Homework #3	CS 372	Rhea Mae Edwards

R5) Since the some loss with voice and video traffic is okay with same-time streaming, voice and video traffic is often sent over TCP rather than UDP in today's Internet, because also since most firewalls are programmed to block UDP traffic, by using TCP for video and voice traffic, such traffic will be let through the presented firewall(s) with not much worries of the voice and video traffic being blocked by a firewall.

R6) Yes, it is possible for an application to enjoy reliable data transfer even when the application runs over UDP where the developer can add reliability at the application layer.

R10) We needed to introduce timers in our rdt protocols, because packet would get loss that the client would not receive which in turn will not notify anything was sent but was actually sent, so the sender would be waiting for an expecting acknowlegment message but would not receive one because the client didn't receive a packet that was initially loss. So having a timer would "realize" this issue and possibly a very long time/endless time of waiting for that acknowledgement message, and the sender will have that "realization" of needing to resend that packet to the client because they didn't receive it, after a decent/pre-determined amount of time.

P15) Cross-Country Example, Figure 3.17

Channel Utilization $> 98\%$

$L = 1500$ bytes $= 12000$ bits

$RTT \approx 30\,ms \approx 0.030\,s$

$R = 1\,Gbps = 10^9\,bps$

Window Size = ?

$$U_{sender} = \frac{L/R}{RTT + L/R}$$

$$d_{trans} = \frac{L}{R}$$

$$d_{trans} = \frac{12000}{10^9} = 1.2 \times 10^{-5}\,s$$

$$0.98 = \frac{(1.2\times10^{-5})N}{0.03 + (1.2\times10^{-5})} \longrightarrow N = 2450.98$$

The window size would have to be about $\boxed{\text{2451 packets}}$ big.

P24) a) False, because the sender will only send packets within its and only move on with its window when the earliest packet in its window have been acknowlegde. Those ACK messages are the only way the sender's window would progress.

b) False, because the receiver will only send ACK messages for the next packet that it is expecting until it gets it no matter which packet is sent to it.

c) False, because the sender will only send ACK messages for the expected packet its waiting for, and not send any other packet ACK message.

d) True, because it will wait and only send ACK messages for the packet it is expecting.

Homework #3	CS 372	Rhea Mae Edwards

P26) L Bytes
MSS = 536 Bytes   Host A → Host B

a) L = ? So TCP sequence #'s not exhausted
TCP Sequence Number Field = 4 Bytes

4 Bytes = 32 bits
Maximum Value L = $\boxed{2^{32} \text{ bits}}$ so TCP sequence numbers not exhausted.

b) d_{trans} = ?
66 Bytes added before packet sent over 155 Mbps link
→ Transport, Network, and Data-Link Header
Ignore Flow Control and Congestion Control
→ Allow A continuous back to back sent segments

536 - 66 = 470 Bytes left of data to use

$2^{32}(0.125)$ = 536,870,912 Bytes

536870912 / 470 = 1,142,279 packets

1142279 (536) = 6.12×10^8 Bytes

6.12×10^8 Bytes = 4.9×10^9 bits = 4898 Mbits

4898 / 155 = 31.6 seconds

It will take $\boxed{31.6 \text{ seconds}}$ to transmit the file.

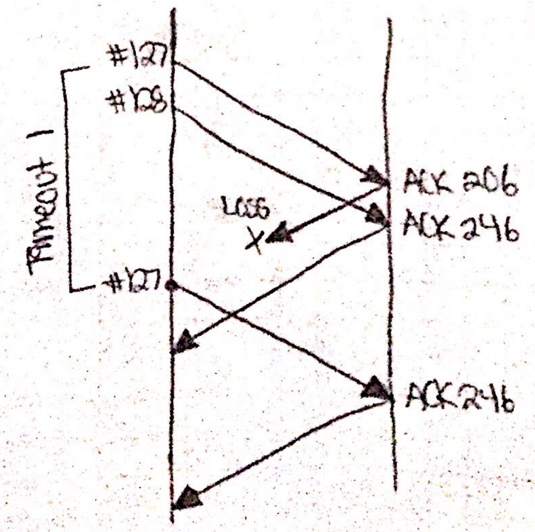
P27) Host A → Host B
Up to 126 Bytes have already been received
Segment 1 = 80 Bytes , Sequence # 127 , Source Port # 302
Segment 2 = 40 Bytes   Destination Port # 80
ACK sent whenever segment received

a) Sequence # 128
Source Port # 302
Destination Port # 80

b) Acknowledgment # 206
Source Port # 80
Destination Port # 302

c) Acknowledgment # 162

d) Host A   Host B



Homework # 3	CS 372	Rhea Mae Edwards

P40) Consider 3.58, Assuming Usage of TCP Reno Behavior

a.) Time Intervals when TCP Slow Start is Operating:
- 1 second to 6 seconds
- 23 seconds to 26 seconds / beyond

b.) Time Intervals when TCP Congestion Avoidance is Operating:
- 6 seconds to 16 seconds
- 17 seconds to 22 seconds

c.) Since the graph shows it didn't drop to zero, it dropped to about half the window size, it couldn't have been by a timeout, after the 16th transmission round, segment loss must have been detected by a triple duplicate ACK.

d.) Since the graph dropped all the way to the window size valued at zero, after the 22nd transmission round, segment loss must have been detected by a timeout.

e.) Initial Value of ssthresh at the First Transmission Round = 32 segments

f.) Value of ssthresh at the 18th Transmission Round = 21 segments (Half of 42 segments)

g.) Value of ssthresh at the 24th Transmission Round = 15 segments (Half of 29 segments)

h.) 70th Segment is Sent at the 7th Transmission Round
↳ Based of the initial expotential growth represented by the graph

i.) Packet loss detected after 26th Round by a Triple Duplicate ACK:
the Congestion Window Size = 8 segments
ssthresh = 4 segments (Half of 8 segments)

j.) Suppose TCP Tahoe is Used
Triple Duplicate ACKs at 16th Round
At the 19th Round:
Congestion Window Size = 0 segments
ssthresh = 21 segments (Half of 42 segments)

- TCP Tahoe always sets congestion window size to 1 seg

k.) Suppose TCP Tahoe is Used
Timeout Event at 22nd Round
Number of Packets Sent from 17th Round to 22nd Round = ?
↳ Interval would have experienced a Slow Start State

$1 + 2 + 4 + 8 + 16 + 32 = \boxed{63 \text{ packets}}$

17th 18th 19th 20th 21st 22nd

Homework #3	CS 372	Rhea Mae Edwards

P55) Investigate whether either UDP or TCP provides degree of end-point authentication.

a.) Request and Respond within UDP Packet Server
Client with IP Address X Spoofs with Address Y
Will Server send its Response?

Yes, the server will send its response because it does have the same IP address since it was given a request with the same UDP packet it would respond to of the request.

b.) Server receives SYN with IP Source Address Y
Responds with SYN ACK
Receives ACK with IP Source Address Y with correct acknowledgment #
Assuming server chooses random initial sequence #
No "man-in-the-middle"
Can server be certian client is indeed at Y?

The server can be certian that the client is indeed at Y...
But there is really no way mostly that the server can be 100% certian.
There are always ways to manipolate the facade of the client without being 100% certian of the truth of the client entirely.