1) Describe the purpose of the following mechanisms in a reliable data transfer protocol: Checksum, Timer, Sequence Number, Acknowledgment, Negative Acknowledgement, and Window. **(Section 3.4.4)- C.T.S.A.NA.W.**

- Checksum
    - Used to detect bit errors in a transmitted packet
- Timer
    - Used to timeout/retransmit a packet, possible because the packet (or its ACK) was lost within the channel
- Sequence Number
    - Used for sequential numbering of packets. Gaps and/or packets with duplicate sequence numbers allow the receiver to detect missing/duplicate packets.
- Acknowledgment
    - Used by the receiver to tell the sender that a packet or set of packets has been received correctly.
- Negative Acknowledgement
    - Used by the receiver to tell the sender that the packet was not received correctly.
- Window
    - Window size may be set on the basis of the receivers ability to receive and buffer messages. The sender may be restricted to sending only packets with sequence numbers that fall within a given range.

2) Describe the purpose and operation of each field of the UDP segment header. **(Section 3.3.1) PG.204 -- S.D.L.C.**

Four fields, 2 bytes each

- Source port
- Destination port
    - Port numbers allow destination host to pass application data to the correct process running on the destination end system
- Length
    - Specifies number of bytes in the whole UDP Segment (header + data)

- Checksum
    - Provides for error detection. The checksum is used to determine whether the bits within the UDP segment have been altered as it is moved from the source to the destination.

3) Describe the purpose and operation of each field of the TCP segment header, ignoring the flags or urgent data field. **(Section 3.5.2) PG.236**

- Source port
- Destination port
    - Used for multiplexing/demultiplexing data from/to upper-layer applications
- Sequence Number
- Acknowledgement Number
    - Both used by TCP sender and receiver in implementing a reliable data transfer service
- Receive Window
    - Used for flow control. Indicates number of bytes that a receiver is willing to accept
- Length field
    - Specifies the length of the tcp header in 32-bit words
- Options field
    - Used when a sender and receiver negotiate the maximum segment size (MSS) or as a window scaling factor for use in high speed networks.
- Flag field
    - 6 bits.
        - ACK Bit
            - Used to indicate the value carried in the caknowledgement field is valid
        - RST Bit
        - Syn Bit
        - Fin Bit
            - All three used for connection setup and teardown
        - CWR bit
        - ECE bit
            - Both used in explicit congestion notification
        - PSH bit
            - Indicates that the receiver should pass the data to the upper-layer
            - immediately

- URG
    - Used to indicate that there is data in the urgent segment
- Urgent Data Pointer
    - Used to indicate the location of the last byte of the urgent data
- Checksum
    - Provides for error detection. The checksum is used to determine whether the bits within the UDP segment have been altered as it is moved from the source to the destination.

4) Describe the routing and forwarding processes as performed by a router (switch) in:

a) a traditional router network, and

- The routing algorithm function in one router communicates with the routing algorithm functions in other routers to compute the values for its forwarding table. This communication is performed by exchanging routing messages containing routing information according to a routing protocol.

b) an SDN-enabled network.

- Software-Defined Network
    - ○ Network is software defined because the controller that computes forwarding tables and interacts with routers is implemented in software

- A physically separate remote controller computes and distributes the forwarding tables to be used by each and every router. In a SDN the routing functionality is seperate from the physical router, the routing device performs forwarding only.

(Section 4.1.1)PG.306

5) Describe the following packet scheduling/queue management methods: FIFO, Priority, Round Robin, and WFQ. **(Section 4.2.5) PG.325**

FIFO

- **First in First Out**
  - Packets arriving at the link output queue wait for transmission if the link is currently busy transmitting another packet.
    - If there isn't enough space in the buffer, the queue will decide whether packet will be dropped or whether other packets will be removed from the queue to make space for the arriving packet

Priority

- **Priority Queueing**
  - Packets arrive at the output link and are classified into priority classes upon arrival at the queue
  - E.G. - a network operator might give VOIP packets priority over non-real time traffic such as SMTP or IMAP email packets

Round Robin

- Packets are sorted into classes and then it alternates service among the classes
  - E.G - a class 1 packet is transmitted, followed by a class 2 packet, followed by a class 1 packet, followed by a class 2 packet, and so on.

WFQ - weighted fair queueing

- Arriving packets are classified and queued in appropriate per-class waiting area
- Similar to round robin but each class is assigned a weight. WFQ will give each class a different amount of time depending on the weight of the class relative to the weight of the other classes.

6) CIDR and IPv4 subnetting **(Section 4.3.3) PG. 334**

SUBNET

- is an isolated network

IPV4

- Each interface needs an ip address, a portion of of an interfaces ip address is determined by the subnet to which it is connected.

CIDR Classless InterDomain Routing

- subnet portion of address of arbitrary length
- address format: a.b.c.d/x, where x is # bits in subnet portion of address

+ *Understand that a subnet is an isolated network and understand how ipv4 and cidr use subnetting.*

7) Describe the purpose of each field in the IPv6 datagram header.

(Section 4.3.5) PG.348

- **Version**
  - 4 bit field which identifies the IP version number
- **Traffic class**
  - 8 bit field which can be used to give priority to certain datagrams within a flow
- **Flow label**
  - 20 bit field used to identify a flow of datagrams
- **Payload length**
  - 16 bit unsigned integer giving the number of bytes in the ipv6 datagram following the header.
- **Next header**
  - Field which identifies the protocol to which the contents of this datagram will be delivered.
- **Hop limit**
  - The contents of this field are decremented by one by each router that forwards the datagram. If the hop limit = 0, the datagram is discarded.

- **source/destination addresses**

    - Indicated where the IP datagram is going and where its coming from.
- **Data ?**
    - This is the payload portion of the ipv6 datagram where the payload will be removed when the datagram reaches its destination.

8) Describe the purpose of each field in the IPv4 datagram header, ignoring the flags, identifier, and fragmentation offset. **(Section 4.3.1) PG. 330**

Version Number - 4 bits that specifiy the IP protocol version of the datagram

Header Length - 4 bits needed to determine where in the IP datagram the payload actually begins

Type of Service - allow different types of IP datagrams to distinguish from each other

Datagram Length - total length of IP datagram (header plus data) measured in bytes

Time-to-live - number of remaining times datagram can be processed. It is decremented by 1 each time it’s processed. Upon hitting 0, the router drops the datagram

Protocol - indicates which specific transport-layer protocol to which the data portion of the datagram should be passed to

Header checksum - detects bit errors in a received IP datagram

Source and destination IP addresses - has the ip address of source that created datagram and end destination for datagram to be delivered to

Options - allow an IP header to be extended

Data (payload) - contains the transport-layer segment (TCP or UDP) to be delivered to the destination. Can also carry other types of data, such as ICMP messages