

NOTES LINK -> ALL QUESTION BANK

QUESTION BANK

Unit 3: Medium Access sub layer

Ques. No.	Question	Marks
1	What is bridge? Bridges are used to connect two subnetworks that use interchangeable protocols. It combines two LANs to form an extended LAN. The main difference between the bridge and repeater is that the bridge has a penetrating efficiency.	2
2	What is a repeater? Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.	2
3	Define the term medium access control mechanism. The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.	2
4	What is a switch? Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network	2
5	Define router. Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.	2
6	What is channel allocation? When there are more than one user who desire to access a shared network channel, an algorithm is deployed for channel allocation among the competing users. The network channel may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum. Channel allocation algorithms allocate the wired channels and bandwidths to the users, who may be base stations, access points or terminal equipment.	2

NOTES LINK -> ALL QUESTION BANK

	<p>Channel Allocation Schemes</p> <p>Channel Allocation may be done using two schemes –</p> <ul style="list-style-type: none"> • Static Channel Allocation • Dynamic Channel Allocation 	
7	<p>What is more difficult among error detection and error correction? Explain.</p> <p>Error detection is a method that can look at some data and detect if it has been corrupted while it was stored or transmitted.</p> <p>Error correction is a step better than error detection; when it detects an error it tries to put the data back to how it should have been.</p>	2
8	<p>Define ARQ.</p> <p>ARQ stands for Automatic Repeat Request also known as Automatic Repeat Query. ARQ is an error-control strategy used in a two-way communication system</p>	2
9	<p>Define Ethernet</p> <p>Ethernet is a type of communication protocol that is created at Xerox PARC in 1973 by Robert Metcalfe and others, which connects computers on a network over a wired connection. It is a widely used LAN protocol, which is also known as Alto Aloha Network. It connects computers within the local area network and wide area network. Numerous devices like printers and laptops can be connected by <u>LAN and WAN</u> within buildings, homes, and even small neighborhoods.</p>	2
10	<p>What is Sliding Window Protocol?</p> <p>The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in <u>TCP (Transmission Control Protocol)</u>.</p> <p>In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.</p>	2

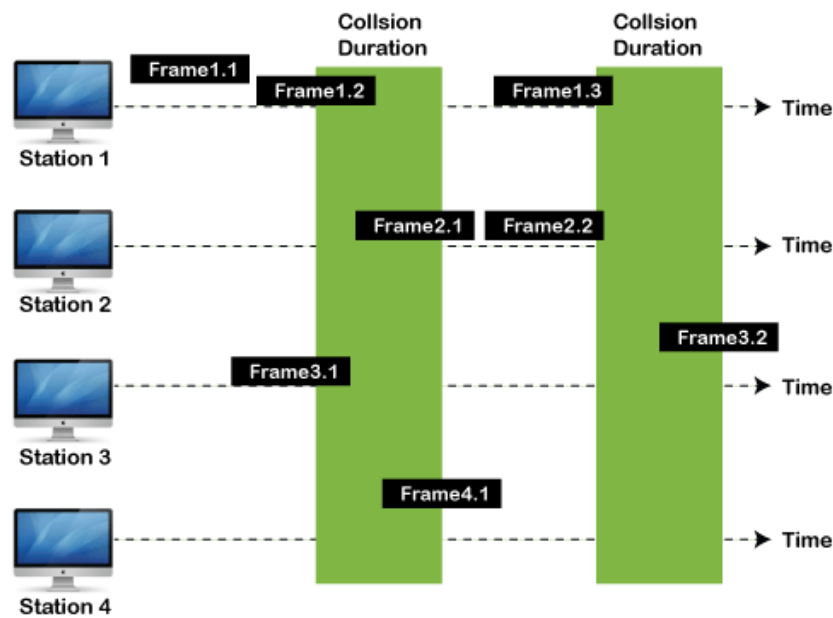
	<h1>Types of Sliding Window Protocol</h1> <p>Sliding window protocol has two types:</p> <ol style="list-style-type: none">1. Go-Back-N ARQ2. Selective Repeat ARQ			
11	<p>What are the functions of MAC?</p> <p>Functions of MAC Layer</p> <ul style="list-style-type: none">• It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.• It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.• It resolves the addressing of source station as well as the destination station, or groups of destination stations.• It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.• It also performs collision resolution and initiating retransmission in case of collisions.• It generates the frame check sequences and thus contributes to protection against transmission errors.	5		
12	<table><tr><td><p>Write short notes on Go-back N protocol.</p><p>Go-Back-N ARQ</p><ul style="list-style-type: none">• If a frame is corrupted or lost in it,all subsequent frames have to be sent again.• If it has a high error rate,it wastes a lot of bandwidth.• It is less complex.• It does not require sorting.• It does not require searching.</td><td><p>Selective Repeat ARQ</p><ul style="list-style-type: none">• In this, only the frame is sent again, which is corrupted or lost.• There is a loss of low bandwidth.• It is more complex because it has to do sorting and searching as well. And it also requires more storage.• In this, sorting is done to get the frames in the correct order.</td></tr></table>	<p>Write short notes on Go-back N protocol.</p> <p>Go-Back-N ARQ</p> <ul style="list-style-type: none">• If a frame is corrupted or lost in it,all subsequent frames have to be sent again.• If it has a high error rate,it wastes a lot of bandwidth.• It is less complex.• It does not require sorting.• It does not require searching.	<p>Selective Repeat ARQ</p> <ul style="list-style-type: none">• In this, only the frame is sent again, which is corrupted or lost.• There is a loss of low bandwidth.• It is more complex because it has to do sorting and searching as well. And it also requires more storage.• In this, sorting is done to get the frames in the correct order.	5
<p>Write short notes on Go-back N protocol.</p> <p>Go-Back-N ARQ</p> <ul style="list-style-type: none">• If a frame is corrupted or lost in it,all subsequent frames have to be sent again.• If it has a high error rate,it wastes a lot of bandwidth.• It is less complex.• It does not require sorting.• It does not require searching.	<p>Selective Repeat ARQ</p> <ul style="list-style-type: none">• In this, only the frame is sent again, which is corrupted or lost.• There is a loss of low bandwidth.• It is more complex because it has to do sorting and searching as well. And it also requires more storage.• In this, sorting is done to get the frames in the correct order.			

NOTES LINK -> ALL QUESTION BANK

	<ul style="list-style-type: none">• It is used more.	<ul style="list-style-type: none">• The search operation is performed in it.• It is used less because it is more complex.	
13	<p>Explain the concept of ALOHA.</p> <p>ALOHA Random Access Protocol</p> <p>It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.</p> <p>Aloha Rules</p> <ol style="list-style-type: none">1. Any station can transmit data to a channel at any time.2. It does not require any carrier sensing.3. Collision and data frames may be lost during the transmission of data through multiple stations.4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.5. It requires retransmission of data after some random amount of time.	5	
14	<p>Differentiate between Pure ALOHA and Slotted ALOHA.</p> <p>Pure Aloha</p> <p>Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a</p>	5	

random amount of time, called the backoff time (T_b). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

1. The total vulnerable time of pure Aloha is $2 * T_{fr}$.
2. Maximum throughput occurs when $G = 1/2$ that is 18.4%.
3. Successful transmission of data frame is $S = G * e^{-2G}$.



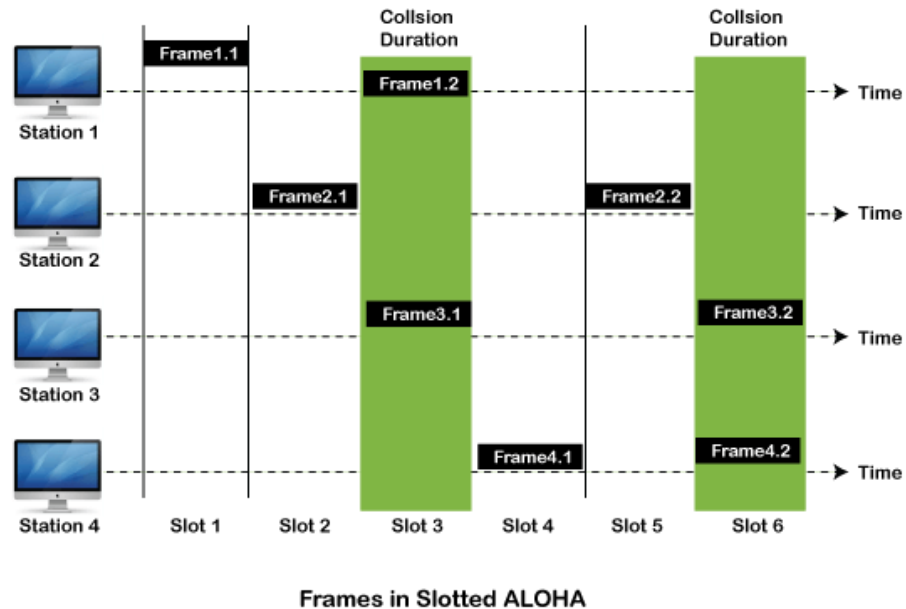
Frames in Pure ALOHA

Slotted Aloha

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

NOTES LINK -> ALL QUESTION BANK

1. Maximum throughput occurs in the slotted Aloha when $G = 1$ that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is $S = G * e^{-2G}$.
3. The total vulnerable time required in slotted Aloha is T_{fr} .



15

Explain (1) Repeater (2) Bridge (3) Router (4) Gateway

1. **Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting if original strength. It is a 2-port device.
2. **Bridge** – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

5

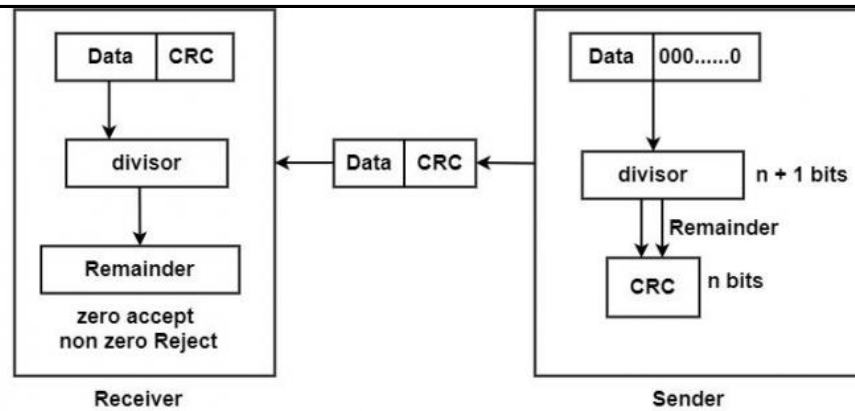
	<p>Types of Bridges</p> <p>a-Transparent Bridges:- These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.</p> <p>b-Source Routing Bridges:- In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.</p> <p>3.Routers – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.</p> <p>3. Gateway – A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.</p>	
16	<p>Explain different LAN transmission methods.</p> <p>LAN data transmissions fall into three classifications: unicast, multicast, and broadcast. In each type of transmission, a single packet is sent to one or more nodes.</p> <p>In a unicast transmission, a single packet is sent from the source to a destination on a network. First, the source node addresses the packet by using the address of the destination node. The package is then sent onto the network, and finally, the network passes the packet to its destination.</p>	5

	<p>A multicast transmission consists of a single data packet that is copied and sent to a specific subset of nodes on the network. First, the source node addresses the packet by using a multicast address. The packet is then sent into the network, which makes copies of the packet and sends a copy to each node that is part of the multicast address.</p> <p>A broadcast transmission consists of a single data packet that is copied and sent to all nodes on the network. In these types of transmissions, the source node addresses the packet by using the broadcast address. The packet is then sent on to the network, which makes copies of the packet and sends a copy to every node on the network.</p>	
17	Define the media access schemes used by LAN protocols.	5
18	<p>What is an error ? Explain the types of errors ?</p> <p>Errors</p> <p>When bits are transmitted over the computer network, they are subject to get corrupted due to interference and network problems. The corrupted bits lead to spurious data being received by the destination and are called errors.</p> <p>Types of Errors</p> <p>Errors can be of three types, namely single bit errors, multiple bit errors, and burst errors.</p> <ul style="list-style-type: none"> Single bit error – In the received frame, only one bit has been corrupted, i.e. either changed from 0 to 1 or from 1 to 0. <div style="border: 2px solid red; padding: 10px; margin: 10px 0;"> </div>	5

NOTES LINK -> ALL QUESTION BANK

	<ul style="list-style-type: none"> Multiple bits error – In the received frame, more than one bits are corrupted. <div style="border: 2px solid red; padding: 10px; margin: 10px 0;"> <div style="display: flex; justify-content: space-between;"> <div>Sent Frame</div> <div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">0</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">0</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">0</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">0</div> </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div>Received Frame</div> <div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">0</div> <div style="border: 1px solid black; padding: 2px; display: inline-block; background-color: #f8d7da;">1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block; background-color: #f8d7da;">0</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">0</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block; background-color: #f8d7da;">1</div> </div> </div> <div style="text-align: right; margin-top: 10px;">Multiple bits error</div> </div> Burst error – In the received frame, more than one consecutive bits are corrupted. <div style="border: 2px solid red; padding: 10px; margin: 10px 0;"> <div style="display: flex; justify-content: space-between;"> <div>Sent Frame</div> <div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">0</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">0</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">0</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">0</div> </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div>Received Frame</div> <div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">0</div> <div style="border: 1px solid black; padding: 2px; display: inline-block; background-color: #f8d7da;">1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block; background-color: #f8d7da;">0</div> <div style="border: 1px solid black; padding: 2px; display: inline-block; background-color: #f8d7da;">0</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">0</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">0</div> </div> </div> <div style="text-align: right; margin-top: 10px;">Burst error</div> </div> 	
19	<p style="color: red;">List any five Networking Connecting Devices with details.</p> <ul style="list-style-type: none"> • Hub • Switch • Router • Bridge • Gateway • Modem • Repeater • Access Point <p>Hubs connect multiple computer networking devices together. A hub also acts as a repeater in that it amplifies signals that deteriorate after traveling long distances over connecting cables. A hub is the simplest in the family of network connecting devices because it connects LAN components with identical protocols.</p> <p style="color: green;">Other discussed above (question-15)</p>	5
20	<p style="color: red;">What are the examples of LAN protocols?</p> <p><i>Ethernet:</i></p> <p>Ethernet was developed by Xerox in 1970s as a member of the IEEE 802.3 Standards. It was initially intended to be tested over coaxial cables,</p>	5

	<p>however, advanced protocols enabled Ethernet LAN to run over special twisted-pair cables or fiber optic cables.</p> <p><i>Token Ring Protocol:</i></p> <p>When the devices are connected in a ring or star topology, the Token Ring Protocol comes into play. This protocol protects the network from data collision, prevents any loss of data, or congestion in the transfer by the token system of data transfer. This protocol passes one or more tokens for a host to host connection between the devices.</p> <p><i>FDDI (Fiber Distributed Data Interface):</i></p> <p>FDDI protocol follows both ANSI and ISO standards which uses optic fiber for fast transmission of data. When copper is used instead of fiber for transmission of data, it is called CDDI (Copper Distribution Data Interface). This can cover up to 200 kilometers.</p>	
21	<p>Explain how errors are detected using CRC.</p> <p>The Cyclic Redundancy Checks (CRC) is the most powerful method for Error-Detection and Correction. It is given as a kbit message and the transmitter creates an $(n - k)$ bit sequence called frame check sequence. The out coming frame, including n bits, is precisely divisible by some fixed number. Modulo 2 Arithmetic is used in this binary addition with no carries, just like the XOR operation.</p> <p>Redundancy means duplicacy. The redundancy bits used by CRC are changed by splitting the data unit by a fixed divisor. The remainder is CRC.</p> <p>Qualities of CRC</p> <ul style="list-style-type: none">• It should have accurately one less bit than the divisor.• Joining it to the end of the data unit should create the resulting bit sequence precisely divisible by the divisor. <p>CRC generator and checker</p>	8



Process

- A string of n 0s is added to the data unit. The number n is one smaller than the number of bits in the fixed divisor.
- The new data unit is divided by a divisor utilizing a procedure known as binary division; the remainder appearing from the division is CRC.
- The CRC of n bits interpreted in phase 2 restores the added 0s at the end of the data unit

Example

Message D = 1010001101 (10 bits)

Predetermined P = 110101 (6 bits)

FCS R = to be calculated 5 bits

Hence, $n = 15$ $K = 10$ and $(n - k) = 5$

The message is generated through 2^5 :accommodating 1010001101000

The product is divided by P.

```

      1101010110 ← Q
110101 ) 101000110100000 (
        110101
        111011
        110101
        111010
        110101
        111110
        110101
        101100
        110101
        110010
        110101
        01110 ← R
    
```

NOTES LINK -> ALL QUESTION BANK

	<p>The remainder is inserted to 2^5D to provide $T = 101000110101110$ that is sent.</p> <p>Suppose that there are no errors, and the receiver gets T perfect. The received frame is divided by P.</p> <div><div><div>1101010110</div><div>110101) 101000110101110 (</div><div>110101</div><div>1110111</div><div>1101101</div><div>111010</div><div>110101</div><div>111110</div><div>110101</div><div>101100</div><div>110101</div><div>110101</div><div>110101</div><div>0 ← R</div></div></div> <p>Because of no remainder, there are no errors.</p>																													
22	<p>Discuss about a) GO BACK NARQ and b) Selective repeat ARQ.</p> <table><tr><td>S.N</td><td>Selective Repeat Protocol</td></tr><tr><td>O</td><td>Go-Back-N Protocol</td></tr><tr><td></td><td>In Go-Back-N Protocol, if the sent frame are find suspected then all the frames are re-transmitted from the lost packet to the last packet transmitted.</td></tr><tr><td>1.</td><td></td></tr><tr><td></td><td>Sender window size of Go-Back-N Protocol is N.</td></tr><tr><td>2.</td><td></td></tr><tr><td></td><td>Receiver window size of Go-Back-N Protocol is 1.</td></tr><tr><td>3.</td><td></td></tr><tr><td></td><td>Go-Back-N Protocol is less complex.</td></tr><tr><td>4.</td><td></td></tr><tr><td></td><td>In Go-Back-N Protocol, neither sender nor at receiver need sorting.</td></tr><tr><td>5.</td><td></td></tr><tr><td></td><td>In Go-Back-N Protocol, type of Acknowledgement is cumulative.</td></tr><tr><td>6.</td><td></td></tr></table>	S.N	Selective Repeat Protocol	O	Go-Back-N Protocol		In Go-Back-N Protocol, if the sent frame are find suspected then all the frames are re-transmitted from the lost packet to the last packet transmitted.	1.			Sender window size of Go-Back-N Protocol is N.	2.			Receiver window size of Go-Back-N Protocol is 1.	3.			Go-Back-N Protocol is less complex.	4.			In Go-Back-N Protocol, neither sender nor at receiver need sorting.	5.			In Go-Back-N Protocol, type of Acknowledgement is cumulative.	6.		8
S.N	Selective Repeat Protocol																													
O	Go-Back-N Protocol																													
	In Go-Back-N Protocol, if the sent frame are find suspected then all the frames are re-transmitted from the lost packet to the last packet transmitted.																													
1.																														
	Sender window size of Go-Back-N Protocol is N.																													
2.																														
	Receiver window size of Go-Back-N Protocol is 1.																													
3.																														
	Go-Back-N Protocol is less complex.																													
4.																														
	In Go-Back-N Protocol, neither sender nor at receiver need sorting.																													
5.																														
	In Go-Back-N Protocol, type of Acknowledgement is cumulative.																													
6.																														

	<p style="text-align: right;">individual.</p> <p>7. In Go-Back-N Protocol, Out-of-Order packets are NOT Accepted (discarded) and the entire window is re-transmitted.</p> <p>8. In Go-Back-N Protocol, if Receives a corrupt packet, then also, the entire window is re-transmitted. Efficiency of Go-Back-N Protocol is</p> <p>9. $N/(1+2*a)$</p> <p>In selective Repeat protocol, Out-of-Order packets are Accepted. In selective Repeat protocol, if Receives a corrupt packet, it immediately sends a negative acknowledgement and hence only the selective packet is retransmitted. Efficiency of selective Repeat protocol is also $N/(1+2*a)$</p>	
23	Explain Token passing protocol with its examples.	8
24	<p>Explain different error detection and correction mechanisms with examples.</p> <p>Types of Errors</p> <p>There may be three types of errors:</p> <ul style="list-style-type: none"> Single bit error <div style="display: flex; align-items: center; justify-content: center;"> <div style="text-align: center;"> <p>Sent</p> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1 0 1 1 0 0 1 1</div> </div> <div style="font-size: 2em; margin: 0 10px;">➡</div> <div style="text-align: center;"> <p>Received</p> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1 0 1 1 0 1 1 1</div> </div> </div> <p>In a frame, there is only one bit, anywhere though, which is corrupt.</p> <ul style="list-style-type: none"> Multiple bits error <div style="display: flex; align-items: center; justify-content: center;"> <div style="text-align: center;"> <p>Sent</p> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1 0 1 1 0 0 1 1</div> </div> <div style="font-size: 2em; margin: 0 10px;">➡</div> <div style="text-align: center;"> <p>Received</p> <div style="border: 1px solid black; padding: 2px; display: inline-block;">1 0 1 0 0 1 1 1</div> </div> </div> <p>Frame is received with more than one bits in corrupted state.</p> <ul style="list-style-type: none"> Burst error 	8



Frame contains more than 1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

Error Detection

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver's end fails, the bits are considered corrupted.

Parity Check

One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity.

The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even. If the number of 1s is odd, to make it even a bit with value 1 is added.



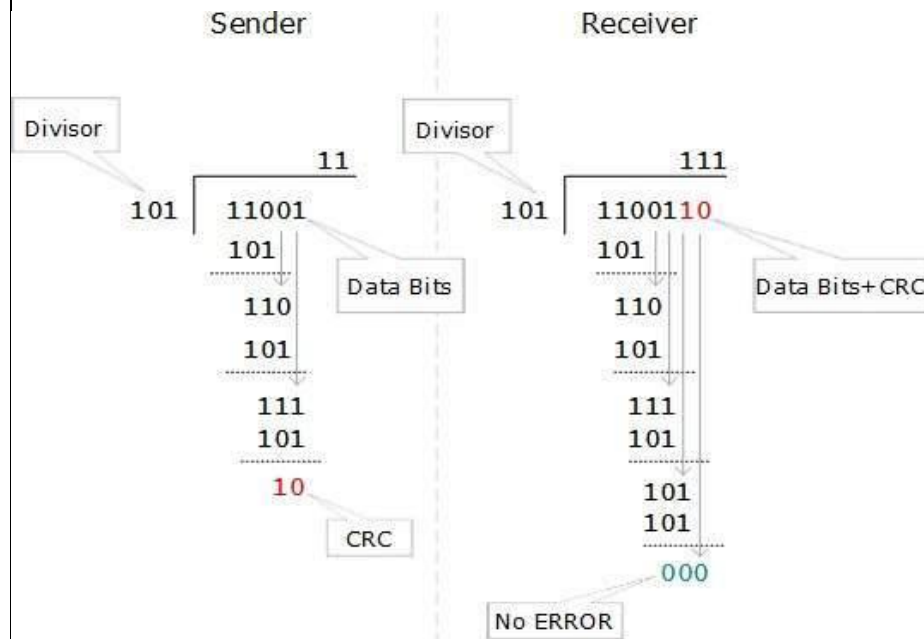
The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But when more than one bits are erroneous, then it is very hard for the receiver to detect the error.

Cyclic Redundancy Check (CRC)

CRC is a different approach to detect if the received frame contains

valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.



At the other end, the receiver performs division operation on codewords using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occurred in transit.

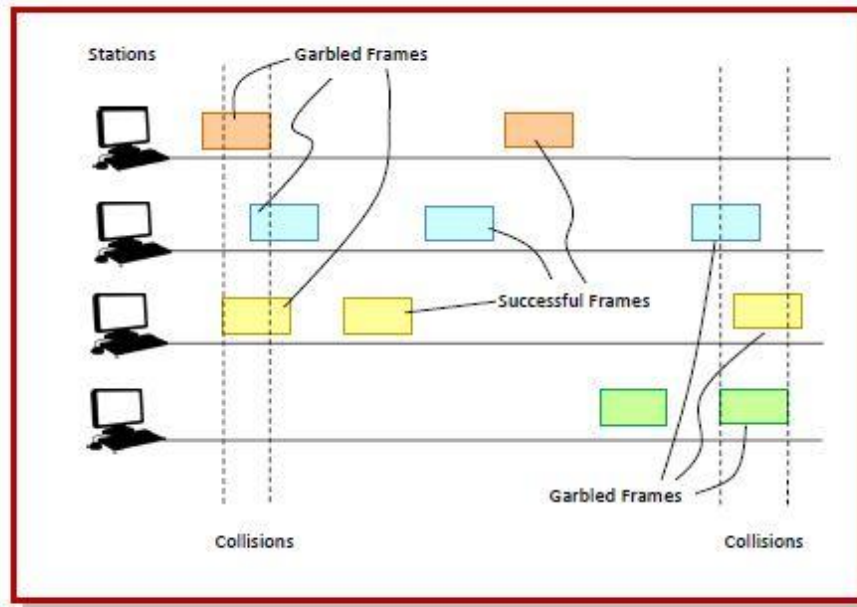
Error Correction

In the digital world, error correction can be done in two ways:

- **Backward Error Correction** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
- **Forward Error Correction** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

	<p>The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.</p> <p>To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection. For example, we take ASCII words (7 bits data), then there could be 8 kind of information we need: first seven bits to tell us which bit is error and one more bit to tell that there is no error.</p> <p>For m data bits, r redundant bits are used. r bits can provide 2^r combinations of information. In m+r bit codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about m+r bit locations plus no-error information, i.e. m+r+1.</p> <p>$2^r \geq m+r+1$</p>	
25	<p>What is ALOHA? Explain its different types.</p> <p>ALOHA is a medium access control (MAC) protocol for transmission of data via a shared network channel. Using this protocol, several data streams originating from multiple nodes are transferred through a multi-point transmission channel. There are two types of ALOHA protocols – Pure ALOHA and Slotted ALOHA.</p> <p>In pure ALOHA, the time of transmission is continuous. Whenever a station has an available frame, it sends the frame. If there is collision and the frame is destroyed, the sender waits for a random amount of time before retransmitting it.</p> <p>Working Principle</p> <p>After transmitting a frame, a station waits for a finite period of time to receive an acknowledgement. If the acknowledgement is not received within this time, the station assumes that the frame has been destroyed due to collision and resends the frame.</p> <p>A collision occurs if more than one frame tries to occupy the channel at the same time. The situation is depicted in the following</p>	8

diagram-

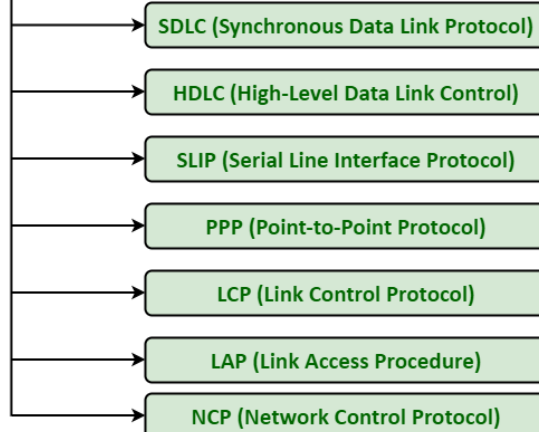


26

Explain the protocols in Data link layer .

8

Data Link Protocols



1. [Synchronous Data Link Protocol \(SDLC\)](#) – SDLC is basically a communication protocol of computer. It usually supports multipoint links even

NOTES LINK ->ALL QUESTION BANK

error recovery or error correction also. It is usually used to carry SNA (Systems Network Architecture) traffic and is present precursor to HDLC. It is also designed and developed by IBM in 1975. It is also used to connect all of the remote devices to mainframe computers at central locations may be in point-to-point (one-to-one) or point-to-multipoint (one-to-many) connections. It is also used to make sure that the data units should arrive correctly and with right flow from one network point to next network point.

2. [High-Level Data Link Protocol \(HDLC\)](#) – HDLC is basically a protocol that is now assumed to be an umbrella under which many Wide Area protocols sit. It is also adopted as a part of X.25 network. It was originally created and developed by ISO in 1979. This protocol is generally based on SDLC. It also provides best-effort unreliable service and also reliable service. HDLC is a bit-oriented protocol that is applicable for point-to-point and multipoint communications both.
3. [Serial Line Interface Protocol \(SLIP\)](#) – SLIP is generally an older protocol that is just used to add a framing byte at end of IP packet. It is basically a data link control facility that is required for transferring IP packets usually among Internet Service Providers (ISP) and a home user over a dial-up link. It is an encapsulation of the TCP/IP especially designed to work with over serial ports and several router connections simply for communication. It is some limitations like it does not provide mechanisms such as error correction or error detection.
4. [Point to Point Protocol \(PPP\)](#) – PPP is a protocol that is basically used to provide same functionality as SLIP. It is most robust protocol that is used to transport other types of packets also along with IP Packets. It can also be required for dial-up and leased router-router lines. It basically

provides framing method to describe frames. It is a character-oriented protocol that is also used for error detection. It is also used to provides two protocols i.e. NCP and LCP. LCP is used for bringing lines up, negotiation of options, bringing them down whereas NCP is used for negotiating network-layer protocols. It is required for same serial interfaces like that of HDLC.

5. Link Control Protocol (LCP) –

It was originally developed and created by IEEE 802.2. It is also used to provide HDLC style services on LAN (Local Area Network). LCP is basically a PPP protocol that is used for establishing, configuring, testing, maintenance, and ending or terminating links for transmission of data frames.

6. Link Access Procedure (LAP) –

LAP protocols are basically a data link layer protocols that are required for framing and transferring data across point-to-point links. It also includes some reliability service features. There are basically three types of LAP i.e. LAPB (Link Access Procedure Balanced), LAPD (Link Access Procedure D-Channel), and LAPF (Link Access Procedure Frame-Mode Bearer Services). It is actually originated from IBM SDLC, which is being submitted by IBM to the ISP simply for standardization.

7. Network Control Protocol (NCP) –

NCP was also an older protocol that was implemented by ARPANET. It basically allows users to have access to use computers and some of the devices at remote locations and also to transfer files among two or more computers. It is generally a set of protocols that is forming a part of PPP. NCP is always available for each and every higher-layer protocol that is supported by PPP. NCP was replaced by TCP/IP in the 1980s.

NOTES LINK -> ALL QUESTION BANK

27

Define Hamming Code? What is the 7 bit Hamming code for 1101?

Hamming code is a set of error-correction codes that can be used to **detect and correct the errors** that can occur when the data is moved or stored from the sender to the receiver. It is a **technique developed by R.W. Hamming for error correction. Redundant bits** – Redundant bits are extra binary bits that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer. The number of redundant bits can be calculated using the following formula:

$$2^r \geq m + r + 1$$

where, r = redundant bit, m = data bit

Hamming (7, 4) code: It is a linear error-correcting code that encodes four bits of data into seven bits, by adding three parity bits.

Example: It is used in the Bell-Telephone laboratory, error-prone punch card reader to detect the error and correct them.

Hamming code:

Bits #	1	2	3	4	5	6	7
Transmitted bits	P_1	P_2	d_1	P_3	d_2	d_3	d_4

$$P_1 = d_1 \oplus d_2 \oplus d_4$$

$$P_2 = d_1 \oplus d_4 \oplus d_3$$

$$P_3 = d_2 \oplus d_4 \oplus d_3$$

Solution:

Given data 1101 i.e.

$$d_1 = 1, d_2 = 1, d_3 = 0, d_4 = 1$$

We can write:

$$P_1 = d_1 \oplus d_2 \oplus d_4 = 1 \oplus 1 \oplus 1 = 1$$

8

NOTES LINK -> ALL QUESTION BANK

	$P_2 = d_1 \oplus d_4 \oplus d_3 = 1 \oplus 1 \oplus 0 = 0$ $P_3 = d_2 \oplus d_4 \oplus d_3 = 1 \oplus 1 \oplus 0 = 0$ <p>Then transmitted final code is</p> <table border="1"><tr><td>P_1</td><td>P_2</td><td>d_1</td><td>P_3</td><td>d_2</td><td>d_3</td><td>d_4</td></tr><tr><td>1</td><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td><td>1</td></tr></table> <p>i.e. 1010101</p>	P_1	P_2	d_1	P_3	d_2	d_3	d_4	1	0	1	0	1	0	1	
P_1	P_2	d_1	P_3	d_2	d_3	d_4										
1	0	1	0	1	0	1										
28	Explain the process of error detection using checksum along with an example.	8														
29	Calculate the Cyclic Redundancy Code(CRC) for data word: 110010101 with Generator = 10101 then n=5	8														
30	Explain various IEEE standards for LAN protocols. IEEE standards in computer networks	Description														

- IEEE 802 It is used for the overview and architecture of LAN/MAN.
- IEEE 802.1 It is used for bridging and management of LAN/MAN.
- IEEE 802.1s It is used in multiple spanning trees.
- IEEE 802.1w It is used for rapid reconfiguration of spanning trees.
- IEEE 802.1x It is used for network access control of ports.
- IEEE 802.2 It is used in Logical Link Control (LLC).
- IEEE 802.3 It is used in Ethernet (CSMA/CD access method).
- IEEE 802.3ae It is used for 10 Gigabit Ethernet.
- IEEE 802.4 It is used for token passing bus access methods and the physical layer specifications.
- IEEE 802.5 It is used for token ring access methods and the physical layer specifications.
- IEEE 802.6 It is used in distributed Queue Dual Bus (DQDB) access method and for the physical layer specifications.
- IEEE 802.7 It is used in broadband LAN.
- IEEE 802.8 It is used in fiber optics.
- IEEE 802.9 It is used in isochronous LANs.
- IEEE 802.10 It is used in interoperable LAN/MAN security.
- IEEE 802.11 It is used in wireless LAN, MAC, and Physical layer specifications.
- IEEE 802.12 It is used in the demand-priority access method, in the physical layer, and in repeater specifications.
- IEEE 802.13 It is not used.
- IEEE 802.14 It is used in cable modems (not used now).

NOTES LINK ->ALL QUESTION BANK

IEEE 802.15 It is used in WPAN (Wireless Personal Area Network).

IEEE 802.16 It is used in Wireless MAN (Wireless Metropolitan Area Network).

IEEE 802.17 It is used in RPR access (Resilient Packet Ring).

NOTES LINK -> ALL QUESTION BANK

Unit 4: Network and Transport Layer

Ques. No.	Question	Marks
1	What is IP address? An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.	2
2	Define Congestion Control? What is congestion ? A state occurring in network layer when the message traffic is so heavy that it slows down network response time. Effects of Congestion <ul style="list-style-type: none">• As delay increases, performance decreases.• If delay increases, retransmission occurs, making situation worse. Congestion control algorithms <ul style="list-style-type: none">• Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse.• Congestive-Avoidance Algorithms (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network.• There are two congestion control algorithm which are as follows:	2
3	What are the responsibilities of network layer? Network layer is the third layer in the OSI model of computer networks. It's main function is to transfer network packets from the source to the destination. It is involved both at the source host and the destination host. At the source, it accepts a packet from the transport layer, encapsulates it in a datagram and then deliver the packet to the data link layer so that it can further be sent to the receiver. At the destination, the datagram is decapsulated, the packet is extracted and delivered to the corresponding transport layer.	2
4	Differentiate between IPv4 and IPv6. IPv4 has a 32-bit address length IPv6 has a 128-bit address length	2

NOTES LINK -> ALL QUESTION BANK

	<p>It Supports Manual and DHCP address configuration</p> <p>In IPv4 end to end, connection integrity is Unachievable</p> <p>It can generate 4.29×10^9 address space</p>	<p>It supports Auto and renumbering address configuration</p> <p>In IPv6 end to end, connection integrity is Achievable</p> <p>Address space of IPv6 is quite large it can produce 3.4×10^{38} address space</p>	
5	<p>What allows TCP to detect lost segments?</p> <p>Acknowledgment number Best explanation: TCP header contains separate fields for sequence number and acknowledgment number. Comparing these values is what allows TCP to detect lost segments and in turn recover from that loss. After detecting the lost segments, the recovery may require retransmission of the lost segments of data. Read more on Sarthaks.com - https://www.sarthaks.com/2447165/what-allows-tcp-to-detect-lost-segments-and-in-turn-recover-from-that-loss</p>	2	
6	<p>Which transport layer feature is used to establish a connection-oriented session?</p> <p>TCP</p> <p>In terms of the OSI model, TCP is a transport-layer protocol. It provides a connection-oriented data transmission service between applications, that is, a connection is established before data transmission begins.</p>	2	
7	<p>What is Remote Procedure Call?</p> <p>A remote procedure call is an interprocess communication technique that is used for client-server based applications. It is also known as a subroutine call or a function call.</p>	2	
8	<p>Which transport protocol is used by remote procedure call (RPC)?</p> <p>The remote procedure calls are defined through routines contained in the RPC protocol. Each call message is matched with a reply message. The RPC protocol is a message-passing protocol that implements other non-RPC protocols such as batching and broadcasting remote calls.</p>	2	
9	What affects TCP window size?	2	
10	Why do we need window management for TCP?	2	
11	Difference between public and private IP addresses?	5	

NOTES LINK ->ALL QUESTION BANK

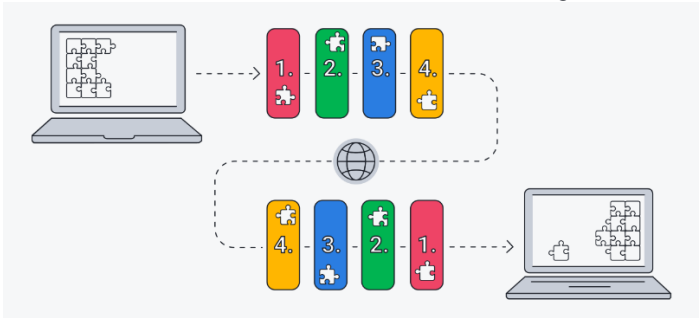
S.No.	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
1.	The scope of Private IP is local.	The scope of Public IP is global.
2.	It is used to communicate within the network.	It is used to communicate outside the network.
3.	Private IP addresses of the systems connected in a network differ in a uniform manner.	Public IP may differ in a uniform or non-uniform manner.
4.	It works only on LAN.	It is used to get internet service.
5.	It is used to load the network operating system.	It is controlled by ISP.
6.	It is available free of cost.	It is not free of cost.
7.	Private IP can be known by entering "ipconfig" on the command prompt.	Public IP can be known by searching "what is my ip" on google.
8.	Range: 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0 - 192.168.255.255 Example: 192.168.1.10	Range: Besides private IP addresses, the rest are public. Example: 17.5.7.8
9.	Private IP uses numeric code that is not unique and can be used again	Public IP uses a numeric code that is unique and cannot be used by other

NOTES LINK -> ALL QUESTION BANK

- | | | |
|-----|--|--|
| 10. | Private IP addresses are secure | Public IP address has no security and is subjected to attack |
| 11. | Private IP addresses require NAT to communicate with devices | Public IP does not require a network translation |

12	<p>What is the sequence of events during remote procedure call?</p> <p>Remote procedure call (RPC): inter-process communication, allows a program to execute a procedure on another computer. Programmers write the same code no matter the procedure is local or remote.</p> <pre>sequenceDiagram participant Client participant Server Note over Client: Call remote procedure Client->>Server: Request Note over Server: Call local procedure and return results Server->>Client: Reply Note over Client: Return from call Note over Client: Wait for result</pre> <p>The diagram illustrates the sequence of events during a Remote Procedure Call (RPC). It shows two horizontal timelines: one for the Client and one for the Server. The Client timeline starts with a solid line, then a dashed line labeled 'Wait for result', and then another solid line. The Server timeline starts with a dashed line, then a solid line labeled 'Call local procedure and return results', and then another dashed line. Arrows indicate the flow of messages: 'Call remote procedure' (Client to Server), 'Request' (Client to Server), 'Reply' (Server to Client), and 'Return from call' (Server to Client). A 'Time' arrow points to the right at the bottom.</p> <ol style="list-style-type: none">1. Client procedure calls client stub in normal way2. Client stub builds message, calls local OS3. Client's OS sends message to remote OS4. Remote OS gives message to server stub5. Server stub unpacks parameters, calls server6. Server does work, returns result to the stub7. Server stub packs it in message, calls local OS8. Server's OS sends message to client's OS9. Client's OS gives message to client stub10. Client stub unpacks result, returns to client	5
13	<p>Write down features of TCP?</p> <p>Features</p>	5

NOTES LINK -> ALL QUESTION BANK

	<ul style="list-style-type: none"> • TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it. • TCP ensures that the data reaches intended destination in the same order it was sent. • TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data. • TCP provides error-checking and recovery mechanism. • TCP provides end-to-end communication. • TCP provides flow control and quality of service. • TCP operates in Client/Server point-to-point mode. • TCP provides full duplex server, i.e. it can perform roles of both receiver and sender. 	
14	<p>What is TCP/IP? How does it work?</p> <p>TCP/IP is a data link protocol used on the internet to let computers and other devices send and receive data. TCP/IP stands for Transmission Control Protocol/Internet Protocol and makes it possible for devices connected to the internet to communicate with one another across networks.</p> <p>Whenever you send something over the internet — a message, a photo, a file — the TCP/IP model divides that data into packets according to a four-layer procedure. The data first goes through these layers in one order, and then in reverse order as the data is reassembled on the receiving end.</p>  <p><i>A diagram of how the TCP/IP model divides data into packets and sends it through 4 different layers.</i></p> <p>The TCP/IP model works because the whole process is standardized.</p> <p>Without standardization, communication would go haywire and slow things</p>	5

NOTES LINK -> ALL QUESTION BANK

	down – and fast internet service relies on efficiency. As the global standard, the TCP/IP model is one of the most efficient ways to transfer data over the internet.	
15	<p>Why remote procedure call (RPC) doesn't fit in OSI model?</p> <p>The main goal of RPC is to hide the existence of the network from a program. As a result, RPC doesn't quite fit into the OSI model:</p> <ol style="list-style-type: none"> 1. The message-passing nature of network communication is hidden from the user. The user doesn't first open a connection, read and write data, and then close the connection. Indeed, a client often doesn't even know they are using the network! 2. RPC often omits many of the protocol layers to improve performance. Even a small performance improvement is important because a program may invoke RPCs often. For example, on (diskless) Sun workstations, every file access is made via an RPC. <p>The principal objective of RPC is to conceal the presence of the system from a program. Thus, RPC doesn't exactly fit <u>into the OSI model</u>.</p>	5
16	<p>What is transport layer? Explain in brief.</p> <p>The transport layer is the fourth layer in the open systems interconnection (<u>OSI</u>) network model.</p> <p>The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. Each of the seven OSI layers is assigned a task or group of tasks.</p> <p>The transport layer's tasks include error correction as well as segmenting and desegmenting data before and after it's transported across the network. This layer is also responsible for <u>flow control</u> and making sure that segmented data is delivered over the network in the correct sequence.</p> <p>Layer 4 (the transport layer) uses the transmission control protocol (<u>TCP</u>) & user data protocol (<u>UDP</u>) to carry out its tasks.</p> <p>The services provided by the transport layer protocols can be</p>	5

NOTES LINK -> ALL QUESTION BANK

divided into five categories:

End-to-end delivery

Addressing

Reliable delivery

Flow control

Multiplexing

17

Differentiate between TCP and IP.

	TCP	IP
Definition	TCP provides the service of exchanging data between applications	IP handles addressing and routing messages to the computers across one or more networks
Connection	Connection Oriented	Connection less method
location	Transport	Internet
Reliability	Reliable	Unreliable
Transfer	Segments to internet layer	Datagrams to physical level
Flow control	Yes	No
Format	TCP segments have a 20 byte header with >= 0 bytes of data	IP datagrams contain a message, or one fragment of a message, that may be up to 65,535 bytes (octets) in length

5

18

Explain the difference between Static and Dynamic IP?

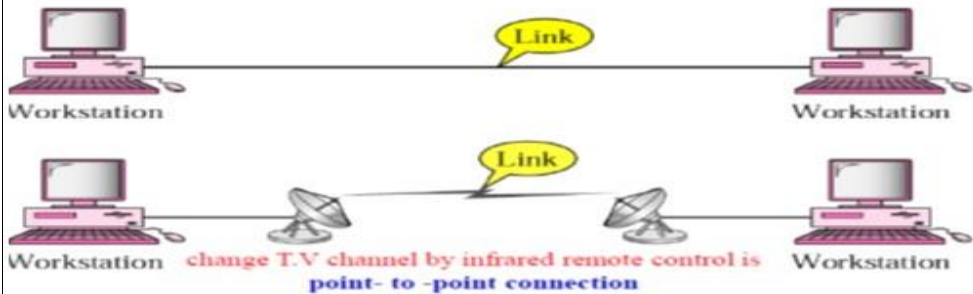
	Static IP Address	Dynamic IP address
S.NO		

5

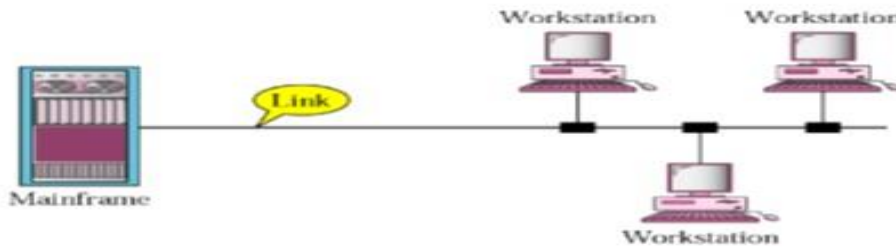
NOTES LINK -> ALL QUESTION BANK

	1.	It is provided by ISP(Internet Service Provider).	While it is provided by DHCP (Dynamic Host Configuration Protocol).	
	2.	Static ip address does not change any time, it means if a static ip address is provided then it can't be changed or modified.	While dynamic ip address change any time.	
	3.	Static ip address is less secure.	While in dynamic ip address, there is low amount of risk than static ip address's risk.	
	4.	Static ip address is difficult to designate.	While dynamic ip address is easy to designate.	
	5.	The device designed by static ip address can be trace.	But the device designed by dynamic ip address can't be trace.	
	6.	Static ip address is more stable than dynamic ip address.	While dynamic ip address is less stable than static ip address.	
	7.	The cost to maintain the static ip address is higher than dynamic ip address.	While the maintaining cost of dynamic ip address is less than static ip address.	
	-	

NOTES LINK -> ALL QUESTION BANK

	<p>computational data is less confidential.</p> <p>where data is more confidential and needs more security.</p>	
19	<p>What is connection? Explain its types.</p> <p>A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For communication to occur, two devices must be connected in some way to the same link at the same time.</p> <p>There are two possible types of connections: point-to-point and multipoint.</p> <p>1.Point-to-Point:</p> <p>A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible which are shown in the following figure.</p>  <p>2.Multipoint:</p> <p>A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link as</p>	5

shown in the following figure.



In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

20

Explain the header format of TCP.

TCP wraps each data packet with a header containing 10 mandatory fields totaling 20 bytes (or octets). Each header holds information about the connection and the current data being sent.

The 10 TCP header fields are as follows:

1. **Source port** – The sending device's port.
2. **Destination port** – The receiving device's port.
3. **Sequence number** – A device initiating a TCP connection must choose a random initial sequence number, which is then incremented according to the number of transmitted bytes.
4. **Acknowledgment number** – The receiving device maintains an acknowledgment number starting with zero. It increments this number according to the number of bytes received.
5. **TCP data offset** – This specifies the size of the TCP header, expressed in 32-bit words. One word represents four bytes.

5

	<p>6. Reserved data – The reserved field is always set to zero.</p> <p>7. Control flags – TCP uses nine control flags to manage data flow in specific situations, such as the initiating of a reset.</p> <p>8. Window size TCP checksum – The sender generates a checksum and transmits it in every packet header. The receiving device can use the checksum to check for errors in the received header and payload.</p> <p>9. Urgent pointer – If URG control flag is set, this value indicates an offset from the sequence number, indicating the last urgent data byte.</p> <p>10. mTCP optional data – These are optional fields for setting maximum segment sizes, selective acknowledgments and enabling window scaling for more efficient use of high-bandwidth networks.</p>							
21	<p>Explain Data Compression and its types.</p> <p>Data Compression is also referred to as bit-rate reduction or source coding. This technique is used to reduce the size of large files.</p> <p>The advantage of data compression is that it helps us save our disk space and time in the data transmission.</p> <p>There are mainly two types of data compression techniques -</p> <ol style="list-style-type: none"> 1. Lossless Data Compression 2. Lossy Data Compression <table border="1" style="width: 100%; margin-top: 10px;"> <thead> <tr> <th style="width: 15%;">S.No</th> <th style="width: 40%;">Lossless data compression</th> <th style="width: 45%;">Lossy data compression</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>	S.No	Lossless data compression	Lossy data compression				8
S.No	Lossless data compression	Lossy data compression						

NOTES LINK -> ALL QUESTION BANK

	1.	In Lossless data compression, there is no loss of any data and quality.	In Lossy data compression, there is a loss of quality and data, which is not measurable.	
	2.	In lossless, the file is restored in its original form.	In Lossy, the file does not restore in its original form.	
	3.	Lossless data compression algorithms are Run Length Encoding, Huffman encoding, Shannon fano encoding, Arithmetic encoding, Lempel Ziv Welch encoding, etc.	Lossy data compression algorithms are: Transform coding, Discrete Cosine Transform, Discrete Wavelet Transform, fractal compression, etc.	
	4.	Lossless compression is mainly used to compress text-sound and images.	Lossy compression is mainly used to compress audio, video, and images.	
	5.	As compare to lossy data compression, lossless data compression holds more data.	As compare to lossless data compression, lossy data compression holds less data.	
	6.	File quality is high in the lossless data compression.	File quality is low in the lossy data compression.	
	7.	Lossless data compression mainly supports RAW, BMP, PNG, WAV, FLAC, and ALAC file types.	Lossy data compression mainly supports JPEG, GIF, MP3, MP4, MKV, and OGG file types.	
22	What is cryptography? Distinguish between symmetric and asymmetric key cryptography. <u>Cryptography</u> is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing".			8

NOTES LINK -> ALL QUESTION BANK

--	--	--

Symmetric Key Encryption

It only requires a single key for both encryption and decryption.

The size of cipher text is the same or smaller than the original plain text.

The encryption process is very fast.

It is used when a large amount of data is required to transfer.

It only provides confidentiality.

The length of key used is 128 or 256 bits

In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.

It is efficient as it is used for handling large amount of data.

Security is less as only one key is used for both encryption and decryption purpose.

The Mathematical Representation is as follows-

$$P = D(K, E(P))$$

where K → encryption and decryption

Asymmetric Key Encryption

It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.

The size of cipher text is the same or larger than the original plain text.

The encryption process is slow.

It is used to transfer small amounts of data.

It provides confidentiality, authenticity, and non-repudiation.

The length of key used is 2048 or higher

In asymmetric key encryption, resource utilization is high.

It is comparatively less efficient as it can handle a small amount of data.

It is more secure as two keys are used here- one for encryption and the other for decryption.

The Mathematical Representation is as follows-

$$P = D(K_d, E(K_e, P))$$

where K_e → encryption key

NOTES LINK -> ALL QUESTION BANK

<p>key</p> <p>P → plain text</p> <p>D → Decryption</p> <p>E(P) → Encryption of plain text</p>	<p>Kd → decryption key</p> <p>D → Decryption</p> <p>E(K_e, P) → Encryption of plain text using encryption key K_e . P → plain text</p>
---	--

23	<p style="color: red;">Which mechanism is used for connection establishment?</p> <p>Connection establishment</p> <p>To establish a connection, TCP uses a three-way handshake. Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections: this is called a passive open. Once the passive open is established, a client may initiate an active open. To establish a connection, the three-way (or 3-step) handshake occurs:</p> <ol style="list-style-type: none"> 1. SYN: The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value A. 2. SYN-ACK: In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number (A + 1), and the sequence number that the server chooses for the packet is another random number, B. 3. ACK: Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e. A + 1, and the acknowledgement number is set to one more than the received sequence number i.e. B + 1. <p>At this point, both the client and server have received an acknowledgment of the connection. The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged. With these, a full-duplex communication is established.</p>	8
24	<p style="color: red;">Discuss TCP-Window Management System?</p>	8

NOTES LINK -> ALL QUESTION BANK

Windowing and Window Size: Window management in TCP is an important concept that ensures reliability in packet delivery as well as reduce the wastage of time in waiting for the acknowledge after each packet.

Window size: window size determines the amount of data that you can transmit before receiving an acknowledgment. Sliding window refers to the fact that the window size is negotiated dynamically during the TCP session.

1. Expectational acknowledgment means that the acknowledgment number refers to the octet that is next expected
2. If the source receives no acknowledgment, it knows to retransmit at a slower rate.

The mechanism of the sliding window style may be understood easily with the help of below given diagrams:

fig-1

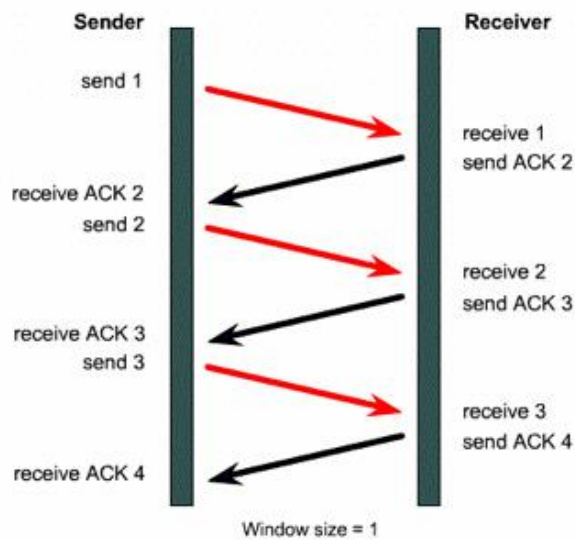
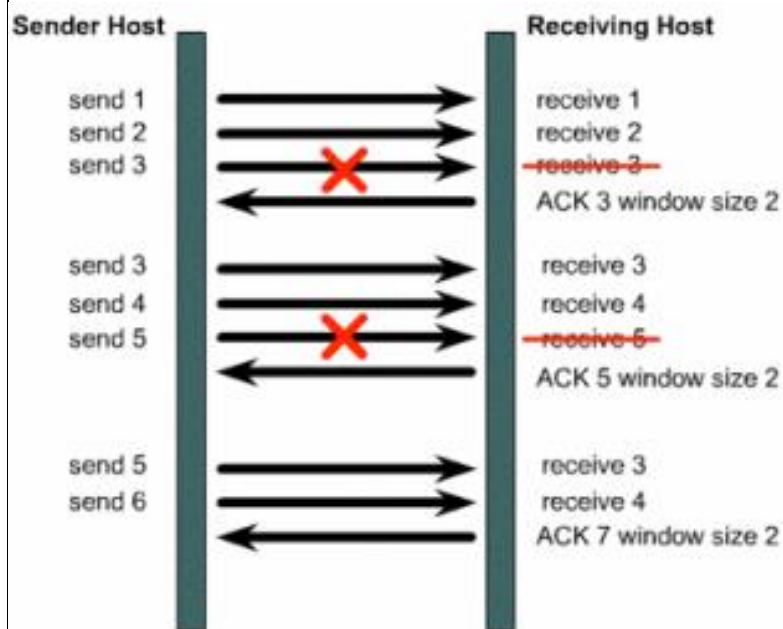
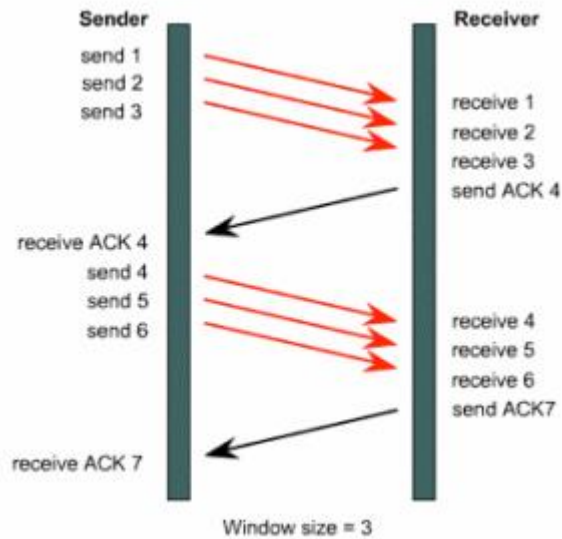
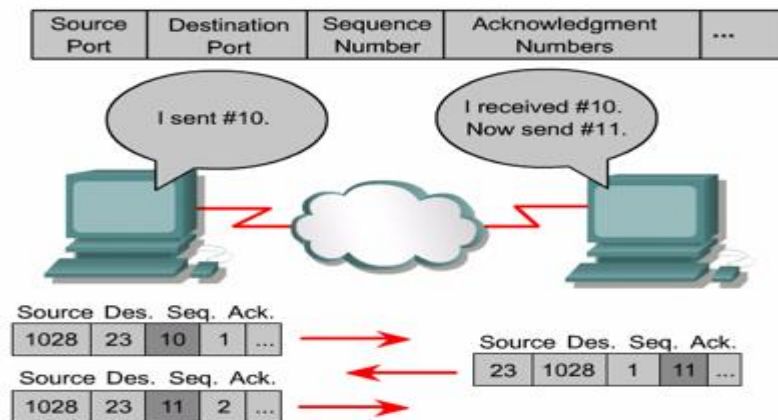


Fig-2





25

What are the various design issues in Transport and Session layers?

8

Design Issues with Session Layer :

1. **Establish sessions between machines –**
 The establishment of session between machines is an important service provided by session layer. This session is responsible for creating a dialog between connected machines. The Session Layer provides mechanism for opening, closing and managing a session between end-user application processes, i.e. a semi-permanent dialogue. This session consists of requests and responses that occur between applications.
2. **Enhanced Services –**
 Certain services such as checkpoints and management of tokens are the key features of session layer and thus it becomes necessary to keep enhancing these features during the layer's design.
3. **To help in Token management and Synchronization –**
 The session layer plays an important role in preventing collision of several critical operation as well as ensuring better data transfer over network by

	<p>establishing synchronization points at specific intervals. Thus it becomes highly important to ensure proper execution of these services.</p> <p>Design Issues with Transport Layer</p> <ul style="list-style-type: none">• Accepting data from Session layer, split it into segments and send to the network layer.• Ensure correct delivery of data with efficiency.• Isolate upper layers from the technological changes.• Error control and flow control.	
26	<p>What are issues and solutions related to TCP in networks?</p> <p>Some the issues and solution related to Transmission Control Protocol (TCP) are as follows –</p> <ul style="list-style-type: none">• Silly window syndrome.• Congestion window management. <p>Silly Window Syndrome</p> <p>This is a problem which arises in TCP flow control. In this the sender window size shrinks to an extremely low value due that the data being sent in each trip is even smaller than the TCP header. Due to which TCP protocol becomes extremely inefficient.</p> <p>Causes</p> <p>The silly window syndrome can occur due to two main reasons, which are as follows –</p> <ul style="list-style-type: none">• The application which needs to send the data produces a short amount of data (1 byte), again and again and	8

the TCP protocol is implemented in such a way that it sends the data as soon as received.

The solution to this is keeping a buffer at the sender end and storing data in it while it's generating and after sufficient data is generated or a time limit is reached (usually a Round Trip Time) then the next data packet will be sent. This is called Nagle's algorithm.

- Another cause can be the receiver can process very low amounts of data, so keep sending updates to decrease the window size to the sender.

The solution to this is the receiver should not send updates to the sender to decrease the window size beyond a certain limit. It must wait for some time limit till it has decent space and then send the update for window size. This is called Clark's algorithm.

Congestion Window Management

This is a method of changing the sender window size based on the network traffic. In this, the window size is initially set to 1 and then increased based on the following phases –

Phase 1 Slow Start

In this phase the size of the window is increased exponentially, that is, the window size doubles for every RTT. This phase is continued till a threshold window size is reached.

Phase 2 Congestion Avoidance

In this phase the window size is increased additively, i.e. the window size is increased by 1 for every RTT. It continues till Congestion is discovered.

Phase 3 Congestion Detection

It occurs when congestion is detected, i.e. a packet was resent. It can be due to 1 of the two reasons given below –

- **Timeout** – In this case, the threshold is reduced to half of current window size and the window size is decreased to 1 and again Phase 1 is started.

NOTES LINK ->ALL QUESTION BANK

	<ul style="list-style-type: none">• Acknowledgement Duplicates – In this case the threshold is reduced to half of current window size and the window size is decreased to the threshold value and again Phase 2 is started.	
27	<p>Explain the concept of Remote Procedure Calls in computer networks.</p> <p>A remote procedure call is an interprocess communication technique that is used for client-server based applications. It is also known as a subroutine call or a function call.</p> <p>A client has a request message that the RPC translates and sends to the server. This request may be a procedure or a function call to a remote server. When the server receives the request, it sends the required response back to the client. The client is blocked while the server is processing the call and only resumed execution after the server is finished.</p> <p>The sequence of events in a remote procedure call are given as follows –</p> <ul style="list-style-type: none">• The client stub is called by the client.• The client stub makes a system call to send the message to the server and puts the parameters in the message.• The message is sent from the client to the server by the client's operating system.• The message is passed to the server stub by the server operating system.• The parameters are removed from the message by the server stub.• Then, the server procedure is called by the server stub. <p>A diagram that demonstrates this is as follows –</p>	8

NOTES LINK -> ALL QUESTION BANK

