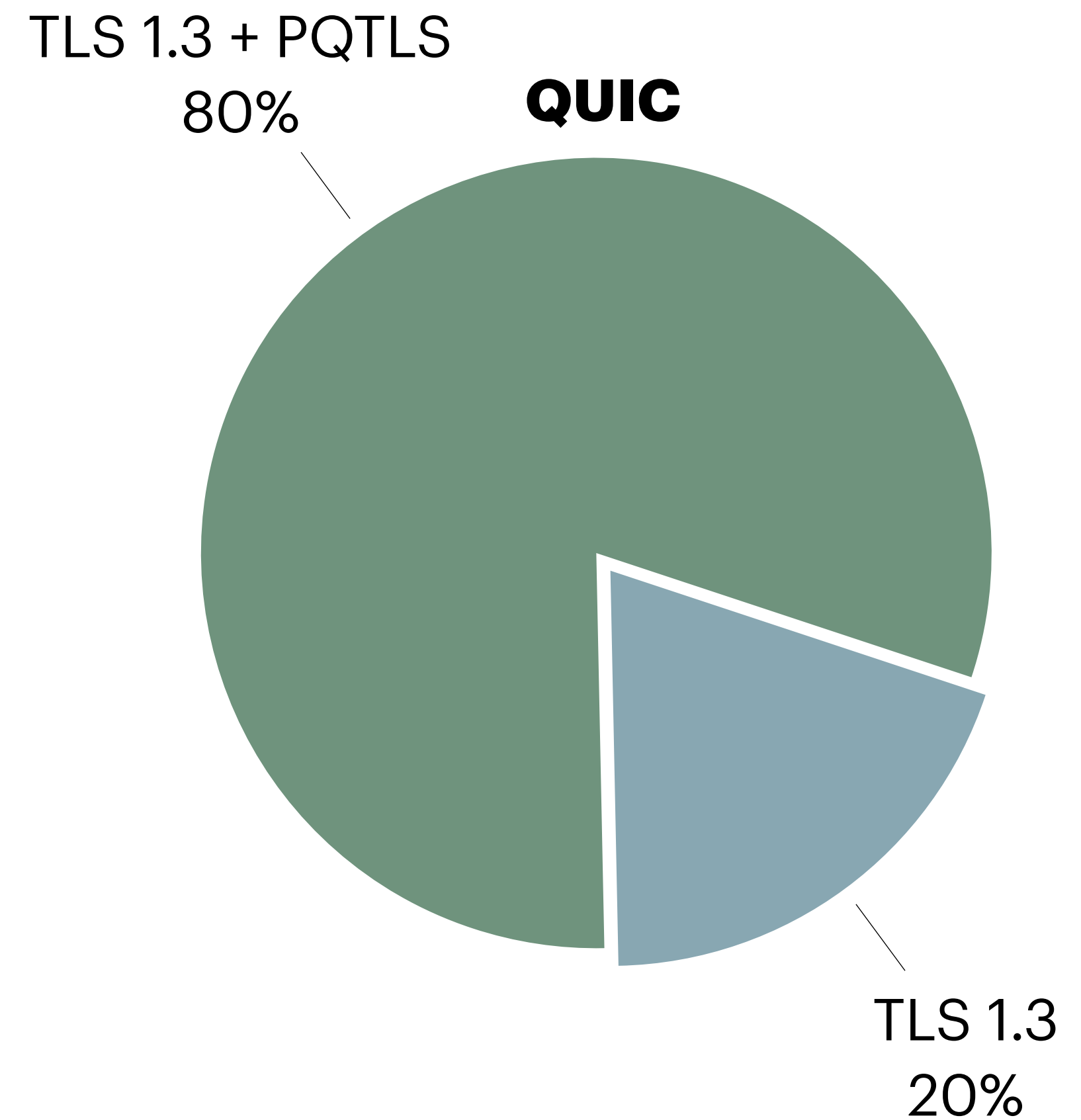
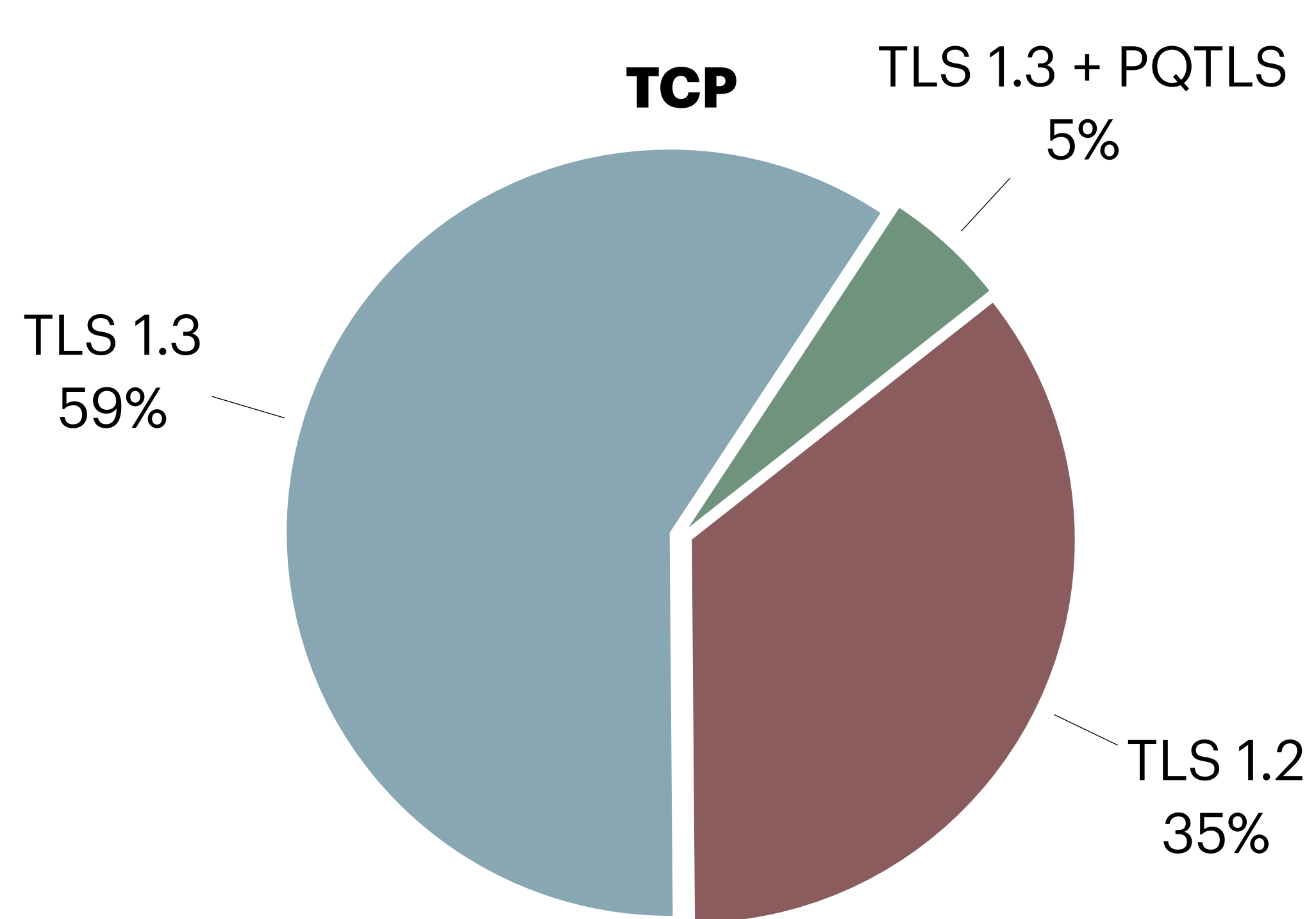
Correlation to QUIC support

Per-connection measurements, **browser** clients



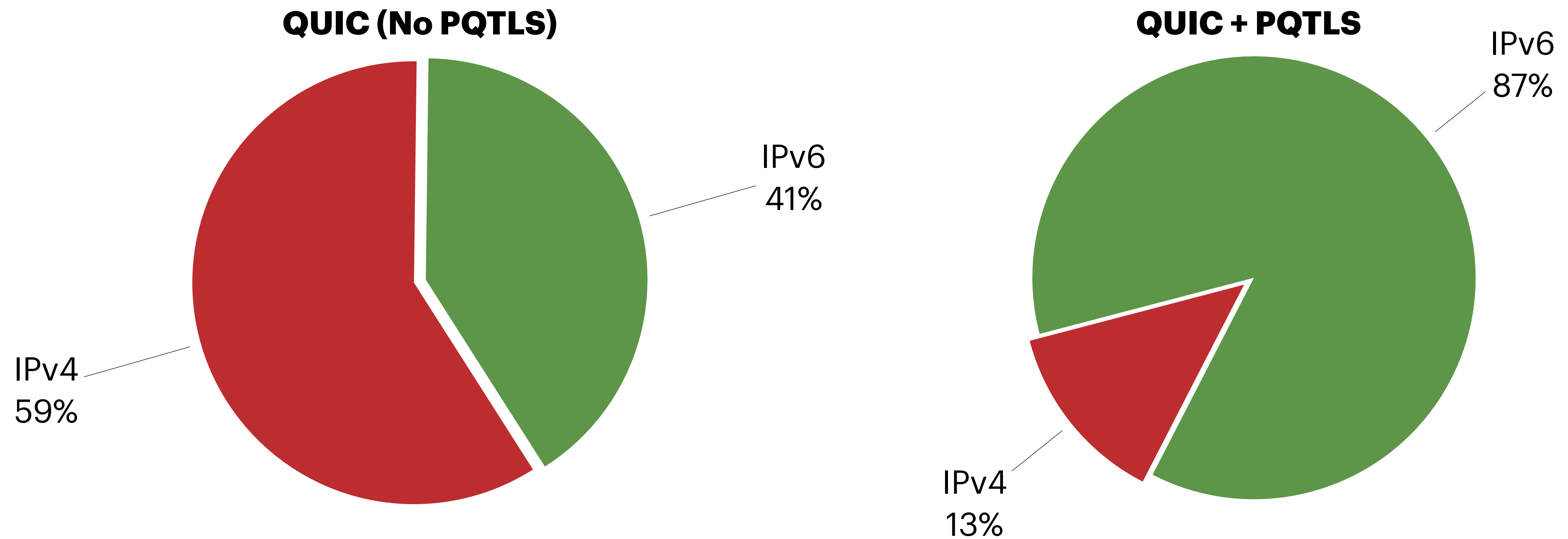
Correlation to QUIC support

Per-connection measurements, **non-browser** clients



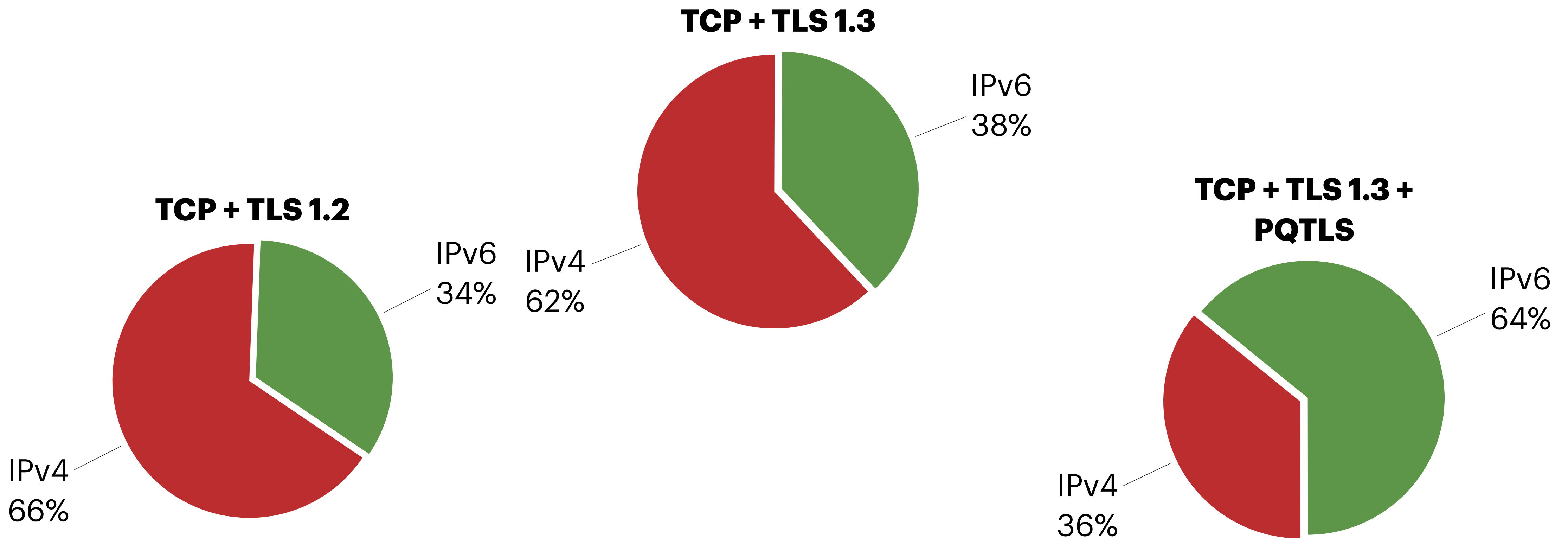
Correlation to IPv6 support

Per-connection **QUIC** measurements, **browser** clients on **dual-stack** networks



Correlation to IPv6 support

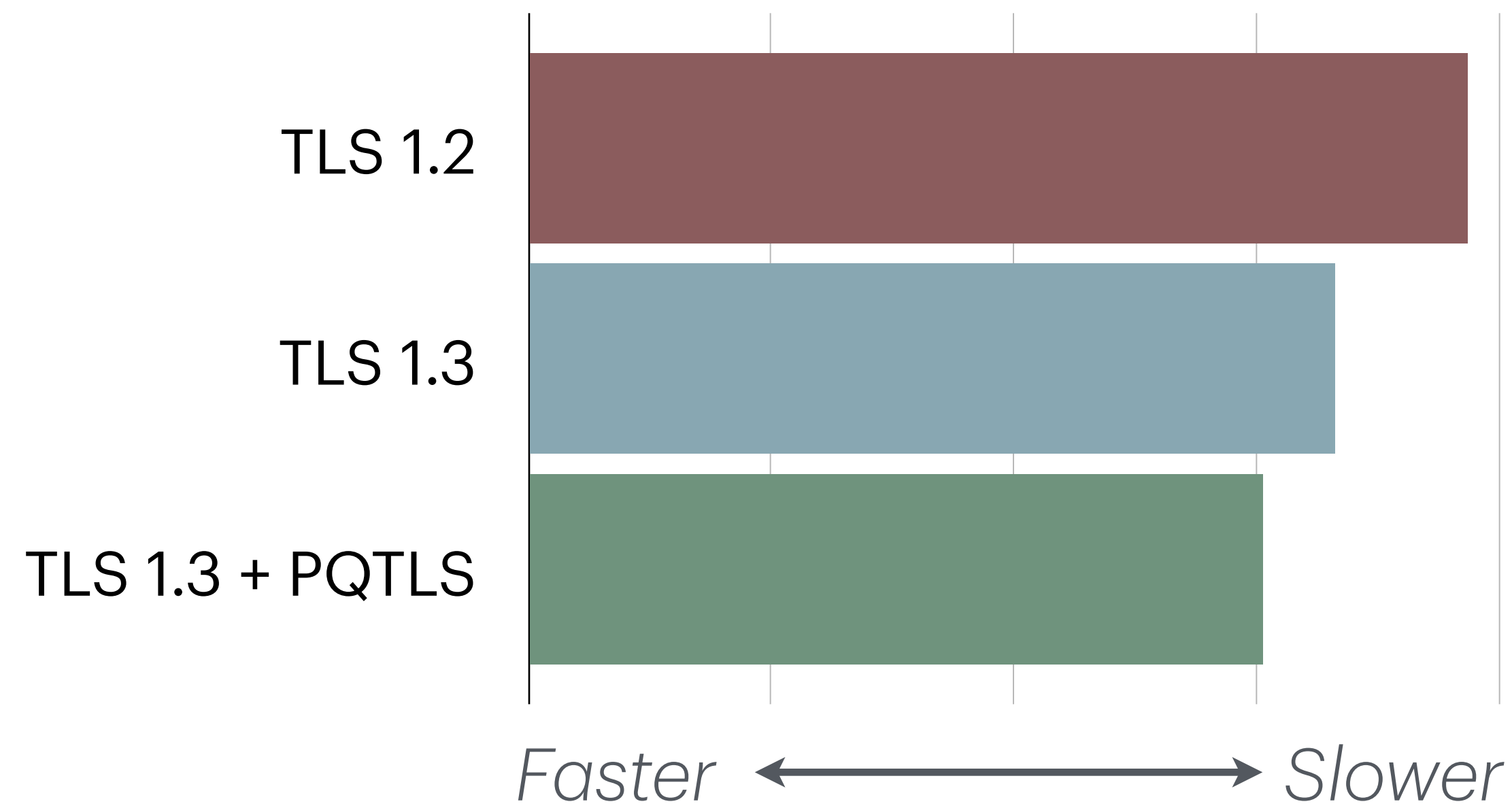
Per-connection **TCP** measurements, **browser** clients on **dual-stack** networks



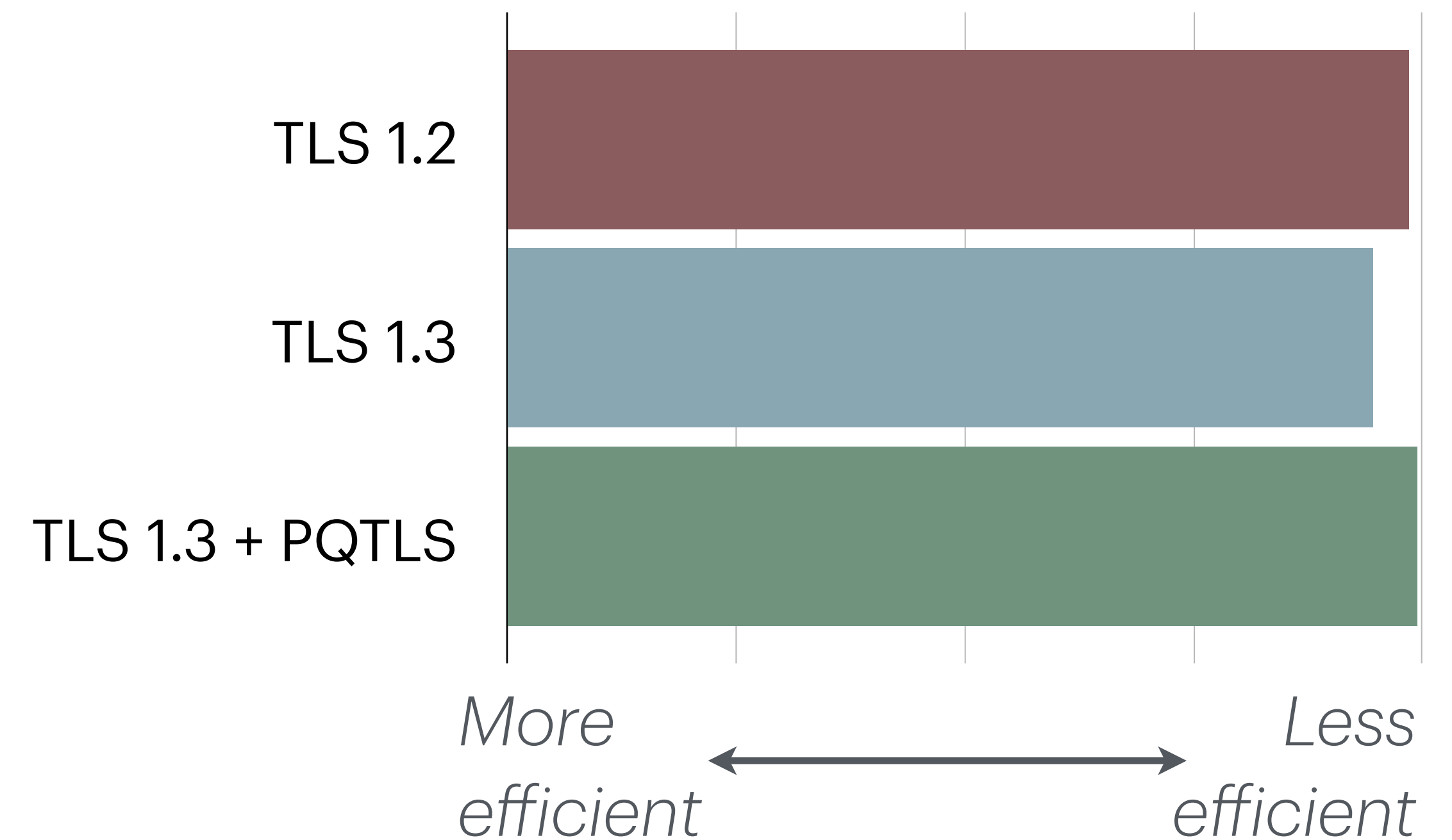
Impact on setup time

Per-connection measurements, TCP browser clients

P90 connection setup time



P90 (setup time / RTT)



Takeaways

- Support for Post-Quantum key exchange is significant for commonly accessed servers
 - Strong correlation between supporting QUIC (HTTP/3) and supporting PQTLS
 - Strong correlation between supporting IPv6 and supporting PQTLS
 - Strongest correlation is supporting QUIC+IPv6 and supporting PQTLS
- Performance impact of PQTLS on connection setup time is less impactful than other factors that optimize connections to servers
 - P90 is less efficient for the same RTT, but most PQTLS servers have lower RTTs to clients

Questions?