

1. Physical Layer

CN
classmate

Date _____
Page _____

Q.1 What are various network devices.

-> There are various network devices used in computer network to facilitate communication and connectivity.

* ① Router : A router is a network device that connects multiple networks together and forwards data packet between them. It operates at the network Layer 3 in OSI model.

* ② Switch : A switch is a device that connects multiple devices within a local area network and enables the exchange of data between them. It operates at the data link layer 2 in OSI model.

* ③ Hub : A hub is a simple network device that connects multiple devices in a LAN and broadcasts incoming data to all connected devices. It lacks the intelligence and efficiency of a switch.

④ Modem : A modem is a device that enables the transmission of data over communication channels. It converts digital signals from computer into analog signals.

⑤ Bridges : A bridges operates data link layer. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port : 2 Port device.

Q.2 Difference FHSS & DSSS

FHSS

DSSS

- ① FHSS is stands for Frequency-Hopping Spread Spectrum.
- ② Multiple frequency are used.
- ③ Frequency reuse is allowed.
- ④ Sender need not wait.
- ⑤ Power strength of the signal is high.
- ⑥ It is never affected by interface.
- ⑦ It is cheaper.
- ⑧ This is the commonly used technique.
- ① DSSS is Stands for Direct - Sequence Spread Spectrum.
- ② Single frequency are used.
- ③ Frequency reuse is not allowed.
- ④ Sender has to wait if the spectrum is busy.
- ⑤ Power strength of the signal is low.
- ⑥ It can be affected by interface.
- ⑦ It is expensive.
- ⑧ This technique is not frequently used.

Q.3 Manchester Encoding

Differential Manchester encoding.

- ① Manchester encoding is a synchronous clock-encoding technique used by the physical layers to encode the clock & data of a synchronous bit stream.
- ① Differential manchester encoding is a line code in which data & clock signals are combined to form a single 2-level self synchronizing data stream.
- ② Low to High represents 1 and High to Low represents 0.
- ② No transition at the start of a bit period represents 1 and transition at the start of a bit period represents 0.
- ③ It provides better signal synchronization.
- ③ It provides less signal synchronization.
- ④ Signal rate is the drawback.
- ④ Signal rate is two times that of NRZ.
- ⑤ Used by IEEE 802.3 specification for Ethernet LAN.
- ⑤ Used by IEEE 802.5 specification for token ring LAN.

Q.4 LAN

MAN

WAN

① LAN stands for local area network.	① MAN stands for metropolitan area network.	① WAN stands for wide area network.
② Operates in small area such as same building.	② Operates in large area such as a city.	② Operates in large area such as country.
③ LAN ownership is private.	③ MAN ownership can private or public.	③ WAN not be owned by one organization.
④ Transmission speed of LAN is high.	④ Transmission speed of MAN is average.	④ Transmission speed of WAN is Low.
⑤ There is less congestion in LAN.	⑤ There is more congestion in MAN.	⑤ there is more congestion than MAN in WAN.
⑥ There is more fault tolerance in LAN.	⑥ there is less fault tolerance.	⑥ there is also less fault tolerance.

Q.S Explain TCP/IP :

Layers 4 :	Application
Layers 3 :	Transport
Layers 2 :	Internet
Layers 1 :	Network access

- ① Application : ① Application layer is responsible for supporting specific network application & services. ② HTTP, FTP, SMTP & DNS protocols operate this layer.
- ② Transport : ① The transport layer provides end-to-end communication between devices on the network. ② TCP & UDP two protocols used in this layer.
- ③ Internet : ① Internet layer is responsible for addressing and routing data packets across different networks. It uses IP to assign unique IP address to device.
- ④ Network Access : ① Is responsible for the physical transmission of data over the network. This layer defines protocols & standard for addressing and transmitting data packets.

Q. OSI Model:

- ⑦ Application
- ⑥ Presentation
- ⑤ Session
- ④ Transport
- ③ Network
- ② Data Link
- ① Physical

Q. Design issues for Layers:

- ① Reliability: Network channels & components may be unreliable, resulting in loss of bits while data transfer.
- ② Scalability: Networks are continuously evolving. The sizes are continually increasing leading to congestion.
- ③ Error Control: Unreliable channels introduce a number of errors in the data streams that are communicated.
- ④ Flow Control: If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. Proper flow control mechanism ~~are~~ need to be implemented.

2. logical link Control

classmate

Data

Page

Q.1 Define:

- ① Error control: Is done to prevent duplication of frame, the errors introduced during transmission from source to destination machines must be detected & corrected at the destination machine.
- ② Flow control: Flow control is done to prevent the flow of data frame at the receiver end.

Q.2 Explain Sliding Window Protocol

- ① The sliding window is a technique for sending multiple frames at a time.
- ② It controls the data packets between the two devices.
- ③ It is also used in TCP.
- ④ ~~Two Types~~

Sliding Window Protocol has two types

Go-Back N ARQ

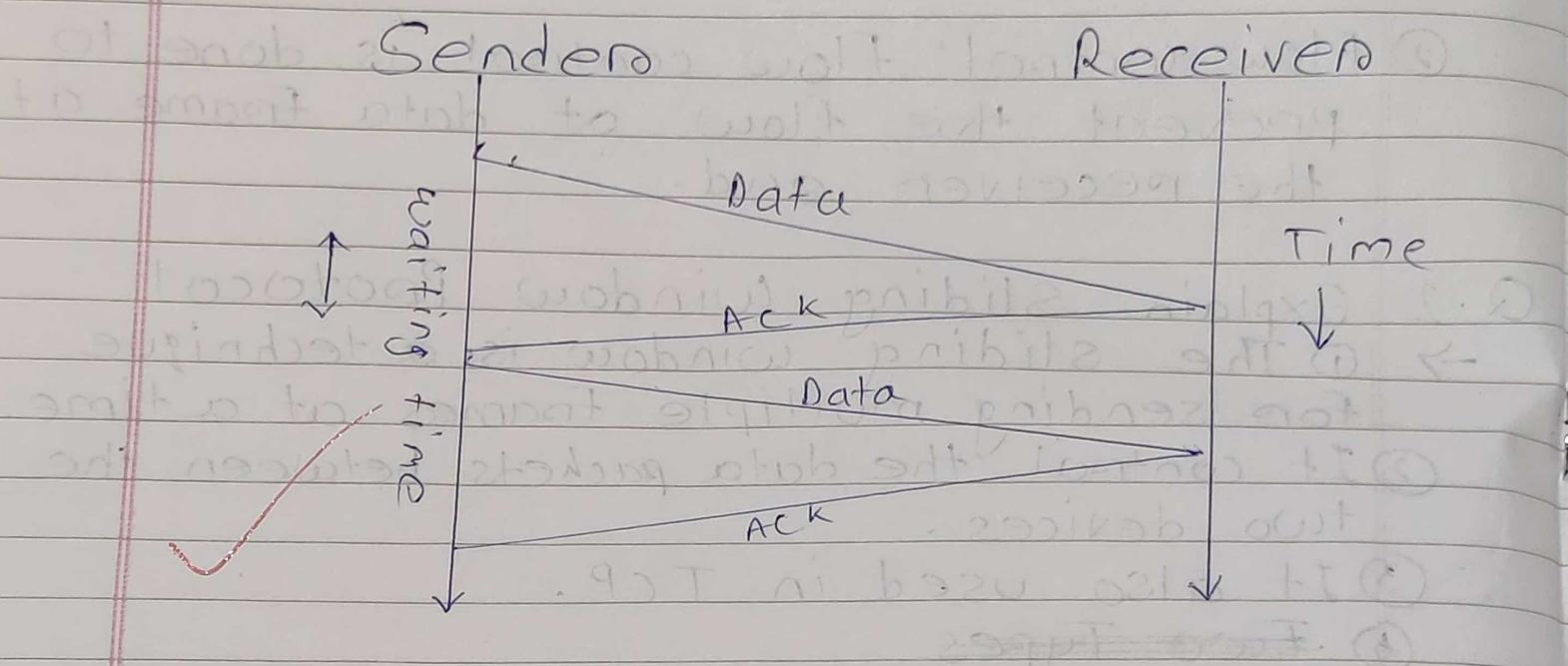
Selective Repeat ARQ

- ① less complex
- ② does not require sorting
- ③ does not require searching
- ④ It uses more bandwidth.
- ⑤ wastes lot of bandwidth.

- ① more complex
- ② sorting is done
- ③ searching is done
- ④ It uses less bandwidth.
- ⑤ loss of low bandwidth.

Q.3 Explain stop and wait protocol?

- ① It is simplest flow control method.
the sender will transmit one frame at a time to the receiver.
- ② This time is sender-waiting time & the sender is idle during time.
- ③ The main advantage of stop & wait protocol is their accuracy.



Features:

- ① It used in connection-oriented communication.
- ② It offers error & flow control.
- ③ It used data link & transport layer.

Q.4 Explain Hamming code with Ex:

- ① Hamming code is a error-correction codes that can be used to detect & correct the errors.
- ② it perform recalculations to detect errors & find the bit position that has error.

Q: Hamming code structure [7 Bit]

P ₇	P ₆	P ₅	P ₄	P ₃	P ₂	P ₁
?	1	0	?	1	?	?

For

P₁: check 1 bit, skip 1 bit.

P₂: check 2 bit, skip 2 bit.

P₄: check 4 bit, skip 4 bit

P ₁ = P ₁	D ₃	D ₅	D ₇
	1	0	1

$\therefore P_1 = \text{even} = 0$

P ₂ = P ₂	D ₃	D ₆	D ₇
	1	1	1

$\therefore P_2 = \text{odd} = 1$

P ₄ = P ₄	D ₅	D ₆	D ₇
	0	1	1

$\therefore P_4 = \text{even} = 0$

When ~~parti~~ parity bits is odd (1)
then this is some error in
hamming code structure.

Q.

HDL C

PPP

P

- ① HDLC stands for High level Data link Control.
- ② HDLC is bit-oriented protocol.
- ③ HDLC is implemented by Point-to-Point link configuration.
- ④ HDLC works at layers 2.
- ⑤ HDLC is used in synchronous media.
- ⑥ HDLC is more costly comparatively.
- ① PPP stands for Point-to-Point Protocol.
- ② PPP is byte-oriented protocol.
- ③ PPP is implemented by Point-to-Point configuration only.
- ④ PPP works at layers 2 & layer 3.
- ⑤ PPP is used in synchronous and asynchronous media.
- ⑥ PPP is less costly comparatively.

3 Medium Access Control

Q. Explain Pure and slotted ALOHA

Pure ALOHA

- ① any station can transmit the data at any time.

- ② The time is continuous and not globally synchronized.

- ③ Vulnerable time for

$$\text{Pure ALOHA} = 2 \times Tt$$

- ④ Maximum efficiency

$$= 18.4\%$$

- ⑤ does not reduce the numbers of collision to half.

- ⑥ The probability of successful transmission of the data packet

$$= G \times e^{-2G}$$

Slotted ALOHA

- ① any station can transmit the data at the beginning of any time slot.

- ② The time is discrete and globally synchronized.

- ③ Vulnerable time for slotted ALOHA = Tt

- ④ maximum efficiency = 36.8%

- ⑤ reduce the number of collisions to half.

- ⑥ The probability of successful transmission of the data packet

$$= G \times e^{-G}$$

Q. Explain WDMA?

- ① WDMA stands for Wavelength Division Multiplexing.
- ② WDM is a technology that increase bandwidth by allowing different data streams at different frequencies to be sent over a single optical fiber network.
- ③ Signals at WDM wavelengths are independent from each other.

Q. Fast Ethernet

- ① Fast ethernet is the succession of 10 - Base - T Ethernet.
- ② The maximum speed of Fast Ethernet is 100 Mbps.
- ③ Fast Ethernet is simple to configure.
- ④ Fast Ethernet generates less delay.
- ⑤ Maximum coverage distance is 10 km.
- ⑥ Round trip delay is 100 to 500 times.

Gigabit Ethernet

- ① Gigabit Ethernet is succession of Fast Ethernet.
- ② Gigabit Ethernet speed is 10 Gbps.

③ Gigabit Ethernet is quite complex to configure.

- ④ Gigabit Ethernet generates less delay.

⑤ Maximum coverage distance is 70 km.

- ⑥ round trip delay is 2000 bit times.

Q. CSMA CD

① It is type of CSMA to detect the collision on a shared channel.

② It is collision detection protocol.

③ It is used 802.3 Ethernet network cable.

④ It works in wired networks.

⑤ It minimizes the recovery time

⑥ It more popular than CSMA CA.

CSMA CA

① It is type CSMA to avoid collision on a shared channel.

② It is collision avoidance Protocol.

③ It is used 802.11 ethernet network cable

④ It works in wireless networks.

⑤ It minimizes the risk of collision.

⑥ It is less popular than CSMA CD.

Q. Static channel Allocation:

① In static channel allocation a fixed portion of the frequency channel is allotted to each user.

② the bandwidth is divided into N channels using FDM.

③ this scheme is also referred as fixed channel allocation.

Q. Dynamic channel allocation:

- ① Frequency bands are not permanent assigned to the users.
- ② this allocation scheme optimizes bandwidth usage and results in faster transmissions.
- ③ Dynamic channel allocation is further divided into centralized and distributed allocation.

4 Network Layer

classmate

Date _____

Page _____

Q.1

IPV 4

① 32 bits address

IPV 6

① 128 bits address

② checksum in
header included

② No checksum

③ Fragmentation done
by routers & source
node.

③ Fragmentation only
by source code.

④ IPsec support
Optional.

④ IPsec support
Required.

⑤ IP configuration
manually.

⑤ IP configuration
Auto

⑥ QoS differentiated
services

⑥ QoS Use traffic
classes & flow labels

Q.2 What is switching.

- ① In large networks there might be multiple paths linking sender and receiver.
- ② There are three types of switching.
- i) Circuit switching
 - ii) Message switching
 - iii) Packet switching.

Packet Switching

① Packet switching less reliable.

② It is store & forward technique.

✗ ③ Transmission of data is done not only by source but also by intermediate routers.

④ Less wastage of resource.

⑤ Is suitable for handling traffic.

⑥ require complex protocols for delivery.

⑦ can follow any route.

Circuit switching

① Circuit switching is more reliable.

② It is not store & forward technique.

③ Transmission of the data is done by the source.

④ Wastage of resource.

⑤ Is not convenient for handling traffic.

⑥ require simple protocols for delivery.

⑦ follows the same route.

Q. congestion control algorithm

→ ① Congestion Control is a mechanism that controls the entry of data packets into the network.

② There are two congestion control algorithm:

i) ~~Leaky~~ Bucket Algorithm

ii) Token bucket Algorithm.

Q. ① RIP : ① RIP stands for Routing information Protocol.

② Is a distance-vector routing protocol

③ Mobile IP : ① Mobile IP is a communication protocol that allows the users to move from one network to another with the same IP address

④ AODV : ① Ad-hoc On-demand Distance Vector.

② Is a loop-free routing protocol for ad-hoc networks.

5 Transport layer

classmate

Date _____

Page _____

TCP

Transmission Control
Protocol

UDP

User Datagram Protocol

- Q. **TCP**
- ① An acknowledgment segment is present
 - ② TCP is slow
 - ③ Retransmission of lost packets is possible.
 - ④ TCP is heavy-weight
 - ⑤ TCP doesn't support broadcasting.
 - ⑥ TCP is a connection oriented protocol.
- ① No acknowledgment segment.
- ② UDP is fast.
- ③ There is no retransmission of lost packets.
- ④ UDP is light-weight.
- ⑤ UDP supports broadcasting.
- ⑥ UDP is the datagram oriented protocol.
- Q. * RTP : ① RTP stands for Real time transport Protocols.
- ② A protocol is designed to handle real-time traffic of the internet.
 - ③ RTP must be used with UDP.
 - ④ RTP supports different formats of file like MPEG and MJPEG.

- * SCTP : ① SCTP stands for Stream Control Transmission Protocol.
- ② SCTP is a computer networking communication protocol in the transport layer.

③ The protocol provides the message-oriented features of the UDP.

Q. TCP Time Management:

- ① TCP stand for transmission protocol time management.
- ② TCP uses timers to manage various aspects of its operation.
- ③ There are 3 key timers used in TCP.
 - i Retransmission Timer.
 - ii Persist Timer.
 - iii Keepalive Timer.

Q. TCP Congestion Control:

- ① TCP congestion control is a mechanism to prevent network congestion.
- ② Ensure fair sharing of available network resources among different TCP connection.
- ③ There are 3 Phases of TCP congestion
 - i Slow start
 - ii Congestion Avoidance
 - iii Congestion Detection

Q. Integrated Services

① Is not Scalable

② Involve per flow setup.

③ Involve end to end service scope.

④ It also called IntServ

Differentiated Services

① Is scalable

② Involve long term setup

③ Involve domain service scope

④ It also called DIFFSen.

Q. ~~The~~ Describe Transport layer services.

① The Transport layer is the fourth layer of the OSI model and play crucial role in providing reliable and efficient communication between end systems over a network.

- ② Some key services provide by transport layer
- i Connection Establishment and termination
 - ii Segmentation and Reassembly
 - iii Reliable Data delivery.
 - iv Flow control.
 - v Congestion control.
 - vi Multiplexing & demultiplexing.

6 Application layer

classmate

Date _____

Page _____

Q. SMTP

POP3

① SMTP stands for Simple Mail transfer Protocol.

② It is used for sending message.

③ SMTP is also known as PUSH protocol.

④ The port no. is 25, 465 & 587

⑤ It is implied between sender mail server & receiver mail server.

⑥ It is an MTA for sending message to receiver.

① POP3 stands for Post office Protocol version 3.

② It is used for accessing message

③ POP3 is also known as POP protocol.

④ The port no. is 110 or 995.

⑤ It is implied between receiver mail server & receiver mail server.

⑥ It is MAA for accessing message from mailbox.

Q. Explain DNS :

- ① DNS stands for Domain Name System
- ② DNS is required for the functioning of the internet.
- ③ DNS is a directory services that provides a mapping between the name of host on network & numerical address.
- ④ DNS is a service that translates the domain name into IP address.

Q. Explain SNMP :

- ① SNMP stands for Simple Network Management Protocol.
- ② SNMP is an application layer protocol.
- ③ Is used to monitor the network detect network faults and sometimes even used to configure remote devices.
- ④ There are 3 ~~SNMP~~ SNMP components
 - i) SNMP manager
 - ii) SNMP agent
 - iii) Management information Base.

Q. Explain DHCP:

- ① DHCP stands for Dynamic Host Configuration Protocol.
- ② It is critical features on which the users of an enterprise network communicate.
- ③ DHCP is based on the client-server model.
- ④ DHCP helps enterprise to smoothly manage the allocation of IP address.