



Advantages to Using TLS 1.3

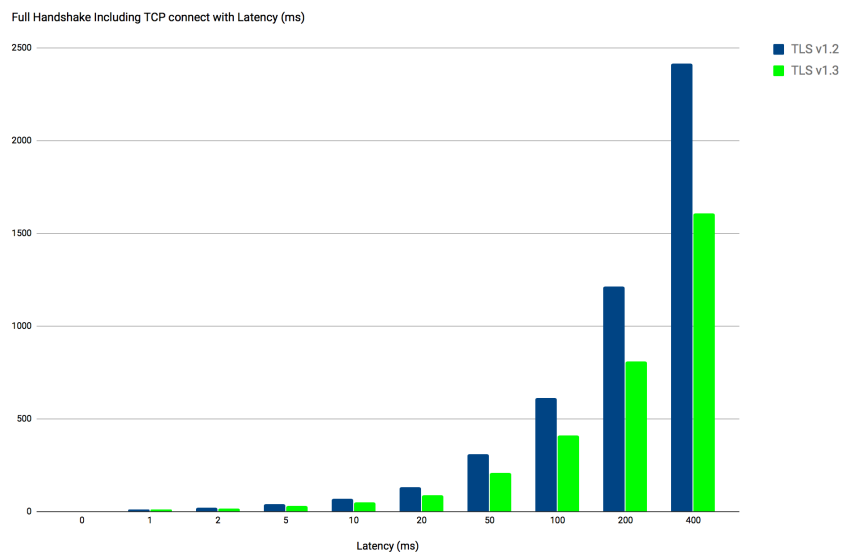
Faster, more secure connections with reduced latency

wolfSSL supports **TLS 1.3** (Drafts 18 and 20) on both client and server side. There are many benefits in changing to the newest version of the TLS specification, including:

- **Quicker connection times** (reduced round-trips during the handshake)
- **Reduced latency**
- **Improved session resumption**
- **More secure crypto by default**

Reduced Round Trips and Latency

One significant difference you will notice is the reduced number of round-trips when performing a full handshake. Older versions of the TLS protocol require two complete round-trips before the client sends the application data. With TLS v1.3 only 1 round-trip is required! Additionally, the server can send application data in response to the client's first handshake message! This means network latency has less impact on the time required to establish a secure connection. The wolfSSL handshake benchmark to the right shows establishing a connection with various latencies to make sure wolfSSL is taking advantage of the reduced latency in TLS 1.3.



Improved Session Resumption

TLS v1.3 has made significant improvements by re-purposing the ticketing system tacked onto older versions of TLS, for session resumption. The server sends the client a new session ticket after the handshake is complete. This ticket, a blob of data to the client, can be a database lookup key like the old session ID. Alternatively, it can be a self-encrypted and self-authenticated value that contains the data for the previous connection. This means the server can be stateless!

Enhanced Security

The specification has been evaluated by cryptographic experts in efforts to prove the security of the protocol. While no security proof is perfect, the previous attacks on renegotiation, protocol version downgrading, compression, CBC and padding have been mitigated and the protocol is generally more resistant to attack.

Learn More

For more information on wolfSSL TLS 1.3 features or to evaluate it, please contact us at info@wolfssl.com. Please send any comments or feedback on wolfSSL's TLS 1.3 support to support@wolfssl.com. Thanks!

www.wolfssl.com

Copyright © 2017 wolfSSL Inc. All Rights Reserved