Problem 1
(a) Name the five layers of the Internet protocol stack
Application, Transport, Network, Link, Security

(b) List two types of access networks.
Ethernet, Wireless LANs

(c) Associate each of the following concept with either packet switching (PS) or circuit switching (CS):
[6 pts]

Store and forward — **PS**

Dedicated resource allocation — **CS**

Queuing — **PS**

(d) Consider a video streaming server with an upload capacity of 200 Mbps and a download capacity of 100 Mbps. It is serving 50 clients simultaneously by *fairly* multiplexing its upload capacity. Each of the clients streaming from the server has an upload capacity of 2 Mbps and a download capacity of 5 Mbps. The Internet is not congested. What is the maximum bit rate at which this client is receiving service? [4 pts]

Upload capacity per client = 200Mbps/50 clients = 4Mbps per client > 2Mbps
Download capacity per client = 100Mbps/50 clients = 2Mbps per client
2Mbps

Problem 2
(a) How long does it take a packet of length 1,000 bytes to propagate over a link of distance 2,500 km, propagation speed 2.5 · 10^8 m/s, and transmission rate 2 Mbps? [5 pts]

Transmission Delay = Length / Transmission rate = (1000bytes * 8 bits/byte) / (2 Mbps * 1,000,000 bits/Mb) = 4ms
Propagation Delay = link distance / speed of propagation = (2500km * 10^3m/km) / (2.5*10^8m/s) = 10 ms
Total time = Transmission Delay + Propagation Delay = 4ms + 10ms = 14ms

(b) More generally, how long does it take a packet of length L to propagate over a link of distance d, propagation speed s, and transmission rate R bps?
[5 pts]
Time = L/R + d/s

Problem 3

(a) In class, we discussed different ways loss can occur as data is transferred over the network. List and provide a brief explanation of the two types of data loss we discussed. (5 points)
Accidental data loss - data loss because of human errors (e.g. deleted files)
Intentional data loss - data loss because data is accessed, stolen, without authorization (e.g. hacking, phishing)

(b) What is the difference between virus and worm? When a malware is included in an Email attachment, is it a virus or worm? (5 pts)
Virus - self replicating infection by receiving/executing object
Worm - self replicating infection by passively receiving object that gets itself executed
A malware included in an email attachment is considered a virus.

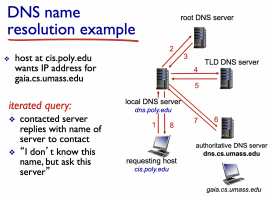
Problem 4

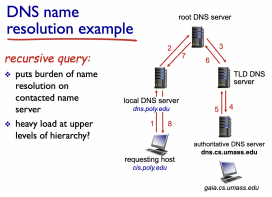
(a) Let the round trip time be T_r and file transfer time be T_f, what is the time to use non-persistent HTTP to get a file? [4 pts]
Time = $2T_r + T_f$

(b) Consider an institution with a 1.5 Mbps incoming channel from the Internet. The average http request rate from all browsers in the institution is 30/second. Each request is for a single object with an average size of 7,000 bytes. Will the incoming channel congested by the http traffic? [6 pts]
Total bandwidth consumed= average request size * request rate = (7000bytes * 8 bits/byte * 30 seconds)
*** (1Mb / 1,000,000 bits) = 1.68Mbps**
1.68Mbps > 1.5Mbps Yes, the incoming channel will be congested.

Problem 5
(a) In BitTorrent, a peer sends chunks "tit-for-tat" to four neighbors currently sending chunks to it at the highest rates. And every 30 seconds it "optimistically unchokes" a randomly selected peer, i.e., sends chunks to it. Why is it *necessary* for the system to have chunks sent to randomly selected peers?
[5 pts]
To check if there are chunks that send even higher rates than the previously selected four.

(b) Compare DNS recursive query and iterative query. [5 pts]





Problem 6

(a) List the advantages and disadvantages by comparing client-server to peer-to-peer [5 pts]

CS - Pros: Robust security. Cons: Less efficient - Single point of failure, bottlenecks

P2P - Pros: More efficient, fault tolerant. Cons: Security risk, complex

(b) Compute the Internet checksum of the following 16-bit integers, using the following steps: [5 pts]

1 1 0 1 0 1 1 1 0 1 0 1 0 0 1 1
1 1 0 0 1 0 0 1 0 1 0 1 0 1 1 1

1. *add*

11010000010101010

2. *one's complement sum*

11010000010101011 ← add one bit

00101111101010100 ← invert

3. *Internet check sum*

101111101010100

Problem 7

(a) Given $T_A = 0$, $T_P = 0$ and $P = 0$, the maximum utilization formula for the sliding window protocol is

$U = 1$ for $WT_F > T_F + 2\tau$

and $U = WT_F / (T_F + 2\tau)$ otherwise

where T_F denotes the transmission time of a frame, W the send window size, and τ the one-way propagation time. Suppose the link transmission rate is 10 megabits/second, frame size = 10,000 bits, and τ = 10 msec. We would like to choose W such that U is at least 0.8. Determine W. Show your derivation steps. [10 pts]

T_F =frame size/transmission rate = 10,000 bits/10Mbps*1,000,000 bits/1Mb = 0.01 seconds

U = W*0.01/(0.01 + 2*10 msec * (1 sec/1000 msec)) => U=W*0.01/0.03 => U=W/3

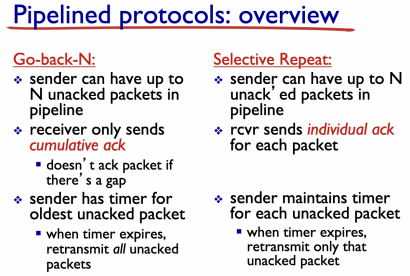
W/3 >= 0.8 → W >= 2.4 W >= 3

Problem 8

(a) In design of the reliable data transfer protocol, what mechanism is used to handle the case that the receiver may receive a segment with errors? (3pts)

Checksum

(b) Compare go-back-N and selective repeat. list their advantages and disadvantages. (7pts)



Go-Back-N: Simpler, less efficient in bandwidth utilization and selective retransmission

Selective Repeat: More efficient, increased complexity

Problem 9

Host A and B are directly connected with a 100 Mbps link. There is one TCP connection between the two hosts, and Host A is sending to Host B an enormous file over this connection. Host A can send its application data into its TCP socket at a rate as high as 120 Mbps but Host B can read out of its TCP receive buffer at a maximum rate of 50 Mbps. Describe the effect of TCP flow control. [10 pts]

Since the link capacity is only 100 Mbps, Host A's sending rate can be at most 100 Mbps. Still, Host A sends data into the receive buffer faster than Host B can remove the data. The receive buffer fills up at a rate of roughly 40 Mbps. When the buffer is full, Host B signals to Host A to stop sending data by setting RcvWindow = 0; Host A then stops sending until it receives a TCP segment with RcvWindow > 0. Host A will thus repeatedly stop and start sending as a function of the RcvWindow values it receives from Host B.