**LS (Transport Layer Security) is a protocol used for secure communication over the internet. TLS 1.2 has been widely used for many years, but it has some limitations and weaknesses. TLS 1.3 is the latest version of the protocol, which was released in August 2018, and it has several improvements and enhancements over TLS 1.2.**

The technical details of TLS 1.3 and its differences from TLS 1.2 are as follows:

Handshake process: The handshake process in TLS 1.3 has been redesigned to be faster and more secure. It reduces the number of round trips required to establish a connection and eliminates several vulnerabilities that existed in TLS 1.2. In TLS 1.3, the client sends the initial message with its encryption preferences and a session ticket if it has one. The server responds with its own encryption preferences, a digital certificate, and a key exchange message. The client and server then exchange additional messages to verify the authenticity of the certificate, exchange keys, and establish a secure connection.

Cipher suites: TLS 1.3 has removed support for several older and less secure cipher suites that were present in TLS 1.2. It only supports the most secure cipher suites that provide perfect forward secrecy, which means that even if the private key is compromised, past communications are still protected.

Encryption: TLS 1.3 uses stronger encryption algorithms for data in transit. It uses AEAD (Authenticated Encryption with Associated Data) ciphers such as AES-GCM and ChaCha20-Poly1305, which provide both confidentiality and integrity protection for the data being transmitted.

Key exchange: TLS 1.3 introduces new key exchange mechanisms that provide better security and performance. It uses Elliptic Curve Diffie-Hellman (ECDHE) for key exchange by default, which provides forward secrecy and is less vulnerable to attacks than the RSA key exchange used in TLS 1.2.

0-RTT mode: TLS 1.3 introduces a new 0-RTT (zero round-trip time) mode, which allows clients to resume a previous session without any round-trips to the server. This can improve the performance of web applications, but it also introduces some security risks and should be used with caution.

Certificate authentication: TLS 1.3 has improved the authentication process for digital certificates. It requires that servers provide a digital signature for the CertificateVerify message to prove their identity, and it also provides better protection against impersonation attacks.

Privacy: TLS 1.3 has improved privacy protections by reducing the amount of information that is exchanged during the handshake process. It hides the server's RSA or DSA key, and it also hides the length of the pre-master secret, making it harder for attackers to launch attacks against the handshake process.

The advantages of using TLS 1.3 over TLS 1.2 are:

Better security: TLS 1.3 eliminates several known vulnerabilities and weaknesses in TLS 1.2, making it more secure against attacks such as protocol downgrade attacks, padding oracle attacks, and timing attacks.

Faster performance: TLS 1.3 reduces the number of round-trips required to establish a connection, and it also eliminates unnecessary processing and handshake messages, making it faster and more efficient than TLS 1.2.

Improved privacy: TLS 1.3 provides better privacy protections by reducing the amount of information exchanged during the handshake process and by hiding sensitive information such as the server's RSA or DSA key.

Stronger encryption: TLS 1.3 uses stronger encryption algorithms and cipher suites, providing better protection for data in transit.

Reference:  
<https://www.a10networks.com/glossary/key-differences-between-tls-1-2-and-tls-1-3/>