Michael Cabana
27527489

TA2: Transport Layer

Q1: UDP is a connectionless protocol. This means there is no delay when trying to establish a connection. No handshaking between sender and receiver allows for faster transfer of data. UDP also does not have congestion control which allows it to “blast” away as fast as desired. This is important in things like online gaming and video streaming where losing one packet will not effect the experience. In this case, speed is what is important.

Q2: Two segments with identical destination ports and IP addresses might be delivered to two different sockets because of how the transport layer distinguishes these segments. Since segments consist of a 4 tuple identifier, their source IP and port are used to distinguish these segments. This situation can not happen with UDP sockets because UDP segments are identified with a 2-tuple of destination port and IP.

Q3: UDP headers impose a theoretical limit on the size of the data that can be carried in a UDP segment because headers include a 16-bit length field. This field specifies the length in bytes of the entire datagram. The theoretical limit then is (2^16 - 1) - 8 = 65,527 bytes. This problem might be addressed by using IPv6 as the underlying IP protocol which allows you to specify a larger size for the segment.

Q4: What comes to mind is that since UDP is connectionless, if UDP segments are being delivered at a constant, this would leave no room for TCP to attempt a connection and delivery. A client host would have to periodically check for incoming TCP connections at a suitable rate to not be detrimental to whatever the UDP based experience is.

Q5:

Q6: TCP header padding is used to ensure that the TCP header ends and data begins on a 32-bit boundary and is composed of zeros.

Q7: Flow control is when the rate at which the sender is sending is matched against the rate at which the receiving application is reading. It does this by having the sender maintain a variable called the recipe window to help give the sender an idea of how much free buffer space is available. Congestion control is the throttling of the TCP sender due to congestion in the network. TCP does this by limiting send rate as a function of perceived network congestion.

Q8: EstimatedRTT = (1 - a) * EstimatedRTT + a * SampleRTT

SampleRTT	**EstimatedRTT**
a = 0.125	30
26	29.5
32	29.8125
24	29.0859375

Q9: In TCP Reno, the new window size will be 13kb : cwnd = 18/2 = 9 + 4(linear growth) = 13
In TCP Tahoe, the new window size will be cwnd = 1 + 1 + 2 + 4 (exp growth) + 1(linear) = 9

Q10: SYN flooding can be used as a DDoS attack on a server when the client does not respond to the server with the expected ACK response during a 3-way handshake. Half-open connections bind resources from the server and can eventually take up all available resources on the server barring other clients form connecting. There are many countermeasures to such an attack. These being Filtering, increasing backlog, reduce the sya-recived timer, recycle old half-open connections, SYN cache, SYN cookies, Hybrid approaches such as the combination of the previous 2, as well as firewalls and proxies (rfc 4987).