**CSE 471 – Assignment 1**

1. **A)** SPDY is application-level protocol for transporting web content which aims to reduce latency (up to 64%)of page loads. SPDY has true request pipelining without FIFO restrictions. SPDY allows for unlimited concurrent streams over a single TCP connection. Unlike HTTP, each request in SPDY is assigned a **"stream ID"**, which allows us to use a single TCP channel.

**B)** Chrome, Firefox (from v11.0), Opera (since v12.10), Internet Explorer 11(since v3), Amazon’s Silk Browser for the Kindle Fire, Safari 8.

**C)** Since **SPDY** does not actually replace HTTP and it modifies the way HTTP requests and responses are sent, the server can be easily applied to side applications, providing ease of use and a fast client-server connection.

1. As opposed to HTTP/1.1, which keeps all requests and responses in plain text format, HTTP/2 uses the binary framing layer to encapsulate all messages in binary format. HTTP/2 can use a single TCP connection to send multiple streams of data at once so no resource blocks any other but HTTP/1.1 loads resource in and order so there is resource blocking while loading. Another difference is compressing HTTP messages to make them smaller this means faster loading. Finally, push content before client ask for it.
2. All performance enhancements of HTTP/2 is the new binary framing layer, which dictates how the HTTP messages are encapsulated and transferred between the client and server. In HTTP/2, the binary framing layer encodes requests/responses and cuts them up into smaller packets of information, greatly increasing the flexibility of data transfer. It allows the protocol to having faster connection.
3. Multiplexing supports multiple HTTP requests and responses asynchronously via a single TCP connection. It allows faster loading times on resources which means if one response is taking too long then other’s don’t have to wait for it to finish. The client receives the frames and arranges them according to their stream id.
4. Server push allows specifying resources in the HTTP header of the webpages, so the browsers know about those specified resources before needing to go through the webpages and their files to be able to find those resources. This allows browsers to start downloading those resources early because they wouldn't need to wait until discovering those resources to make requests for downloading necessary files.
5. **A)** QUIC (Quick UDP Internet Connections) is a new generation Internet protocol that speeds online web applications that are susceptible to delay, such as searching, video streaming etc., by reducing the round-trip time (RTT) needed to connect to a server. It replaces TCP with UDP and encrypts most of the data to transfer.

**B)** QUIC an advantage over TCP is that the connection setup is much faster. It uses **64-bit connection detection**and various streams to transport data within a connection. Therefore, a QUIC connection is not necessarily bound to a specific port, an IP address or a specific endpoint. QUIC packages are always authenticated and **largely encrypted** (including payload). The parts of the header that are not in encrypted form are protected from injection and tampering by **authentication on the receiver’s end.**

1. 0-RTT doesn’t have to wait for two handshakes (TCP then TLS) to complete a secure network connection. Connection setup takes fewer packets to complete than TCP + TLS and can be resilient after close. This means you start getting data faster the first time you connect to a service, and potentially faster the second time.
2. In standard HTTP+TLS+TCP, TCP needs a handshake to establish a session between server and client, and TLS needs its own handshake to ensure that the session is secured. QUIC only needs a single handshake to establish a secure session. In QUIC every packet has a new sequence number, including retransmission packets, which enables for a more accurate round-trip-time (RTT) calculation. QUIC does significantly decrease HOL blocking with using multiplexing. QUIC brings its own unique identifier for a connection, the Connection UUID, which makes it possible to migrate networks and keep the same Connection UUID.
3. The FLoC clusters individuals with similar browsing patterns into large groups or cohorts and assigns unique cohort IDs. Unlike in third-party cookies that reveal information about each individual, in the FLoC model, the only information revealed to third parties is this cohort ID.