CSC 4200/5200 Final,

Dec 9th, 2020, 10PM CST

**Q1 – 20points**  
  
1) True or False: 5 pts

* Transport layer operates between two hosts - False -> Network Layer
* UDP is a reliable packet delivery service – False -> It is unreliable
* TCP provides flow control between applications - True
* TCP provides congestion control in the network - True
* UDP is a connection oriented protocol – False -> Connectionless oriented

2) In the context of the transport layer, what is a flow? 2 pts

3) A three way handshake in TCP is where three packets are exchanged between client and the server. They are SYN from the client, SYN+ACK from the server, and ACK from the client. Why does TCP perform a three-way handshake? 4 pts

This handshake is what starts the connection. The client sends a SYN, short for synchronize and is the first step in establishing a communication between two systems. The server then sends a SYN+ACK back, this is to synchronize the communications between the two systems and ACK to acknowledge that a packet was received. This is so that the client won’t need to send more SYN requests and know that the next packet is ready to be received. The client sends back an ACK to let the server know that it is now ready to receive information from it.

4) In the three-way handshake, TCP clients use a random initial sequence number. What do you think would happen if all sequence numbers started at 0? 4pts

There would be a huge security risk to start. Ports are also reused, and you might end up using someone else’s previous connection.

5) How will TCP perform in the following scenarios? Answer in terms of throughput and retransmission. 5Pts

|  |  |  |
| --- | --- | --- |
| **Scenario** | **Throughput (High/Low)** | **Retransmission (High/Low)** |
| Transmitting a large file | HIGH | LOW |
| Transmitting a large file over a lossy link | HIGH | HIGH |
| Receive buffer is much smaller than the send buffer | LOW | HIGH |
| Transmitting a large file to Mars (assume a lossless channel) | LOW | LOW |
| A small file over a very lossy link | LOW | HIGH |

**Q2: 20 pts**

1) What is Min-Max fair queuing? 2Pts

It is when you take the principles of Min-Max and apply it to Fair Queuing, which maintains a separate queue for each flow. The formula: Assuming *n* clients, capacity *c*, == *c/n for each client*. If client, C1, does not want *c/n*, then divide the excess capacity equally among others   
== *c/n + (c/n – c1)/n-1*

2) If you have to divide 30Mbps available bandwidth between 5 clients, what would the allocation look like using min-max fair queuing? The client requests are: 10Mbps, 10Mbps, 5Mbps, 5Mbps, and 6Mbps. Write the numbers for each step. 5pts

**Step 1 Step2   
 c/n UNUSED == 2MBPS c/n + (c/n – c1)/n-1**

Client 1 - 6 MBPS Client 1 - 7 MBPS

Client 2 - 6 MBPS Client 2 - 7 MBPS

Client 3 - 5 MBPS Client 3 - 5 MBPS

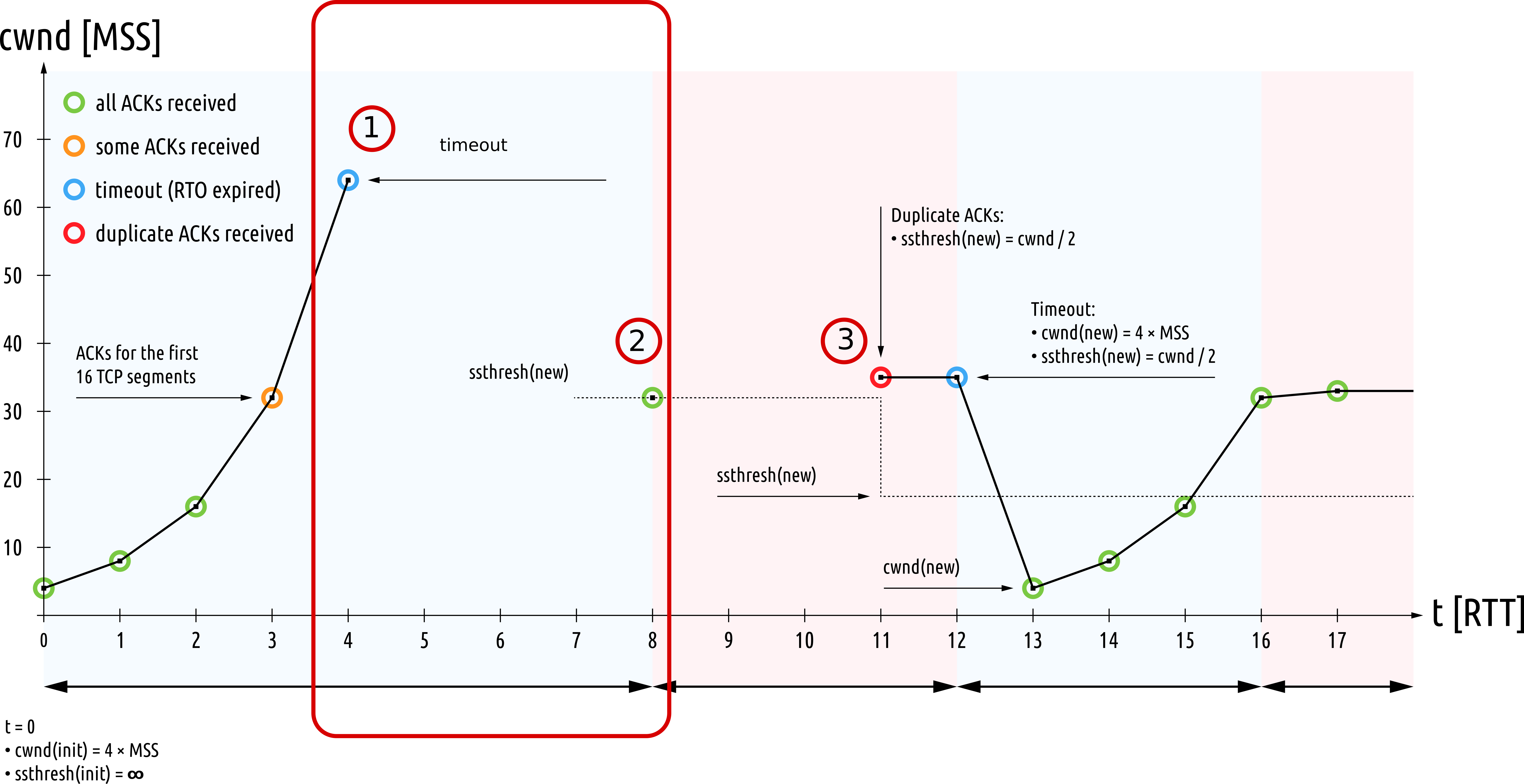
Client 4 - 5 MBPS Client 4 - 5 MBPS

Client 5 - 6 MBPS Client 5 - 6 MBPS

3) In TCP slow start, why don’t we start with a massive window? 3pts

Loss is indicated by timeout; a massive window could exceed the timeout threshold. Hence, we have slow start that will grow exponentially to that threshold then grow linearly. This is so that we can accurately detect loss.

4) Complete the following picture - consider a TCP flow that is using AIMD (additive increase and multiplicative decrease) . Draw lines between 1, 2, and 3 to show what happens during time 4 and 11. **5pts**



5) Calculate the TCP window size where the throughput is 15Mbps, and the RTT is 2ms. Minimum segment size = 1500 Bytes. **5pts**

15mbps = w / (2\*2ms) =

= (15mb/1s) \* (0.004s/1ms) \* (1,000,000b/1mb) =

= 60,000 window size

**Q3 - 20pts**

1) True of false? **5pts**

* Multimedia applications are loss tolerant - True
* File transfer applications are delay tolerant – False -> Not delay tolerant
* Web documents are not time sensitive - True
* Email application can tolerate loss – False -> Not loss tolerant.
* Text messages need high bandwidth – False -> Elastic, can be high or low.

2) What are the different modes for DNS query? 3 pts

Iterative and Recursive

3) If you are running a DNS server for your university, would you allow both DNS query modes? Explain why or why not. 3 Pts

I would only allow iterative DNS. This is due to the high amount of internet traffic now for university websites. Recursive DNS puts a large strain the higher up the hierarchy there is, so to combat that, iterative would be the best way to go.

4) HTTP/3 might abandon TCP and instead use UDP at the transport layer (QUIC).

(a) What aspects of HTTP applications do you think will benefit from this change? 5 pts

You would be able to download more HTTP requests at the same time from the same server. You can have multiple connections open to the same server that would allow more web objects to be sent simultaneously. This also helps with delay in online web applications by reducing RTT.

(b) What would break if you use QUIC? 4pts

Your firewall could possibly break. If a firewall is used to analyzing HTTP traffic then the QUIC protocol could be misunderstood by your firewall.

**Q4: 20 pts**

1) Write two differences between stateful and stateless firewall. 4Pts

Stateless treats each packet in isolation and does not relate to connection state; while stateful firewalls maintain context about active sessions and use “State information” to speed pack processing. Stateless is much faster than stateful. Stateless does not inspect traffic while stateful does.

2) True or False - you can filter packets with an invalid state using access control lists (ACLs). Why or why not? 3pts

True, the ACL can be augmented to indicate need to check connection state.

3) If you had an insecure channel of communication where everything is intercepted, how would you use public key cryptography to secure your communication? 3Pts

Everyone is a conversation can make two keys, a public and personal key. These keys are connected, and if encoded using someone’s personal key, only they will be able to decode it.

4) Draw arrows from left to the right and match the following items. 5 pts

|  |  |
| --- | --- |
| HTTP | Separation of control and data plane |
| SSL | Encrypted communications |
| VPN | Application layer Request/response |
| Software Defined Networking | Secure Socket |
| IPSec | Enchilada authentication |

5) Briefly describe the idea behind Software Defined Networking and how does it help solve Internet ossification (*ossification - a tendency toward or state of being molded into a rigid, conventional, sterile, or unimaginative condition*) ? 5Points

SDN is more like cloud computing; in that, it is more dynamic, agile, and programmatically configured. It is more flexible compared to traditional networks and can sustain higher bandwidth loads. It centralizes network intelligence into one by disassociating the forwarding process of network packets or separating the data plane and control plane. This ability to be uniquely configured can allow for many different paths of networking, making it the opposite of ossification.

## Q5: 20 points

1) What are the four aspects of network security? 4Points

Confidentiality, Authentication, Message integrity, Access and Availability.

2) Since SSL already provides an encrypted socket layer, do we need IPSec? Why or why not? 4 points

The need for IPSec is situational. In most cases, since we have SSL we do not need IPSec, however if the organization requires the use of IPSec for some condition to be met, then we would need IPSec. However, SSL provides better performance, more limited attack defense, and better support, so overall, we do not need IPSec compared to SSL.

3) We can use public key cryptography at the application layer to encrypt data between users. Why do we need SSL/IPSec/VPN at all? 5Points

SSL is used to hide all application data as it traverses the internet, IPSec does not require special knowledge or key exchange and it can route through multiple subnets. VPN can protect AES keys, this way the key can be sent to the client.

4) What is enchilada authentication? 2Points

It is a part of IPSec used to authenticate a packet starting from ESP hdr to EPS trl. It uses 20-Round ChaCha and Rijndael with 14 rounds and 256-bit block size.

5) True or False: 5points

|  |  |
| --- | --- |
| Asymmetric key cryptography is generally faster than symmetric key cryptography: False |  |
| IPSec provides transport layer security: False |  |
| Firewalls are slower than ACLs: False |  |
| Symmetric key cryptography can protect users from eavesdropping: False |  |
| Intrusion detection systems filter packets: False. |  |