Name = naveed

Id = 14703

Program = BS(SE)

sessional = Assigment

Date = 22/6/2020

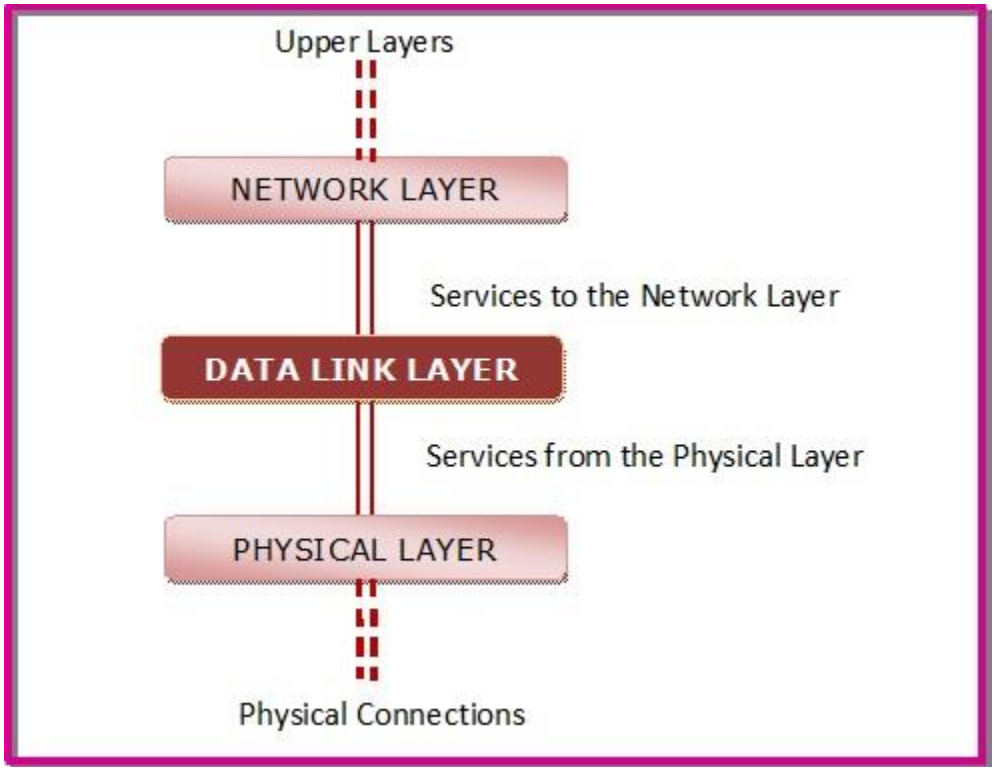
# Question no 1

Briefly describe the services provided by the data link layer ?

**Answer**:

In the OSI (Open System Interconnections) Model, each layer uses the services of the layer below it and provides services to the layer above it. The primary function of the data link layer is to provide a well-defined service interface to the network layer above it.

**Diagram:**



## Types of services:

There are three types services which are following.

- **Unacknowledged connectionless service :**

  Here, the data link layer of the sending machine sends independent frames to the data link layer of the receiving machine. The receiving machine does not acknowledge receiving the frame. No logical connection is set up between the host machines. Error and data loss is not handled in this service. This is applicable in Ethernet services and voice communications.

- **Acknowledged connectionless service :**

  Here, no logical connection is set up between the host machines, but each frame sent by the source machine is acknowledged by the destination machine on receiving. If the source does not receive the acknowledgment within a stipulated time, then it resends the frame. This is used in Wifi (IEEE 802.11) services.

- **Acknowledged connection-oriented service :**

  This is the best service that the data link layer can offer to the network layer. A logical connection is set up between the two machines and the data is transmitted along this logical path. The frames are numbered, that keeps track of loss of frames and also ensures that frames are received in correct order. The service has three distinct phases –

# Question no 2 part(1)

1. Compare and Contrast
   - byte-oriented and bit-oriented protocols

**Bit oriented Protocol-:** Bit oriented protocol is a communication protocol that sees the transmitted data as an opaque stream of bite with no symantics, or meaning, controls codes are defined in the term bits.

**Byte Oriented Protocol -:** Byte oriented protocol is also a communication protocol in which full bytes are used as control codes.Byte Oriented Protocol is also known as character - Oriented Protocol

# Question no 2 part(2)

- byte-stuffing and bit-stuffing

**Answer:**

**Byte stuffing:**

is a mechanism to convert a message formed of a sequence of bytes that may contain reserved values such as frame delimiter, into another byte sequence that does not contain the reserved values.

**Bit stuffing:**

is the mechanism of inserting one or more non-information bits into a message to be transmitted, to break up the message sequence, for synchronization purpose.

# Question no 2 part (3)

- flow control and error control

**Answer:**

**Difference B/W Flow Control And Error Control:** Flow control and Error control are the control mechanism at data link layer and transport layer. Whenever the sends the data to the receiver these two mechanisms helps in proper delivering of the reliable data to the receiver. The main difference between the flow control and error control is that the

**flow control**: observes the proper flow of the data from sender to receiver, on the other hand,

**error control** :observes that the data delivered to the receiver is error free and reliable.

# Question no 2 part (4)

- HDLC and PPP

**Answer:**

## Difference Between HDLC and PPP

The major difference between HDLC and PPP is that HDLC is the bit oriented protocol, while PPP is the character-oriented protocol. The HDLC and PPP are the crucial data link layer protocols used in WAN (wide area network) where the HDLC can also be implemented with PPP for the efficient results.

HDLC describes the encapsulation technique employed on the data in the synchronous serial data link. On the other hand, the PPP protocol deals with the encapsulation of the data transported in the point-to-point links and it could be synchronous or asynchronous

# Question no 2 part (5)

- Go-Back-N ARQ protocol and Selective-Repeat-ARQ protocol
  **Answer:**

## Difference Between Go-Back-N and Selective Repeat Protocol:

Both Go-Back-N Protocol and Selective Repeat Protocol are the types of sliding window protocols.
The main difference between these two protocols is that after finding the suspect or damage in sent frames go-back-n protocol re-transmits all the frames whereas selective repeat protocol re-transmits only that frame which is damaged.

# Question no 2 part (6)

- circuit-switched network and a packet-switched network

**Answer:**

**Definitions:** Packet-switched networks move data in separate, small blocks -- packets -- based on the destination address in each packet. When received, packets are reassembled in the proper sequence to make up the message. Circuit-switched networks require dedicated point-to-point connections during calls.

Circuit-switched networks and packet-switched networks have traditionally occupied different spaces within corporations. Circuit-switched networks were used for phone calls and packet-switched networks handled data. But because of the reach of phone lines and the efficiency and low cost of data networks

# Question no 2 part (7)

- space-division and time-division switches

**Answer:**

## Space Division Switching:

The fundamental operation of a switch is to setup and release connection between subscribers. It involves direct connection between subscriber loops at an end office or between station loops at a PBX. The switches are hardware and/or software devices capable of creating temporary connections between two or more subscribers. In this section, the space division switching is described and in section 5.6, time division switching is explained.

### Multistage Switching

It is inefficient to build complete exchanges in single stages. Single stage can only be used to interconnect one particular inlet outlet pair. Also the number of crosspoints grows as the square of the inputs for grading, N (N-1)/2 for a triangular array and N (N-1) for a square array. Also the large number of crosspoints on each inlet and outlet line imply a large amount of capacitive loading on the message paths. Therefore, it is usual to build exchanges in two or three stages to reduce the number of crosspoints and to provide alternative paths.

# Question no 3

Explain the protocols for noiseless and noisy channels

**Answer:**

## Noiseless Channel:

An ideal channel in which no frames are lost, duplicated or corrupted is regarded as Noiseless Channel.

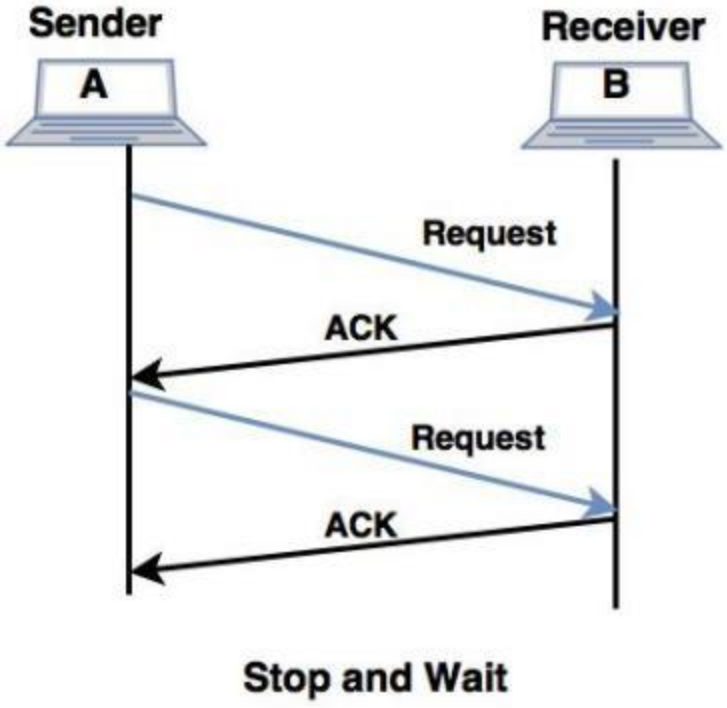
## Simplest Protocol

- In simplest protocol, there is no flow control and error control mechanism. It is a unidirectional protocol in which data frames travel in only one direction (from sender to receiver).
- Also, the receiver can immediately handle any received frame with a processing time that is small enough to be negligible.
- The protocol consists of two distinct procedures :a sender and receiver. The sender runs in the data link layer of the source machine and the receiver runs in the data link layer of the destination machine. No sequence number or acknowledgements are used here.

## Stop and Wait Protocol

- The simplest retransmission protocol is stop-and-wait.
- Transmitter (Station A) sends a frame over the communication line and then waits for a positive or negative acknowledgement from the receiver (station B).
- If no error occurs in the transmission, station B sends a positive acknowledgement (ACK) to station A.
- Now, the transmitter starts to send the next frame. If frame is received at station B with errors, then a negative acknowledgement(NAK) is sent to station A. In this case, station 'A' must retransmit the old packet in a new frame.
- There is also a possibility that the information frames or ACKs may get lost.
- Then, the sender is equipped with a timer. If no recognizable acknowledgement is received when the timer expires at the end of time out interval, the same frame is sent again.

- The sender which sends one frame and then waits for an acknowledgement before process is known as **stop and wait.**




Noisy Channels

Consider the normal situation of a communication channel that makes errors. Frames may be either damaged or lost completely.

## 1. Stop and Wait Automatic Repeat Request:

- In a noisy communication channel, if a frame is damaged in transit, the receiver hardware will detect this when it computes the checksum.
- If a damaged frame is received, it will be discarded and transmitter will retransmit the same frame after receiving a proper acknowledgement.
- If the acknowledgement frame gets lost and data link layer on 'A' eventually times out. Not having received an ACK, it assumes that its data frame was lost or damaged and sends the frame containing packet 1 again. This duplicate frame also arrives at data link layer on 'B', thus part of file will be duplicated and protocol is said to be failed.
- A typical approach to solve this problem is the provision of a sequence number in the header of the message.

- The receiver can then check the sequence number determine if the message is a duplicate since only message is transmitted at any time.
- The sending and receiving station needs only 1-bit alternating sequence of '0' or '1' to maintain the relationship of the transmitted message and its ACK/ NAK.
- A modulo-2 numbering scheme is used where the frames are alternatively label with '0' or '1' and positive acknowledgements are of the form ACK 0 and ACK 1.

**2. Sequence numbers:**

- The protocol specifies that frames need to be numbered. This is done by using sequence number. A field is added to the data frame to hold the sequence number of that frame.
- The sequence numbers are based on modulo-2 arithmetic.
- Stop-and-wait ARQ is the simplest mechanism for error and flow control.

# Question no 4

1. Explain Piggybacking in HDLC.

**Answer:**

Piggybacking data is a bit different from Sliding Protocol used in the OSI model. In the data frame itself, we incorporate one additional field for acknowledgment (called ACK).

Whenever party A wants to send data to party B, it will carry additional ACK information in the PUSH as well.

For example, if A has received 5 bytes from B, which sequence number starts from 12340 (through 12344), A will place "ACK 12345" as well in the current PUSH packet to inform B it has received the bytes up to sequence number 12344 and expects to see 12345 next time. (ACK number is the next sequence number of the data to be PUSHed by the other party.)

Three rules govern the piggybacking data transfer.

- If station A wants to send both data and an acknowledgment, it keeps both fields there.
- If station A wants to send the acknowledgment, after a short period of time to see whether a data frame needs to be sent, then decide whether send an ACK frame alone or attach a data frame with it.
- If station A wants to send just the data, then the previous acknowledgment field is sent along with the data. Station B simply ignores this duplicate ACK frame upon receiving

# Question no 5

Explain blocking in a switched network ?

**Answer:**

In multistage switching, blocking refers to times when one input cannot be connected to an output because there is no path available between them—all the possible intermediate switches are occupied

# Question no 7

List three techniques of digital-to-digital conversion?

**Answer:**

List three techniques of digital-to-digital conversion.

The three different techniques described in this chapter are line coding, block coding, and scrambling.Distinguish between a signal element and a data element. A data element is the smallest entity that can represent a piece of information (a bit). A signal element is the shortest unit of a digital signal. Data elements are what we need to send; signal elements are what we can send. Data elements are being carried; signal elements are the carriers. Distinguish between data rate and signal rate. The data rate defines the number of data elements (bits) sent in 1s. The unit is bits per second (bps). The signal rate is the number of signal elements sent in 1s. The unit is the baudDefine baseline wandering and its effect on digital transmission. In decoding a digital signal, the incoming signal power is evaluated against the baseline (a running average of the received signal power). A long string of 0s or 1s can cause baseline wandering (a drift in the baseline) and make it difficult for the receiver to decode correctlyDefine a DC component and its effect on digital transmission. When the voltage level in a digital signal is constant for a while, the spectrum creates very low frequencies, called DC components, which present problems for a system that cannot pass low frequencies. Define the characteristics of a self-synchronizing signal. A self-synchronizing digital signal includes timing information in the data being transmitted. This can be achieved if there are transitions in the signal that alert the receiver to the beginning, middle, or end of the pulseList five line coding schemes discussed in this book. In this chapter, we introduced unipolar, polar, bipolar, multilevel, and multi transition coding. Define block coding and give its purpose. Block coding provides redundancy to ensure synchronization and to provide inherent error detecting. In general, block coding changes a block of m bits into a block of n bits, where n is larger than m. Define scrambling and give its purpose. Scrambling, as discussed in this chapter, is a technique

that substitutes long zerolevel pulses with a combination of other levels without increasing the number of bits. 10. Compare and contrast PCM and DM. Both PCM and DM use sampling to convert an analog signal to a digital signal. PCM finds the value of the signal amplitude for each sample; DM finds the change between two consecutive samples

# Question no 6

2. Two neighboring nodes (A and B) use a sliding-window protocol with a 3-bit sequence number. As the ARQ mechanism, go-back-N is used with a window size of 4. Assuming A is transmitting and B is receiving, show the window positions for the following succession of events:
   - Before A sends any frames
   - After A sends frames 0, 1, 2 and receives acknowledgment from B for 0 and 1
   - After A sends frames 3, 4, and 5 and B acknowledges 4 and the ACK is received by A

**Answer:**

a. Before A sends any frames

b. System A - Initial

c. System B – Initial

d. 0 1 2 3 4 5 6 7 0 1 2 3

e. b. System A sends 3 frames F0, F1, F2 System

f. B receives 3 frames F0, F1, F2

g. No acknowledgments received

h. No acknowledgments sent System A

i. System B 0 1 2 3 4 5 6 7 0 1 2 3 c. System A receives RR3 from B

j. System B sends RR3 System

k. A System B 0 1 2 3 4 5 6 7 0 1 2 3 d.

l. System A sends F3, F4, F5, F6 System B sends RR4

m. System A receives RR4 System

n. B receives F4, F5, F6 System

o. A System B

p. 0 1 2 3 4 5 6 7 0 1 2 3

q. 0 1 2 3 4 5 6 7 0 1 2 3

r. 0 1 2 3 4 5 6 7 0 1 2 3

s. 0 1 2 3 4 5 6 7 0 1 2 3

t. 0 1 2 3 4 5 6 7 0 1

# Question no 8

What is the number of bits in an IPv4 address? What is the number of bits in an IPv6 address?

**Answer:**

An **Internet Protocol Version 6 address** (**IPv6 address**) is a numerical label that is used to identify a network interface of a computer or a network node participating in an IPv6 computer network and for locating it in the network. IP addresses are transmitted in the fields of the packet header to indicate the source and the destination of each network packet. The IP addressof the destination address is used to make decisions about routing IP packets to other networks.

IPv6 is the successor to the first addressing infrastructure of the Internet, Internet Protocol (IPv4). In contrast to IPv4, which defined an IP address as a 32-bit value, IPv6 addresses have a size of 128 bits. Therefore, IPv6 has a vastly enlarged address space compared to IPv4.

# Question no 9

3. Distinguish between data rate and signal rate.

**Answer:**

## The difference:

Digital data is very different from digital signal. The process of converting digital data to digital signal is called as line coding.Now, to discriminate between data and signal, data is what we need to send. But signal is what we can send. So, signal is the carrier which carries data.Also, keep in mind that the smallest entity of the data, that can represent a piece of information is called data element and shortest meaningful unit of a signal is called signal element. Consider this as in the following scenario – Consider a train. Each carriage is a signal element. Each passenger inside the train is a data element. The train as a whole is a signal and all passengers together represent a data.

## Data rate and Signal rate:

- Data rate – Number of data elements transmitted per second.
- Signal rate – Number of signal elements transmitted per second.

Now, the unit of data rate is bit rate. And the unit of signal rate is pulse rate/ modulation rate/ baud rate or simply baud. From the previous example, we can see that, a carriage in a train can carry more than one person. So, if you consider the number of person is more than one per carriage, you can say that bit rate is greater than baud rate for the signal.

# Question no 10

What is NAT? How can NAT help in address depletion?

**Answer:**

## What is NAT?

Network Address Translation (NAT) is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a

router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.As part of this capability, NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that address. NAT offers the dual functions of security and address conservation and is typically implemented in remote-acceenvironments**..** Basically, NAT allows a single device, such as a router, to act as an agent between the Internet (or public network) and a local network (or private network), which means that only a single unique IP address is required to represent an entire group of computers to anything outside their networ**.** In order to configure traditional NAT, you need to make at least one interface on a router (NAT outside) and another interface on the router (NAT inside) and a set of rules for translating the IP addresses in the packet headers (and payloads if desired) need to be configured. In order to configure Nat Virtual Interface (NVI), you need at least one interface configured with NAT enable along with the same set of rules as mentioned above.For more information, refer to Cisco IOS IP Addressing Services Configuration Guide or Configuring the NAT Virtual Interface. Cisco IOS software-based NAT is not fundamentally different from the NAT function in the Cisco PIX Security Appliance. The main differences include the different traffic types supported in the implementations. Refer to Cisco PIX 500 Series Security Appliances and NAT Configuration Examples for more information on the configuration of NAT on Cisco PIX devices (includes the traffic types supported).