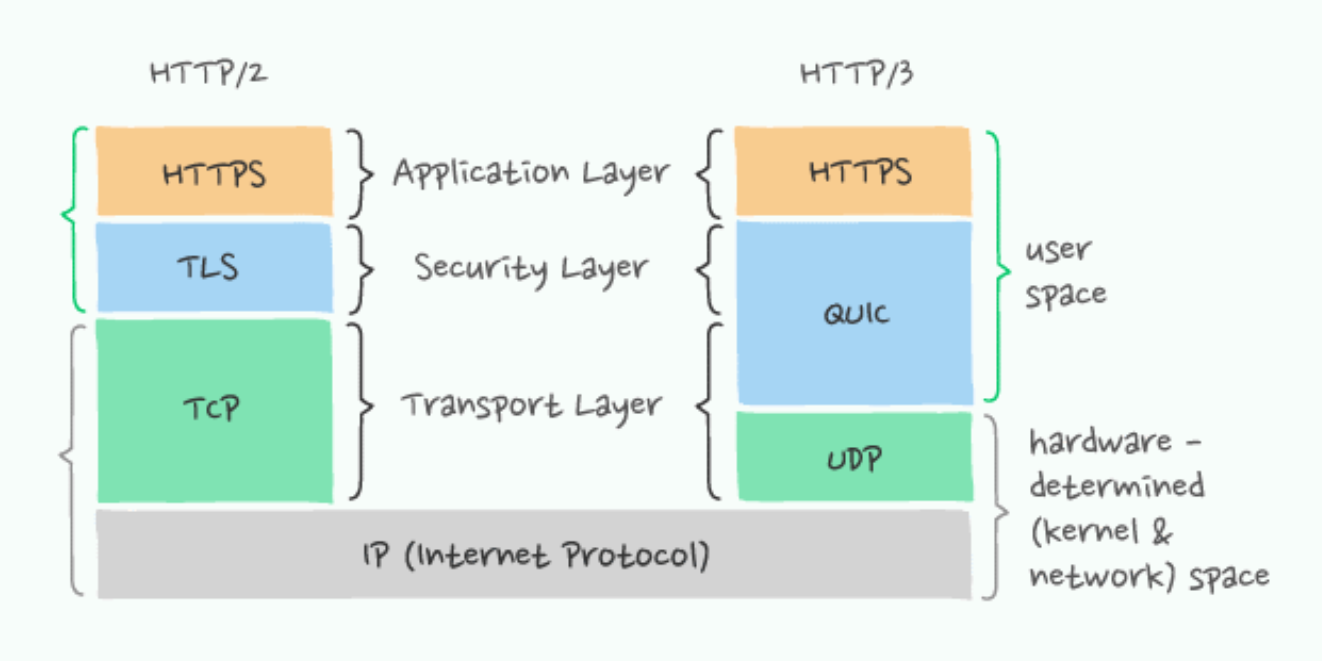
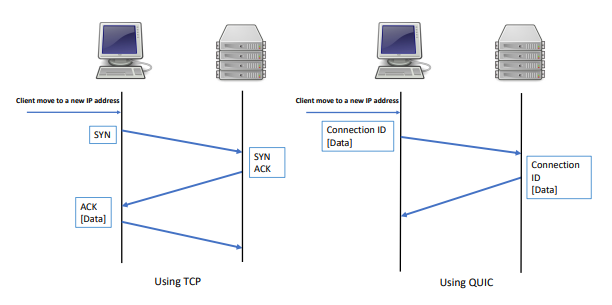
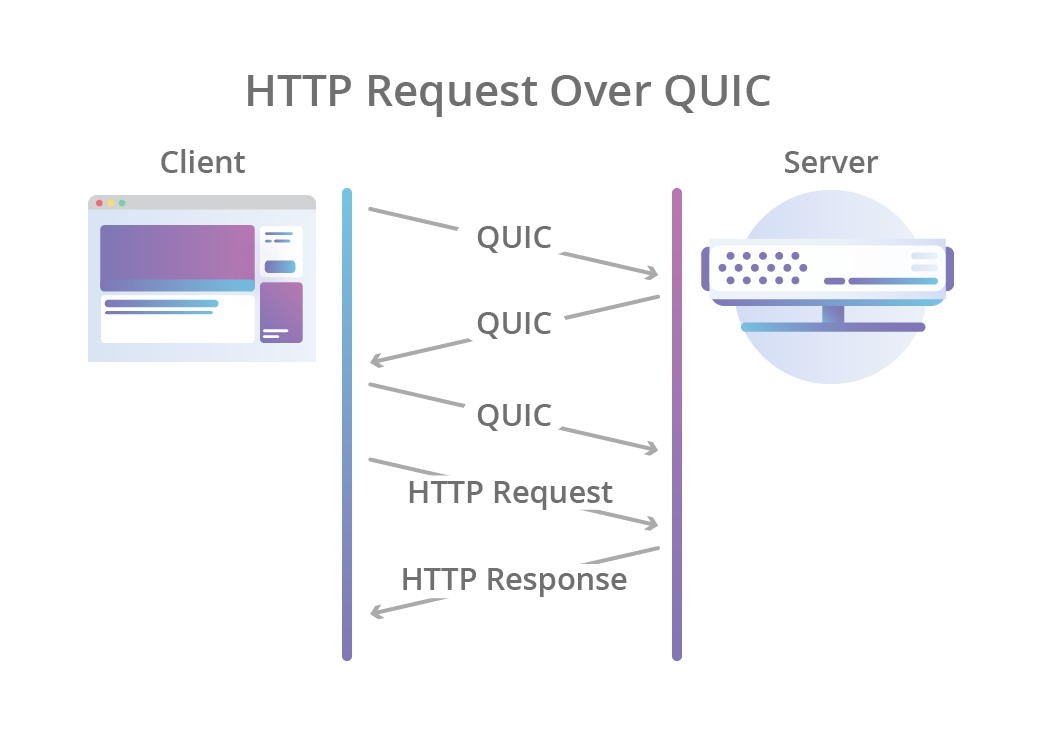
**HTTP3**

HTTP3 is the newest one in the among the protocols and it is meant to replace its predecessors. HTTP3 is a new standard process in the development that will change how web browsers and web servers interacts. It provides a major user experience improvement as it promises to be faster, more reliable and more secure. While still being developed it was already supported by the all major browsers.

One of the main difference in HTTP3 is that it runs on a new transport protocol: **QUIC**, which is a new internet transport protocol initially developed by Google among other things introduced streams at the transport layer.



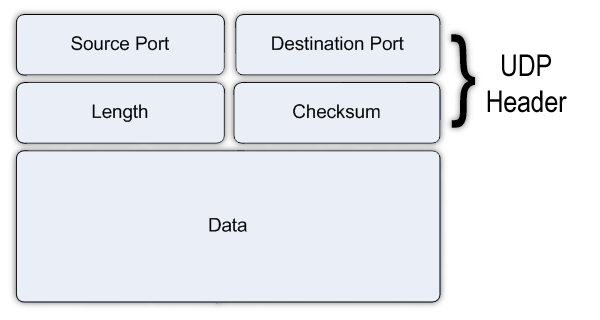
Quick streams are delivered independently such that in most cases packet loss affecting one stream does not affect others. This is because QUIC packets are encapsulated on the top of **UDP** (User Datagram Protocol).

**Key features of QUIC and HTTP/3 vs TCP+TLS and HTTP/2:**

* Reduced connection establishment time - 0 round trips in the common case
* Improved congestion control feedback
* Multiplexing without head of line blocking
* Connection migration
* Transport extensibility
* Optional unreliable delivery

*Reference:* *https://www.chromium.org/quic/*

UDP itself is a connectionless protocol and therefore technically unreliable that means that the packets can get lost. However, QUIC identify the lost data and then re- transfer the missing bytes to ensure seamless user experience.



UDP assures network traffic in the form of datagrams, as implied by its name. One message unit is included in a datagram. The first eight bytes of the datagram are taken up by the header information, while the remaining bytes are made up of the message data. Each of the four fields in a UDP datagram header takes up two bytes.

Source port number: This field indicates the sender's port, which is considered to be the port to which any necessary answers may be sent. It is 0 if it is not utilized.

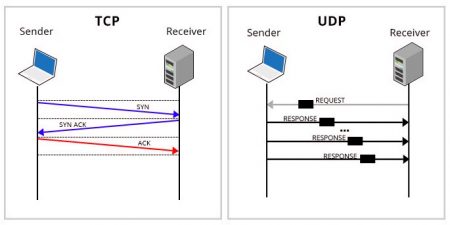
Destination port number: This field identifies the port of the receiver

Datagram size/Length: This field defines the entire datagram length including the header and data. The minimum length is 8 bytes as it is the length of the header.

Checksum: The data and header are checked for mistakes using the checksum field.

UDP ports: UDP programs use datagram sockets to create host-to-host connections. These sockets are in charge of establishing connections between UDP applications and the service ports that act as data transmission endpoints. Port numbers are used to identify ports.

How Does UDP work?

UDP uses IP to transfer a datagram from one computer to another. It collects data in a UDP packet and adds its own header data to the packet to carry the data. This data consists of the source and destination ports for communication, the packet length and a checksum. UDP packets are despatched to their destinations after being enclosed in an IP packet.

UDP, unlike TCP, does not ensure that the packets reach their intended recipients. As opposed to TCP, UDP does not establish a direct connection with the receiving machine. Instead, it sends the information out and depends on the intermediary hardware to deliver it to the intended recipient computers.

The majority of programs wait for any responses they anticipate getting in response to UDP packets. An application either transmits the packet again or gives up if it doesn't get a response within a predetermined amount of time.

Although there is no assurance that the data being transmitted will arrive at its intended location, this transmission technique does offer a minimal overhead and is frequently used for services that don't have to function perfectly the first time.

Also since quick uses UDP there is no need to complete a complex three-way handshake to initiate the first connection. The includes: Initiating, encrypting and the exchange of keys into the initial handshake process. It takes only one round trip to establish a path for communication instead of multiple round trips just to establish a connection. Moreover, encryption and authentication are provided by default.