1. What is the capacity $C$ of a channel with a bandwidth of 10,000 Hz and a signal to noise ratio of 100 (S/N=100) (3 points)

   $$C = B \log_2(1+S/N) = 10000 \cdot \log_2(101)$$

2. What are the two missing layers in the TCP/IP model compared to the OSI model? How are the tasks of the two layers handled in the TCP/IP model? (3 points)

   Session Layer and Presentation layers. Both tasks handled by application layer. Presentation layer tasks handled by utility functions like ntohs(), htonl(), ntohl() and htonl(). Session layer tasks handled by cookies.

3. A data link layer employs (7,4) hamming code for error correction. Illustrate how a sequence of 4 data bits 1100 will be sent. (5 points)

   $1 1 0 \ x\ 0 \ x \ x$
   $1\ 0\ 0\ 1\ \ x = 1$
   $1\ 1\ 0\ x\ \ x = 0$
   $1\ 1\ 0\ x\ \ x = 0$
   Hamming code 1100001

4. A data link layer employs a window size of 5. The receiver receives the following sequence of frames numbered 0,1,3,5,6,4,2,5,0. For each of the nine frames indicate what the receiver should do (send ACK? Store? Discard? Provide frame to higher layer?) (9 points)

   Packet numbers 0 to 9
   0: store and send ACK
   1: store and send ACK
   3: store and send ACK
   5: store and send ACK
   6: store and send ACK
   4: store and send ACK
   2: store and send ACK
   5: drop and send ACK (retransmission)
   0: store and send ACK (not retransmission – 7,8,9 have been lost.

5. Explain why the throughput of slotted ALOHA is twice as high as that of pure ALOHA. What are the efficiencies of slotted and pure ALOHA? (5 points)

   Plain ALOHA has a vulnerable period equal to two packet durations (2T). If one station begins transmission at time $t$, no other station should commence transmission during the interval $t$ and $t+2T$.

   Slotted ALOHA has a vulnerable period of $T$. If one station begins transmission at time $t$, no other station should commence transmission during the interval $t$ and $t+T$.

   The efficiency of pure ALOHA is $1/2e$. The efficiency of slotted ALOHA is $1/e$

6. What is the need for imposing a minimum packet length in Ethernet (3 points)

   To detect collision the packet duration much be at least as long as the round trip duration. If the packet duration is smaller the sender may not sense a collision as the transmission is completed before the collision is sensed.
7. Why does 802.11 packet format include more than 2 addresses? (3 points)

In Ethernet the source and destination within a LAN typically have a bridge in between. Bridges do not have MAC addresses. In 802.11 between the source and destination MAC addresses one or more access points may be present. The MAC addresses of wireless access points are specified using additional address fields.

8. Give an example of circumstances under which you would use (4 points)
   1. pure ALOHA
   2. slotted ALOHA
   3. CSMA
   4. CSMA-CD

Explain.

Pure ALOHA is used when stations cannot sense the medium and do not have any kind of time-synchronization.
Slotted ALOHA is used when when stations cannot sense the medium, but are time-synchronized.
CSMA is used when stations can sense the medium but cannot sense collisions.
CSMA-CD is used when stations can sense the medium and sense collisions. (in pure ALOHA, slotted ALOHA and CSMA collisions can be inferred by lack of ACK)

A satellite serving 100 stations can receive a maximum of 10,000 packets per second. If the channel is being utilized optimally
   I. What is the average number of packets sent by every station? (for plain and slotted ALOHA)
   II. How many packets (per second) suffer collisions? (for plain and slotted ALOHA)

Plain ALOHA: The max number of packets that can be received collision free is 10,000/2e = 1840 per second. This will occur if all stations together will transmit 5,000 packets per second on an average (50 per station per second). 5000-1840 = 3160 (per second) will suffer collision.

Slotted ALOHA: The max number of packets that can be received collision free is 10,000/e = 3680 per second. This will occur if all stations together will transmit 10,000 packets per second on an average (100 per station per second). 10000-3680 = 6320/sec will suffer collision.

2. Assume that you are designing a CSMA-CD protocol which permits (9 points)
   ● maximum bit-rate of 1 Mbps
   ● maximum distance of 1250 m between any two stations (no repeaters are used)
   ● maximum packet size of 1000 bits

The velocity of propagation of electromagnetic waves in the medium is 250 million m/s. Determine other parameters of the system like minimum packet size, minimum packet duration, maximum round trip time.
What is the efficiency when the maximum allowed packet size is used for all packets? What is the efficiency if we use packet size of 500 bits?

L = 1250 m, c=250 million m/s
Propagation delay \( t = 5 \) micro seconds
R = 1 Mbps (1 bit per microsecond) packet size = 1000 bits; packet duration \( P = 1000 \) micro second
Minimum packet duration = \( 2 \times 5 = 10 \) microseconds
Minimum packet size = 10 bits.
Efficiency = \( P/(P+2te) = 1000/(1000+10e) \)
If packet size is 500 Efficiency = \( P/(P+2te) = 500/(500+10e) \)

3. Explain the hidden station and the exposed station problems in CSMA-CA. Is exposed station problem handled in 802.11? Why? (3 points)
A and B, B and C, C and D within range, A and C, B and D, A and D not within range

Hidden station problem: A is hidden from C. When A transmits to B, C will sense the medium as being free. If C transmits collision will occur at B

Expose station problem: B is exposed to C: When C is transmitting to D, if desired, B can transmit to A. However as B senses that the channel is not free, B will not transmit – leads to loss of efficiency.

Both problems can be addressed by using RTS-CTS handshake. However exposed station problem is not addressed in 802.11 as the sender will also need to receive an ACK. Specifically, when C transmits to D, B cannot transmit to A as B's transmission will collide with the ACK sent from D to C.

4. Briefly explain the concept of backward learning in bridges. (3 points)

Backward learning is the process of learning the topology by inspecting from addresses. Bridges inspect from addresses in MAC frames received through every line. If from address X is received through line 2 then line 2 should be used to send a MAC frame to X.

1. What is flooding? Explain the need for sequence number and age. (5 points)

A node receiving a packet through one link sends the packet through all other links. Sequence number is required to control flooding. A node will flood a packet (identified by a source and sequence number) only once. The last known sequence number for every node is stored. Only packets with sequence number higher than the stored sequence number (for that sender) will be flooded. Age is required to ensure that wrapping around of sequence numbers does not cause confusion.

2. Highlight the fundamental differences between distance vector and link-state routing approaches. (6 points)

Both enable nodes to determine the shortest path to any other node in the subnet.

In DV every node sends its routing table (distance to each node in the subnet) to all its neighbors. In LS every node floods its link state (the list of neighbors and distance to neighbors) to all nodes in the subnet

DV does not provide nodes with complete topology information. LS does.

3. Briefly discuss the three main approaches for congestion control (6 points)

Warning bit: When a packet passes through a congested router the router sets a bit in the packet. When the packet reaches the destination the destination sends a packet back to the source with a warning bit set. In any connection if a packet is received with a warning bit the sender slows down the rate at which packets are sent.

Choke packets: A congested router sends a choke packet to the sender requesting the sender to slow down

Hop-by-hop choke: A congested router sends a choke packet to the previous hop (another router) to buffer more packets and slow down transmission in the specific line.
4. An IP packet received by a router carries a payload of size 800 bytes. The layer-2 protocol used by the router does not support payload sizes greater than 400, necessitating fragmentation of the IP packet. Indicate the contents of the IP packets before and after fragmentation. Make reasonable assumptions and specify the values in the IP headers of every packet (the old packet and each fragment). (10 points)

Original packet: Payload 800 bytes, header 20 bytes

Fragments: Largest payload of each frame is 400. As each frame payload will have a header, the largest IP payload in each frame cannot be more than 380 bytes.

Need three fragments: fragment offsets should be multiple of eight.
For example:
  first fragment 376 bytes IP payload – MAC payload 396 bytes
  second fragment 376 bytes of IP payload – MAC payload 396 bytes
  third fragment 48 bytes of IP payload – MAC payload 68 bytes

All fragments will have the same IP identification number.
The first fragment will have offset 0, and MF bit set to 1.
The second fragment will have offset 47 and MF bit set to 1
The third fragment will have offset 94 and MF bit set to 0.

5. Explain the advantages and disadvantages of NATs (8 points)

Advantages:
Solves the IP explosion problem
Provides organizations with the ability to control access to server within the organization

Disadvantages:
Breaks many protocols – like FTP, H.263
Violates protocol hierarchy. A NAT is simultaneously a layer 3 (network layer) and layer 4 (transport layer) component. To work around application protocols broken by NATs, they also had to become layer 5 (application layer) components.
Slowed down speed of Ipv6 adoption.

6. What are some compelling reasons that motivated IPv6? Why do you think IPv6 is not prevalent yet? (5 points)
Increase address space
Reduce routing table sizes
reduce router overhead

Reasons why it is not prevalent:
NATs
CIDR works well enough to reduce routing table sizes
Many routers are pure hardware units and cannot be made to work with Ipv6.

What are the 3 important timers used in the TCP layer. Explain their purpose.

Retransmission timer: Started whenever a TCP packet is sent. If ACK is not received before the timer fires the packet is retransmitted.

Persistence timer: started whenever the other side advertises zero window size. If a non zero window size is not advertised before the timer fires a reminder is sent to prevent deadloack.
Keep alive timer: To periodically send TCP packets without payload to keep the connection alive. Helps the end-points distinguish between a dead connection and a connection where the applications do not have any data to send at this time (but desire to keep the connection).

Explain the need for dynamic window sizes in TCP.

Transport layer end-points participating in a TCP connection allocate buffer space for storing application data received from the other end. As A receives application data from B, the application data is stored in A's buffer till the application layer of A is ready to read from the buffer and then clear the buffer. The window size advertised by A informs B of the remaining buffer space at A. If the window size advertised by A is 500, B will not send more than 500 application bytes until it hears a new window size advertisement from A.