**Name:** Coral S. Schmidt Montilla  **ID:** 148830

**Objective:**

Upon completion of this activity, youRecognize differences between transport level security protocols and protocols in other TCP/IP layers.

**Student Instructions:**

Based on the reading and the article at [SSL vs TLS - What's the Difference?](https://www.globalsign.com/en/blog/ssl-vs-tls-difference). Please, discuss which model is better and for what in a discussion group.

When discussing secure online communication, SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are often mentioned together—but they are not the same. SSL was the original encryption protocol used to secure connections, but it is now outdated, vulnerable, and officially deprecated. TLS is its modern successor and has seen several upgrades, with the latest version being TLS 1.3. While “SSL certificate” remains common industry jargon, what’s actually securing data today is TLS. Understanding the difference is essential for setting up secure servers and ensuring encrypted web traffic is properly protected.

TLS offers significant improvements over SSL, particularly in how it handles the handshake process. SSL required multiple roundtrips to establish a session, which introduced latency and opened the door to downgrade attacks. TLS 1.2 addressed some of these issues, and TLS 1.3 refined the process further—reducing the handshake to a single roundtrip and introducing zero roundtrip resumption (0-RTT) for returning connections. It also eliminated outdated cryptographic algorithms, reduced the number of cipher suites, and implemented forward secrecy by default. These enhancements make TLS not only faster but significantly more secure.

In short, TLS is the superior protocol in both performance and security. SSL should be disabled wherever it’s still in use, and systems should be updated to support at least TLS 1.2, ideally TLS 1.3. Even though legacy terminology like “SSL certificate” persists, it’s the protocol behind the scenes that truly matters—if it isn’t TLS, it’s time to upgrade.