Chapter : 1

Computer Network

(1) Explain Computer Network.

→ It is a set of interconnected autonomous systems that facilities distributed processing of information. It results in better perfomance with high speed of processing.

* Advantage

- Central storage of data : File can be stored on centeral node that can be avalaible to every user
- Faster Problem Solving : An explicit issue can be settled in lesser time.
- Reliability : It implies backing up information. Due to some reason equipment crashes So we can't access data on that PC, another duplicat similar information is accessible on another computer.
- It is highly flexible.
- Security through authorization.
- Boost storage capacity.

* Disadvantage

- It lacks robustness.
- It lacks Independence.
- Virus and malware.
- Cost of the network.

(2) Differentiate LAN, MAN and WAN

LAN	MAN	WAN
• Local area network.	Matropolitan area network.	Wide area network.
• Operates in small area. Such as campus	Operates in large areas. Such as city.	Operates in larger area such as country.
• Ownership is private.	Ownership can be public or private.	It can't owned by one organization.
• Transmission speed is high.	Transmission speed is average.	Transmission speed is low.
• Propagation delay is short.	Propagation delay is moderate.	Propagation delay is long.
• Less congestion	More congestion	More congestion than MAN.
• Design and maintainance are easy	Design and maintenance are difficult.	Design and maintenance are difficult than Man.
• More fault tolerance	Less fault tolerance	Less fault tolerence

(3) Explain Network Topology

→ The physical topology of LAN refers to the way in which the station are physically interconnected.

→ It is also defined as, the manner in which nodes are geometrically arranged and connected is known as topology of network.

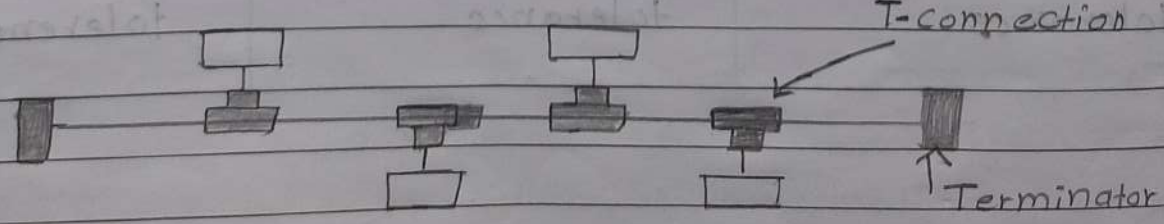
→ Network topology refers to the physical layout of the network.
Each topology has it's own strengths and weakness.

→ There are four types of topologies are used in network.

(i) Bus
(ii) Star
(iii) Ring
(iv) Mesh

(i) Bus Topology :

- It is also called horizontal topology.
- In this multiple devices are connected one by one, by means of connectors or cables.



- When one computer sends signal up the wir all the computers on the network recieve the information, but only accept the information using address matching.
- Bus is passive ~~technology~~ topology beccause it requires termination. Cable can not be left unterminated in bus network.
- Terminators were the 50 Ω registors that were connected to each end of cable.

Advantage

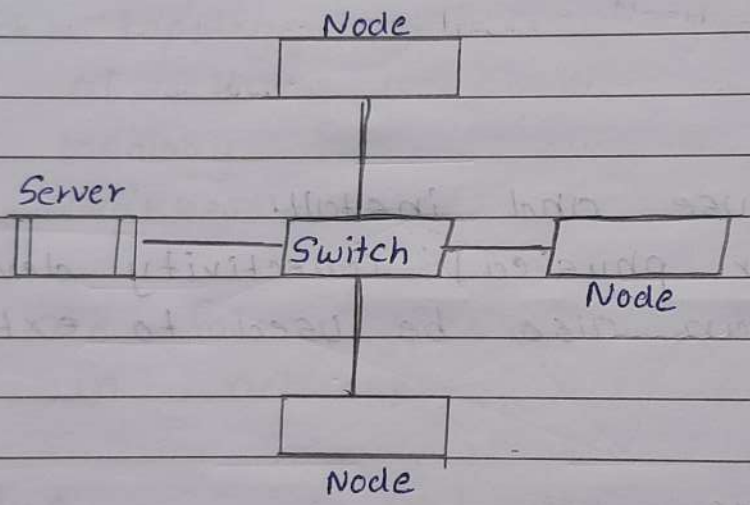
- Easy to use and install.
- Need fewer physical conectivity device.
- Repeater can also be used to extend network
- Low cost.

Disadvantage

- Heavy network traffic can slow a bus
- Difficult to troubleshoot a bus.
- Failure of cables affects all devices on the network.
- Difficult to add new node.

(ii) Star Topology

- It consists of a number of devices connected by point to point links to a central hub.
- Easy to control and traffic flow is simple.
- Data travels from sender to central hub and then to the receiver.



Advantage

- Easy to modify and add new network.
- Troubleshooting techniques are easy.
- Failures of any node don't bring down the whole star network.

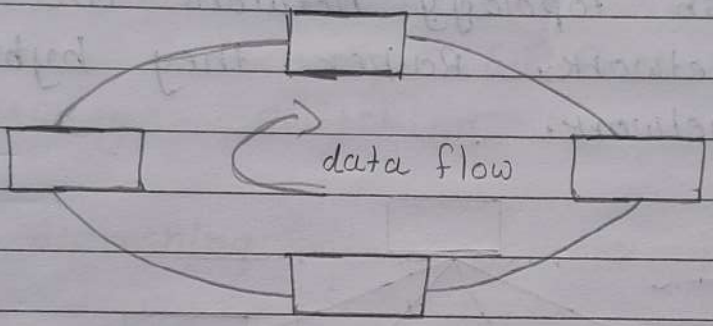
Disadvantage

- If central hub fails, the whole network fails.
- Each device requires it's own cable segmant.
- Installation is moderately difficult.

(iii) Ring Topology

-> In this each computer is connected to the next computer with the last one connected to the first. The signals travel on this cable is only one direction.

-> Ring is an active network. Termination is not require.



Advantage

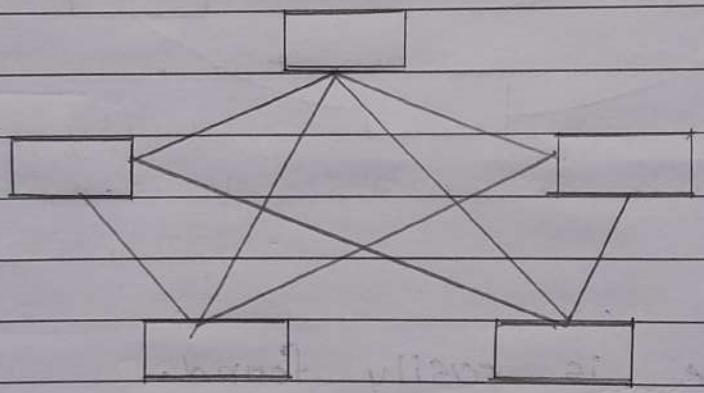
-> Cable failure is easily found.
-> Every node is given equal access so no one node can monopolize the network.

Disadvantage

-> Adding or removing node can disrupts network.
-> Difficult to troubleshoot ring network.
-> Failure of one node can affect the whole network.
-> Cost of cable is more.

(iv) Mesh Topology

- It has a link between each device in the network. It is more difficult to install as number of device is more.
- Much more bandwith avalcaible in mesh configuration is wasted.
- Most mesh topology network are not true mesh network. Rather they hybrid Mesh network.



Advantage

- Troubleshooting is easy.
- Isolation of network failures is easy.

Disadvantage

- Difficulty of Installation
- Costly because maintaining redundant link.
- Difficulty to reconfiguration.

(4) Explain Switching fabrics.

→ Switching fabric is a topology where different network node and terminals are connected with each other via number of switches Usually it uses crosbar switches.

→ The topology is used in high speed network like fiber Channel and infiniband.

→ There are three types of switching.
(i) Circuit Switching (ii) Packet switching
(iii) Message switching

(i) Circuit switching

- There is physical connection b/w transmitter and reciever.
- All the packet using same path.
- Needs end to end path before data transmision
- Reverses entire bandwith in advance.
- Charge is based on distance and time but not on traffic
- Waste of bandwith is possible.
- Congestion occur for per minute.

- It can not support store and forward transmission.
- Not suitable for handling interactive traffic.
- Recording of packet is not possible.

* Advantage

- Fixed bandwith, guaranteed capacity
- Low variance end to end delay

* Disadvantage

- Connection setup and tear down introduce extra overhead.
- User pay for circuit, even when not sending data.
- Other user can't use circuit even it's free.

(ii) Packet Switching

- No physical path is require blw transmitter and receiver.
- Packet travel independantly.
- No need end to end path before data transmission
- Does not reserve bandwith in advance.
- Charge is based on number of byte and connect time.
- No waste of bandwith.
- Congestion occurs for per packet.
- It support store and forward trasmission.
- Suitable for handling interactive traffic.
- Recording of packet is possible.

* Advantage

- Use resource more effectively.
- Very little setup and tear down time.
- More flexible.
- Improved bandwith

* Disadvantage.

- Complex protocol
- Algorithms are more complicated.
- Difficult to bill customers.
- Switching processor must be powerfull.

(iii) Message Switching

- No physical path is set in advance b/w transmitter and receiver.
- Packets are stored and forward.
- No need end to end path before data transmission.
- Does not reserve bandwith in advance.
- Charge is based on number of byte and distance.
- No waste of bandwith.
- No congestion or very less congestion.
- It support store and forward transmission.
- Suitable for handling interactive traffic.
- Recording of packet is possible.

* Advantage

- Efficient traffic managment.
- Reduce network traffic congenstion.
- Efficient use of transmission channel.

* Disadvantage

- Because of store and forward, transmission delay is in deduced.
- Each node require large capacity for storing.

(5) Explain Connection Oriented and Connectionless services.

-> Connection oriented and connectionless are two type of services that is offered by layer.

-> In connection oriented direct path is established blw source and destination.

The telephone system is the example of the connection oriented service.

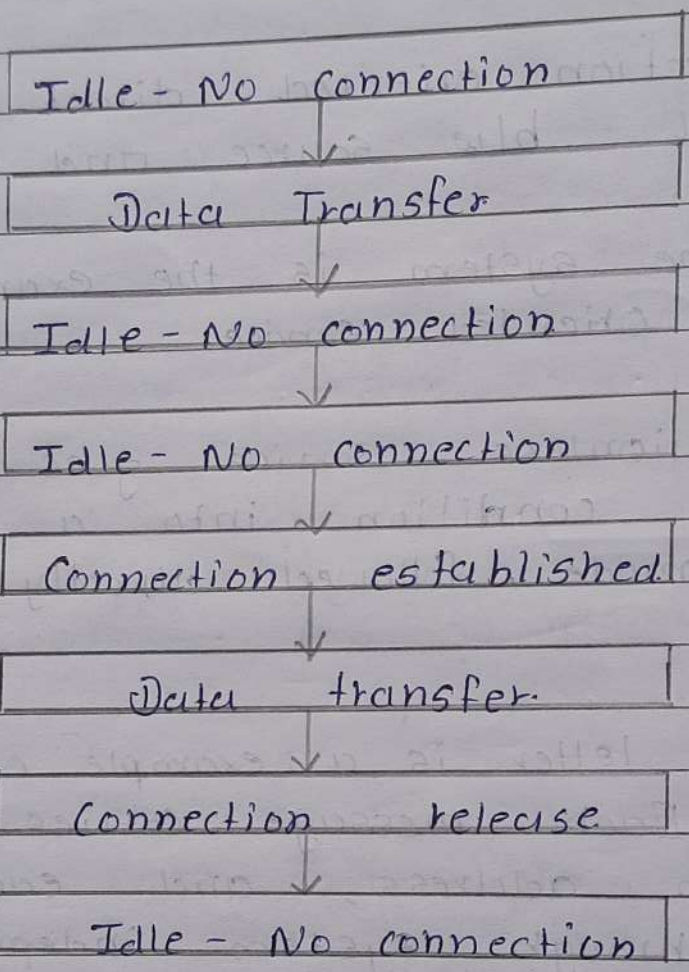
-> The connectionless service goes directly from an idle condition into a data transfer mode, followed directly by idle condition.

. Mailing a letter is a example of connectionless service. Each messaye carries the full destination address, and each one is routed through system independent of all the others.

-> Each service can be characterized by a quality of service. Some services are reliable in the sense that they never lose data.

→ reliable service is implemented by having receiver acknowledge the receipt of each message, so the sender is sure that it arrived.

Connectionless →



Connection oriented →

→ In connectionless service there is no acknowledge, no flow control and no error control.

→ In connection oriented service there is acknowledge, flow of control and error control.

(6) Explain OSI Reference Model.

-> The ISO was one of the first organizatio to formally define a common way to connect computers. Their architecture called Open System Interconnection.

-> The international organization for standardizati devlope the OSI reference model. OSI model is the most widely used model for networking.

-> OSI Model is a seven layer standard.

-> The OSI model does not specify the communication standard or protocol to be used to perform networking task.

-> Provide following Service.

- Peer-to-Peer logical service with layer physical implementation.
- Standards for communication blw system.
- Each layer should perform a well define function
- Defines point of interconnection for the exchange of information blw System.

* Principles

- A layer should be created where a different abstraction is needed.
- Each layer should perform well defined function.
- The function of each layer should be chosen with an eye toward defining.
- The layer boundaries chosen to minimize information flow.

* Layers

(i) Physical layer : It is the lowest layer of OSI model.
It is a function to transmit individual bits from one node to another over a physical layer

Functions : Physical characterstic of interface and media.
Representation of bits,
Data rate,
Synchronization of bits.

(ii) Data linker : It is responsible for the reliable transfer of data frames from one node to another connected by physical layer.

Function : Physical addressing, flow control, Error control, Access control, Framing

(iii) Network layer : It manages the delivery of individual data packets from source to destination through appropriate addressing and routing.

Function : Logical addressing, Routing

(iv) Transport layer : It responsible for delivery of the entire message from the source host to destination.

Function : Connection control, flow control, Error control, Port addressing

(v) Application Layer : It provides high level APIs to the user. It is responsible for accessing network by user.

Function : Network virtual terminal, Mail service, Directory service, File transfer, Access and managment.

(7) Explain TCP/IP Protocol.

-> TCP/IP stands for Transmission Control Protocol / Internet protocol.

-> It is a set of protocols that allow communication across multiple network.

-> It consist four layer system.
Application layer, Transport layer, Internet layer, Host to network layer.

-> Internet layer is also called network layer. Internet layer handles communication from one machine to other.
Routing of packet takes place in internet layer.

-> Host to network layer is responsible for accepting and transmitting IP datagrams. This layer normally includes the device driver in OS.

* Application Layer : It is top most level in TCP/IP model.
  - It is responsible for handling high-level protocol, issues of representation.
  - This layer allow user to interact with application.
  - known application protocols are : TELNET, FTP, SMTP, SNTP,

* Transport Layer : Application programs send data to transport layer. protocol TCP and UDP. An application is designed to choose either TCP or UDP based on service it needs.

* Internet Layer : It is the second layer of TCP/IP model.
- An internet layer is also known as network layer.
- The main responsibility of Internet layer is to send the packet from any network and they arrive at the destination irrespective of the route they take.

* Host to network : This layer is also called network interface layer.
This layer is same as physical and data link layer of OSI model.
It can't define any protocol.
It is responsible for accepting and transmiting IP datagrams.

OSI	TCP/IP
7 layers	4 layers.
Model was first defined before implementation takes place.	Model define after protocol were implemented.
Gives guarantee of reliable delivery of packet.	Transport layer doesn't always guarantee reliable delivery of packet.
It doesn't support Internet working.	It support internet working.
Strict layering.	Lossely layering.
Support connectionless and connection oriented both communication.	Support only connection oriented communication.

(8) Explain Physical, IP [Logical], Port Address.

* Physical Address

- It is lowest level of address and is also reffered as link address.
- The physical address of node is defined by it's LAN or WAN. Physical address is included in the frame by the data linker layer.
- The size and format of physical adresses vary depending on the network. It has authority over the network.
- Data linker layer at sender receive data from upper layer, encapsulates the data in a fram, adds an header.

* Logical [IP] Address

- Logical address are independent of underlying physical network. Since different network can have different address format hence a universal address system is required which can identify each host uniquely.
- Physical address is changes from hop to hop but the logical address remains the same.

* Port Address

- The IP address and physical address are necessary for data to travel from source to destination.
- But a communication process involves TELNET and FTP which requires addresses.
- In TCP/IP architecture the lable assigned to a process is called port address.
- In TCP/IP port address is of 16-bit.

(9) Explain Denial of Service (DOS).

-> In Dos attack, an attacker attemps to prevent legitimate users from accessing information or services.

-> By targetting your computer and network connection, an attacker may be able to use and accessing email, website, Online account etc.

-> The most common and obveious type of Dos attack occurs when an attacker flood a network with information.

-> The Server can process a certain number of request at once so if an attacker oveloads the server with request. It can't process your request.
This is Denial of service because you can't access that site.

-> By sending many or large email message to account an attacker can consume your quota, preventing you from receiving legitimate message.

-> Types of DOS.
(i) Penetration (ii) Eavesdropping
(iii) Man in the middle (iv) Flooding

(i) Penetration :

- Attacker gets inside your machine.
- Can take over machine do whatever he wants.
- Stolen password or insider access.

(ii) Eavesdroping

- Attacker gain access to same network.
- Listen to traffic going in and out of your machine.

(iii) Man-in-the-middle

- Attacker listen output and control output.
- Can substitute message in both direction.

(iv) Flooding

- Congestion may occure in path before your machine.
- Message from legitimate user are crowded out.

(10) Explain Delay and loss in Packet switched Networks.

→ Processing Delay

- Processing delay is a nodal delay and it is defined as the time required examining the packet's header and determining where to direct the packet.
- The processing delay is denoted by [$d_{proc.}$]
- Processing delay also include delay due to the time needed to check for bit-level error in the packet that occurred in transmitting the packet's bits from the upstream router to other router.

→ Queuing Delay

- After nodal processing delay the router directs the packet to the queue that precedes the link to subsequent router.
- The queuing delay denoted by [$d_{queue.}$]
- The queuing delay is observed at the queue the packet experiences a queuing delay as it waits to be transmitted over the link.

→ Transmission Delay

- The transmission delay is defined as the ammount of time required to transmit all of packet bits over the link.
- The transmission delay is denoted by dtrans.
- It is also called as store and forward delay.

$$\text{Transmission delay} = \frac{\text{Packet length}}{\text{Transmission rate}} = \frac{L}{R}$$

→ Propagation delay

- The propagation delay is defined as time required by packet to propagate for transmitting node to receiving node.
- Propagation delay is denoted by d_{prop}.
- Propagation speed of a packet depends on characteristic of physical medium of the link and distance blw the nodes.

(11) Explain Virtual Circuit Networking.

-> Virtual circuit switching is a packet switching methodology whereby a path is established blw the source and the final destination through which all the packets will be routed during a call.

-> This path is called a virtual circuit because to the user the connection appears to be dedicated physical circuit.

(12) Explain Data Encapsulation in Network Layer?

-> Data encapsulation is a process in which some extra info is added to data item to add some feature.
-> We use either OSI or TCP/IP model in our network ~~for~~ and data transmission takes place through various layers in this model.
-> Data encapsulation add some protocol information to the data so that data transmission can take place in proper way. This information either can be added in the header or footer of the data.
-> The data encapsulated on sender's side, starting from the application layer to the physical layer.
-> Each layer takes encapsulated data from previous layer and adds some more information to encapsulate it and some more functionalities with the data.
-> These functionality may be included proper data sequencing, error detection and control, flow control, congestion control, etc.

Chapter : 2

Application Layer

(1) Explain DNS.

→ DNS stands for Domain name System.

→ DNS is a directory service that provides mapping blw the name of a host on the network and its numerical address.

→ DNS is required for functioning of internet.

→ Each node in a tree has a domain name, and a full domain name is a sequence of symbol specified by dots.

→ DNS is a service that translate the domain name into IP addresses. This allows user of networks to utilize user-friendly names when looking for other host instead of reMembering IP address.

→ Eample: Suppose FTP site a. Edusoft had an IP address 132.147.165.50, most of the people would reach site by specifying EduSoft.com.

Therefore domain name is more reliable than IP address.

→ The domain name space is divided into three different section Generic domain, Country domain, Inverse domain.

* Generic Domain : It defines registered hosts according to their generic behaviour.

Each node in a tree defines the domain name which is an index to the DNS database.

It uses three character labels and these labels are describe the organization type.

* Country Domain : It is same as generic domain, but it uses two character country abbreviation in place of three character organizational abbreviation.

* Inverse Domain : It is used for mapping an address to a name when the server has received a request from the client and the server contain the files of only authorized client.

→ Working of DNS

- DNS is a client/server network communication protocol. DNS client sends requests to the server while DNS server send response to the client.

- Client requests contain a name which is converted into an IP address known as a forward DNS looksup while requests containing an IP address which is converted into name known as reserve DNS looksup.

- If a client like a web browser sends a request containing a hostname, then a piece of software such as DNS resolver sends a request to the DNS server to obtain IP address of hostname.

(2) Why do HTTP, FTP, SMTP and POP3 run on top of TCP rather than on UDP?

→ HTTP, FTP, SMTP and POP3 being application layer protocol can run on any of the underlying protocols, be it TCP/IP, IPx/SPx, UDP even on FCP.

- TCP is the most known after transmission protocol due to it's reliability and Ubiquity.
UDP being a connectionless transport protocol, ~~for almost all~~ there can be no guarantee of reliable data transmission.

- The OSI model has been built in such way that each layers work in an abstracted and encapsulated way, which means individual layer don't care about any dealing with the layer above or below it.

- A great example of these 3 layer transmission control protocol working with variety layer 1 protocols. Devices can be linked using fiber channel, ethernet, WiFi and still they use TCP, because TCP will

never come to know what transmission medium is being made.

- It is for these reason we have device drivers so that an Ethernet LAN Card and a WiFi interface can all output data to the next layer, the data link layer in the same universal format.

- So, no matter what the protocol is HTTP/FTP/SMTP all will receive data in same readable universal layer 7 input from making them work in all scenarios.

(3) Explain HTTP.

-> HTTP stands for hyper text transfer Protocol.

-> It is a protocol used to access the data on world wide web (www)

-> HTTP protocol can be used to transfer the data in the form of plain text hyper text, audio, video etc.

-> It is called HTTP because of it's efficiency that allows us to use in a hyper text enviroment where thre are rapid jumps from one document to another document.

-> HTTP is similar to FTP as it also transfer the files from one host to another host. But HTTP is simpler than FTP.

-> HTTP Similar to SMTP as the data is transferred blw client and server. The HTTP differs from the SMTP in the way the messages are sent from client to server and vice versa. SMTP message are stored and forward while HTTP message are deliverd immediatley.

* Features

-> HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from server. When the server receive the request. the server processes the request and sends back the response to the HTTP client after which the client disconnect the connection.

-> HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required to specify content type in MIME-type header.

-> HTTP is a stateless protocol as both the client and server know each other only during the current request.

* Messages

-> Request Message : The request message is sent by the client that consist of request line, header and sometime body.

-> Response Message : The response message is sent by the server to the client that consists of a status line header and sometime a body.

* URL

-> URL stands for Uniform resource locator.

-> URL is a standard way of specifying any kind of information on internet.

-> URL defines four part:

Method	://	Host	:	Port	/	Path

- Method : Method is a protocol used to retreive the document from server.

- Host : Host is a computer where the information is stored and the computer is given an alias name.

- Port : The URL can also contain the port number of the server but it's an optional field.

- Path : Path is the pathname of the file where the information is stored. The path itself contain slashes that seprate the directories from sub-directories and files.

Presistent HTTP	Non-Presitent HTTP
Version is 1.1	Version is 1.0
It uses one RTT.	It uses two RTT.
TCP connection is not closed.	TCP connection is closed after every req-response.
Client make multiple req over the same TCP connection.	client make multiple req on different TCP connection.
It is default mode	It is not default mode.
Request methods are GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS	Request method used are GET, POST and HEAD

(4) Explain Electronic Mail.

→ E-mail is an asynchronous communication medium. Electronic mail is used for sending a single message that includes text, voice, video, graphic to one or more recipients.

→ E-mail is fast, easy to distribute and inexpensive.

→ SMTP is the standard mechanisms for electronic mail in the internet.
SMTP is the TCP/IP mail delivery protocol.

→ E-mail is not a real-time service in that fairly large delays can be tolerated.

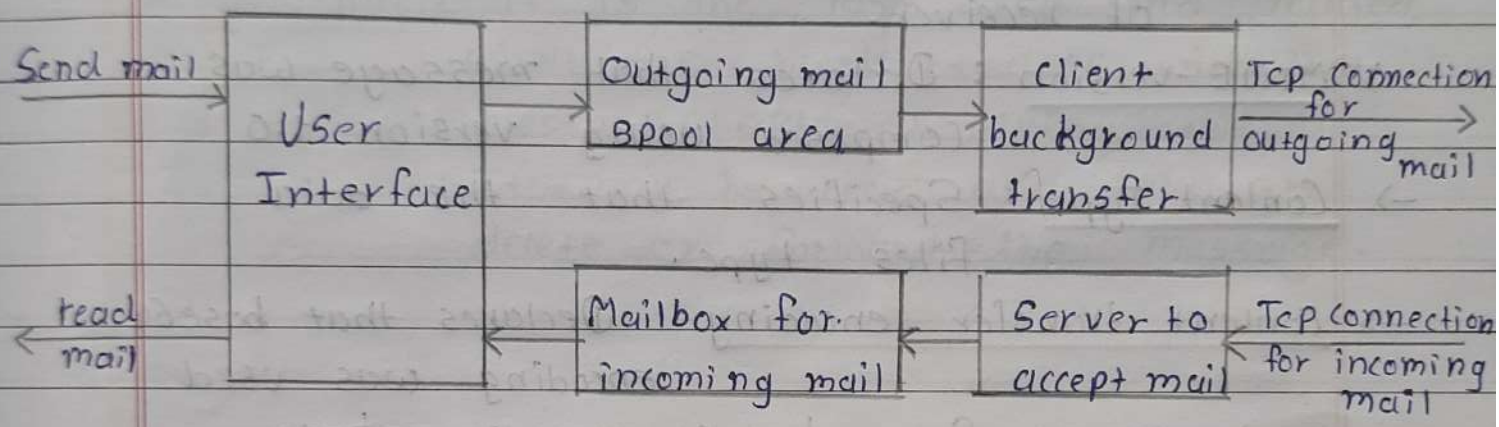
→ It is also not connection oriented in that a network connection does not need to be setup expressly for each individual message.

→ Mail server handles incoming and outgoing mail.

→ The post office protocol (POP) servers store incoming mail while SMTP server relay outgoing mails.

-> The internet service provider (ISP) probably runs both an SMTP server and POP server for it's customers.

-> Following are the ways to access e-mail,
(i) Web based e-mail service
(ii) E-mail through LAN
(iii) Unix shell account.
(iv) Using mail client.



-> To send e-mail to someone, the internet email address must be known to sender.
Email : porwalharsh70 @gmail.com.

-> The email address has two main parts, joind by @. In this example vilus is the username. Username can contain number, underscore, periods and some other special character. commas, space and paranthesses are not allowed.

-> Hotmail.com is the host or domain name.
E-mail address is not case sensitive.

From : Porwal007@gmail.com
To : Harsh007@gmail.com
MIME-Version : 1.0
Content-Type : Img
Content transfe encoding : base64

→ From : indicates the mail Id (address) of sender.
→ To : Indicates the mail Id (address) of receiver.
→ MIME-Version : Declares that message was composed using version 1.0
→ Content Type : Specifies that the data files type.
→ Content transfer encoding : Declares that base64 encoding was used to convert from base64 encoding back to binary.

* Function

→ Composition : It is a process of creating message and answeres. Any text editor can be used for the body of the message. When answering message, the email system can extract the originator's address from the incoming e-mail.

-> Transfer : It is moving message from the originator to the receiver.

-> Reporting : It inform the orginator what happened to the message. Wheather email deliverd or not.

-> Displaying : It is required for reading the email.

-> Disposition : It is the last step and related what the receiver does with the message after receiving it. It may be read and save or delete or forward the message.

(5) Explain client server architecture.

→ The client server architecture is a type of computing system in which one powerful workstation server that request of other system is an exampie of client server technology.

→ The client server architecture is a distributed application structure that partition task or workload blw providers ~~amak~~ of a resource of service called server, and service requester called clients.

→ Client: When we talk about client it mean to talk of person or an organization using a particular service. Similarly in digital world client is a computer capable of receiving information ~~of~~ or using a particular service. from the service provider.

→ Server: When we talk the word server it mean a person or medium that serves something. In digital world server is a remote computer which provides data or access of service.

→ Working

- User enters URL of the website in browser then browser request the DNS server.
- DNS server lookup for the address of web server.
- DNS server respond with IP address of web server
- Browser send over an HTTP/HTTPS request to web server's IP
- Server send necessary files of website.

→ Advantage

- Certilized system with all data in one place.
- Less maintanance cost and data recovery is possible.
- Capacity of client and server can be changed seperately.

→ Disadvantage

- Server are prone to DOS attack.
- Data packet may be spoofed during transmission.
- Login credential and useful information of user are common and MITM attacks are common.

Chapter : 3

Transport Layer

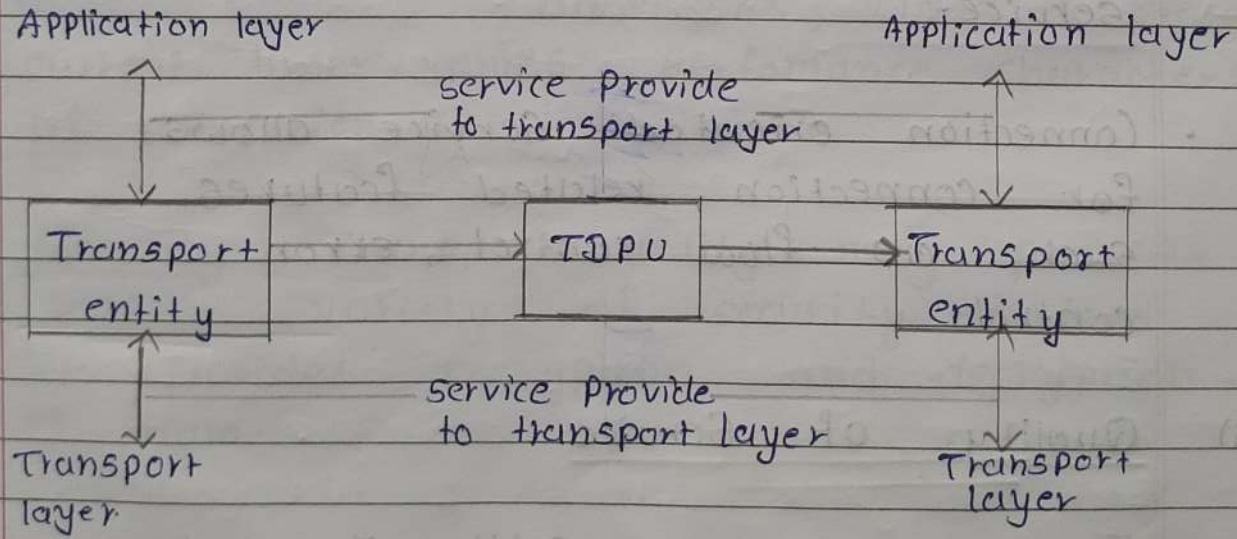
(1) Explain transport layer Service.

→ The transport protocol should provide to higher-level protection.

→ The transport entity that provides service to transport service users, which might be an application process.

→ The hardware and software within the transport layer that does the work is called transport entity.

→ It can be in the OS kernel, in a separate user process or on the network interface card.



Chapter : 3

Transport Layer

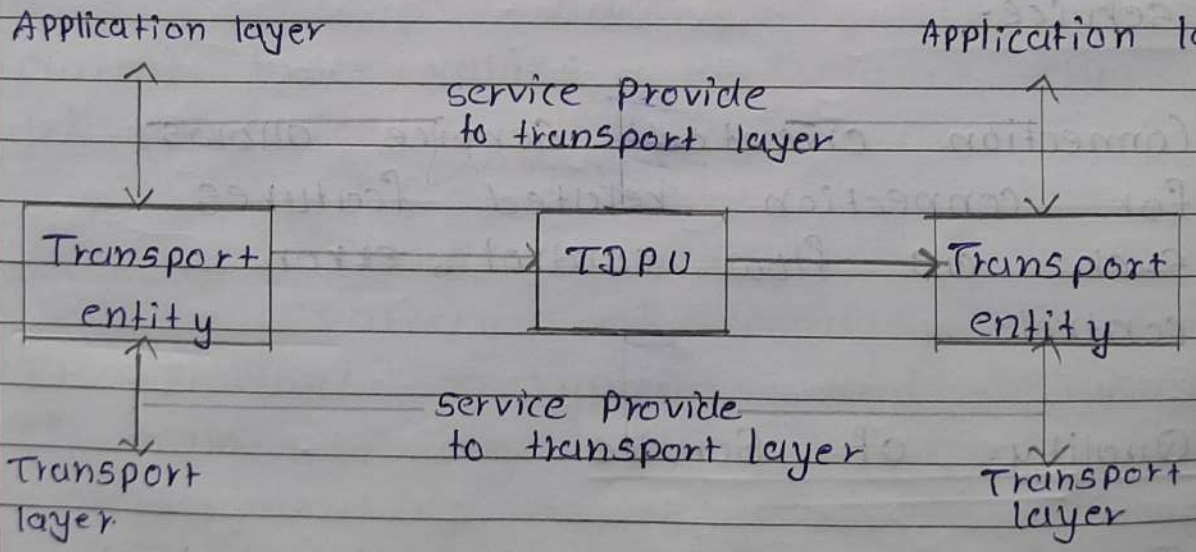
(1) Explain transport layer Service.

→ The transport protocol should provide to higher-level protection.

→ The transport entity that provides service to transport service users, which might be an application process.

→ The hardware and software within the transport layer that does the work is called transport entity.

→ It can be in the OS kernel, in a separate user process or on the network interface card.



→ There are some categories of service.
(i) Type of service
(ii) Quality of service
(iii) Data transfer
(iv) User Interface
(v) Connection Managment
(vi) Status reporting
(vii) Security

(i) Types of service

- It provides two types of service connection oriented and connectionless or diagram service.
- Connection-oriented service provides maintanance and termination of logical connection blw transport service and user. It is reliable service.
- Connection oriented service allows for connection related features such as flow control, error control.

(ii) Quality of Service

- Transport protocol entity should allow the service user to specify the quality of transmission service to be provided.

(iii) Data Transfer

- It transfers data b/w two transport entities. Both user and control data must be transferred. Full duplex service must be provided. Half-duplex and simplex modes may also be offered.

(iv) User Interface : There is not clear mechanism of the user interface to transport protocol should be standardized.

(v) Connection Managment : If connection-oriented service is provided the transport entity is responsible for establishing and terminating connection.

(vii) Status Reporting : It gives following Information Addresses, class of protocol, current timer values, Perfomance characterstics of connection.

(viii) Security : Transport entity may provide a variety of security services. It provides encryption and decryption of data.

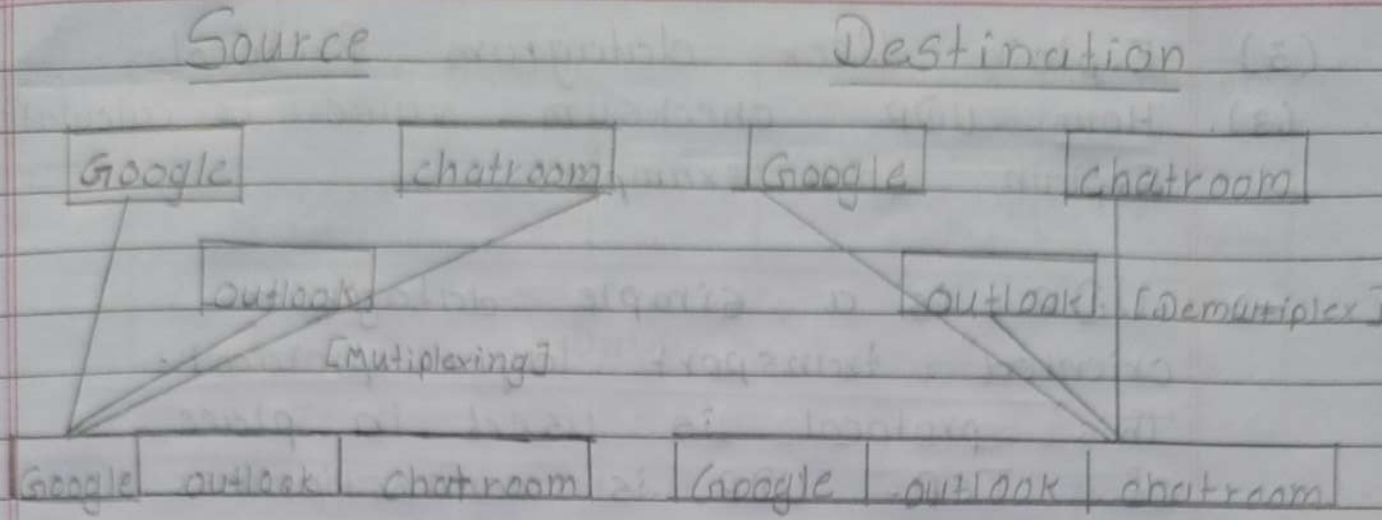
(2) Explain Multiplexing and Demultiplexing.

→ Multiplexing : It is the process of collecting data from multiple application processes of the sender enveloping the data with headers and sending them as a whole to the intended receiver.

- Collected data from various application process segmant contain the source port number, destination port number, header files and data.
- These segmant are passed to network layer which adds the source and destination IP address to get the diagram.

→ DeMultiplexing : Delivering and received segmant at the receiver side to the correct app layer process is called demultiplexing.

- Each datagram has a source IP address and destination IP address.
- Each datagram carries 1 transport layer segmant.
- Each segmant has the source and destination port number.



→ Multiplexing and demultiplexing are just concept that describe the process of transmission of data genrated by different application simultaneously.

When data arrives at transport layer, each data segmant is independantly processed and send to it's appropriate application in the destination machine.

→ The above figure shows that the source computer is using google, outlook, chatroom application at same time.

→ All the data is forwarded to a destination computer.

→ Each application has a segmant put on a wire to be transmitted. It signifies that all application are running simultaneously.

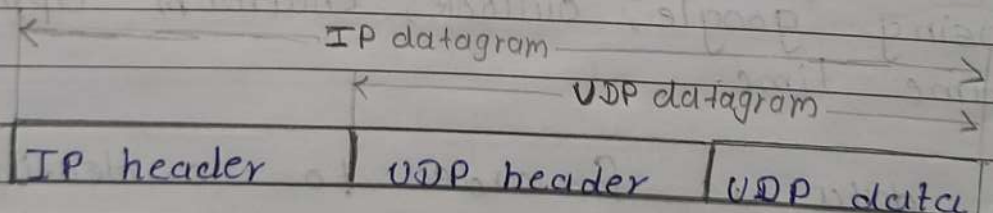
→ Without multiplexing / Demultiplexing user can use only one application at a time.

(3) Explain User datagram Protocol
(3) How UDP checksum value is calculated? Explain with example.

-> UDP is a simple datagram oriented transport layer protocol. This protocol is used in place of TCP. UDP is connectionless protocol provides no reliability or flow control mechanism. It also has no error recovery procedures.

-> Several application layer protocol such as TFTP (Trival File transfer protocol) and the RPC use UDP.

-> UDP makes use of port concept to direct the datagrams to the proper upper-layer application.



-> Diagram shows that encapsulation of a UDP datagram as an IP datagram.

Source Port number 16-bit	Destination Port number 16-bit
UDP length 16-bit	UDP checksum 16-bit
Data	

8 byte

→ UDP datagram contain a source port number and destination port number.
Source port number identifies the ~~receiving~~ port of the sending application process.
Destination port number identifies the receving process on the destination host machine.

→ UDP checksum covers the UDP header and data. both UDP and TCP includes 12-byte pseudo-header with the UDP datagram just for the checksum computation.
This pseudo-header include certain fields from IP header.

→ UDP checksum is end to end checksum. It is calculated by the sender and then verified by receiver. It is designed to ~~each~~ catch any modification of the UDP header or data anywhere b/w sender and receiver.

→ UDP provides only error checking, it does not do anything to recover from error.

→ Example

```
  1 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0
+ 1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
-----------------------------------
1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1
```

→ The carry from MSB is added to the result.

```
  1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1
                                1
-----------------------------------
1 0 1 1 1 0 1 1 1 0 1 1 1 1 0 0
```

→ Checksum is the 1's compliment of result.

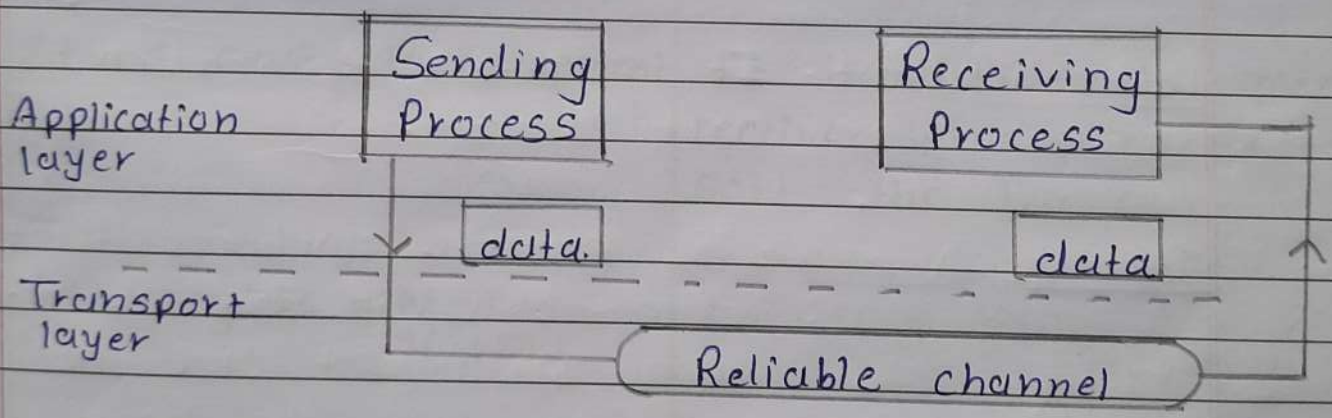
0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 1

(4) Principle of Reliable data transfer.

→ Transport layer protocol are central piece of layered, these provides the logical communication blw computer program process.

→ These process uses logical communication to move data from transport layer to network layer and this data transfer should be reliable and secure.

→ The problem of transfering data occurs not only in transport layer but also in application layer as well as in link layer.



→ In this model, we have design sender and receiver sides of protocol over a reliable channel.

→ In reliable transfer of data the layer receives the data from the above layer breaks the message in the form of segment and put the header on each segment and transfer.

-> Below layer receives the segmants and remove header from each segmant and make it packet by adding to header.

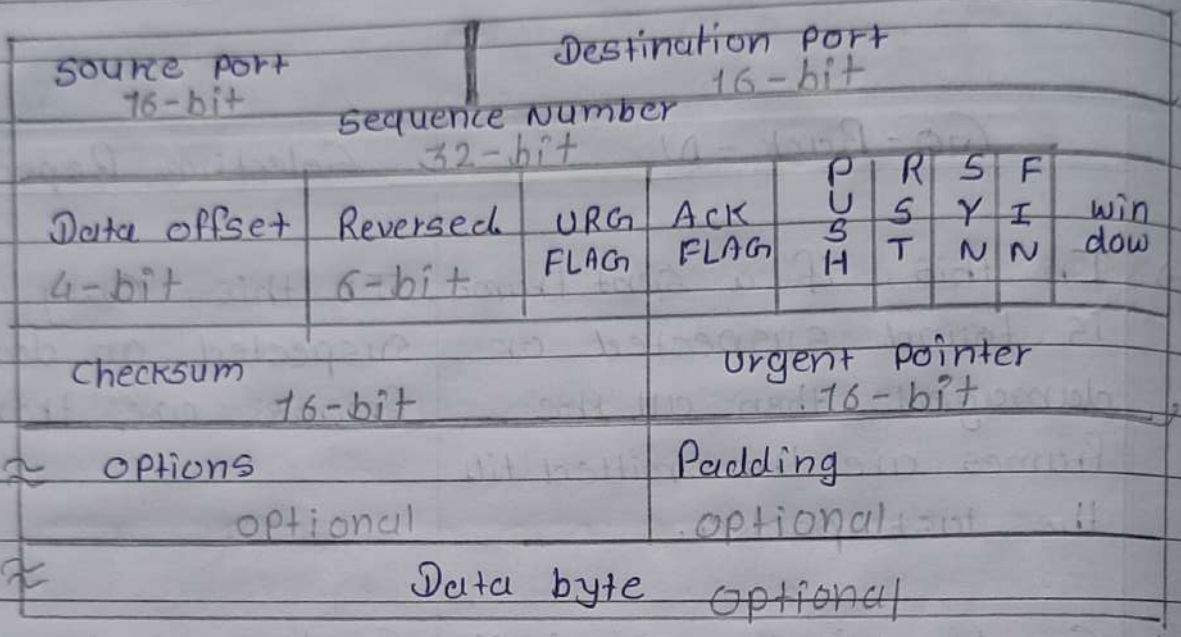
-> The data which is transferred from the above has no transferred data bits corrupted or lost, and all are delivered in the same sequence in which they were sent to the below layer is reliable data transfer protocol.

(5) Difference between Go-Back-N and Selective Repeat.

Go-Back-N	Selective Repeat
→ In this, if a sent frame is found suspected or damaged then all the frames are transmitted till the last packet.	In this, only the suspected or damage frame are transmitted.
→ Sender window size is N.	Sender window size is N.
→ Receiver window size is 1.	Receiver window size is N.
→ It is easier to implement.	It is difficult to implement receiver window needs to sort the frames.
→ Efficiency is $= \frac{N}{(1+2a)}$	Efficiency is $= \frac{N}{(1+2a)}$
→ Acknowledgement type is comulative.	Acknowledgement type is individual.
→ No need to sorting frames	Receiver sides need to sort frames.
→ out-of-order packet are rejected and entire window is re-transmitted.	Out-of-order packet are accepted in selective Repeat protocol.

(6) Explain TCP Segmant Structure.

→



- Source Port: It is a 16-bit source port number used by receiver to reply.

Destination Port: It is 16-bit destination port number.

Sequence Number: The sequence number of first data byte in this segmant. During SYN control bit is set and the sequence number is n, and the first data byte is n+1.

Acknowledgement Number: If the ACK control bit is set, this field contains the next number that receiver expects to receive.

Data offset : The serval 32-bit word in the TCP header shows from where the user data begins.

Reserved bit : It reserved 6-bit for further use.

URG : It indicates urgent pointer field that data type is urgent or not.

ACK : It indicates acknowledgement field that in a segmant is significant.

PUSH : It is set or Reset according to a data type that is sent immediatley or not.

RST : It Reset the connection.

SYN : It synchronized the sequence number.

FIN : It indicates no more data from sender.

Window : It is used in ACK segmant. It specifies number of data bytes the sender is willing to accept. It can be used to control flow of data and congestion.

Checksum : Used for error detection

URgent Pointer : It is used to point data that is urgently required that needs to reach receiving process earliest.

(7) Explain TCP congestion Control.

-> When the load offer to any network is more than it can handle congestion occure.

-> When a connection is established the sender initializes the congestion window to the size of the maximum segmant in use on the connection.

-> When congestion window is 'n' segmants, if all 'n' are acknowledged on the time the congestion window is increased by the byte count corresponding to 'n' segmant.

-> The congestion window keep growing exponentially until either a timeout occurs or the receiver's window reached.

-> The internet congestion control algorithm uses the threshold parameter which is initially 64 kb, in addition to the receiver and congestion window.

-> When timeout occurs the threshold is set to half of the current congestion window and congestion window is reset to one maximum segmant.

→ The maximum segmant size is 1024 bytes, Initially the congestion window was 64 Kb, but a timeout occured, so the threshold is set to 32 Kb and the congestion window to 1 Kb for transmission 0 (zero) here.

→ The congestion window then grow exponentially until it hits the threshold (32 KB). Starting that it grow linearly.

→ Transmission 13 is unlucky and timeout occurs. The threshold is set to half the current window and slow start is initiated all over again.

→ If no more timeout occurs, the congestion window will continue to grow up to the size of receiver's window.

→ At that point it will stop growing and remain constant as long as there are no more timeouts and the receiver's window does not change size.

(8) Compare TCP and UDP.

→

TCP	UDP
It is Connection-oriented.	It is connection less.
Connection is byte stream	Connection is message stream.
Does not support multi casting and broadcasting.	Support broadcasting.
It provides error and flow control.	It does not provide error and flow control.
Supports full duplex transmission.	Does not support full duplex transmission.
It is reliable.	It is Unreliable.
TCP packet is called segment.	UDP packet is called User datagram.

(q) How end to end congestion provided by TCP. and Explain Slow Start Method.

→ TCP uses a form of end to end flow control. Both the sender and receiver agree on a common window size for packet flow. The window size represented the number of bytes that the source can send at a time.

→ The window size varies according to the condition of traffic in the network to avoid congestion.

→ A file of size 'f' with total transfer time of 'A' on a TCP connection results in a TCP transfer throughput

$$r = f/A$$

Bandwith Utilization $(P_u) = r/B$

where, B = Link bandwith

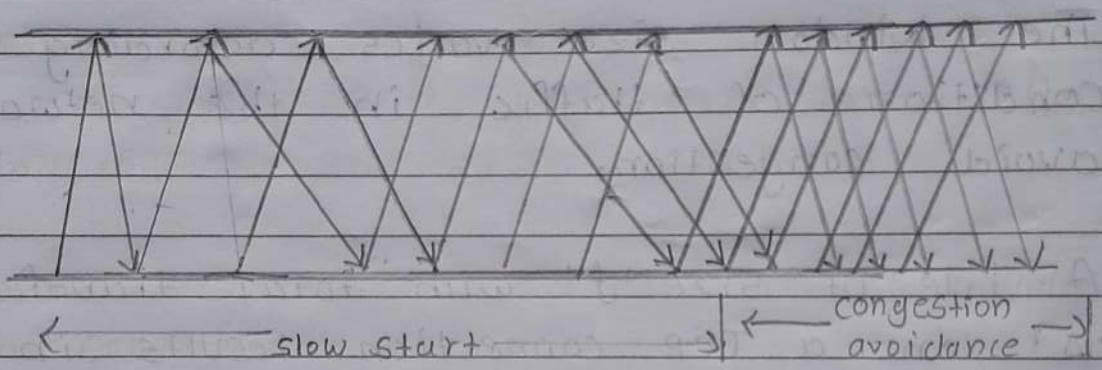
→ TCP has three congestion control method.

(i) Additive Increase
(ii) Slow start
(iii) Retransmit

* Slow - start Method

-> It increases the congestion window size nonlinearly and in most case exponentially, as compared to the linear increase in additive increase.

->



-> Source initially set the congestion window to one packet. When it's corresponding acknowledgment arrives, the source set the congestion window to two packet.

-> Now the source send two packets. On receiving two packets corresponding acknowledgement, TCP set the congestion window size to 4.
Thus the number of packet in transist double for each round trip time.

(10) Difference between flow and congestion control.

	Flow control	Congestion Control
->	It controls the traffic from a particular sender to a receiver.	It controls the traffic entering the network.
->	It prevents receiver from being overwhelmed by the data.	It prevents the network from getting congested.
->	It is responsibility handled by data link layer and transport layer.	It is the responsibility handled by network layer and transport layer.
->	Sender is responsible for transmitting extra traffic at receiver's side	Transport layer is responsible for transmiting extra traffic into network.
->	Sender transmits the data slowly to the receiver.	Transport layer transmit the data into the network layer.

(11) Explain Proxy Server.

→ A proxy server is a machine which act as an intermediary between the computers of a LAN and Internet. It is a program that act as intermediary between web browser and a web server.

→ Most of the time proxy server is used for the web and when it is an HTTP proxy.

→ Proxy server is also used to control and monitor outbound traffic.

→ Proxy server is associate with firewall and also caching program. The functions of proxy, firewall and caching can be in seprate server programs and combine in single package.

→ Most proxies have catche, the ability to keep pages commonly visited by user in memory, so they can provide them quickly as possible.
In computer science cache means temporary data storage.

→ A proxy server with ability to cache information is genrally called a proxy cache server.

Chapter : 4 Network Layer

(1) Explain Routing algorithm.

→ A host or router has a routing table with an entry for each destination, or a combination of destination, to route IP packet. Routing table can be dynamic or static.

→ The main function of network layer is to route packets from source to destination. To accomplish this a route through the network must be selected, ~~destination~~ genrally more than one route is possible. The selection of route genrally based on shortest route through the network.

→ The shortest route means route that passes through the least number of nodes. This shortest root selection result in least number of hopes per packet. A routing algorithm is design to perform this task.

→ There are 3 types of routing.

(i) Static routing
(ii) Dynamic routing
(iii) Default routing

(i) Static routing : In this the network topology determines the initial paths.
- Static routing becomes cumber some for bigger networks.
- It is a process in which we have to manually add routes to the routing table.

→ Advantage : Minimal CPU/Memory overhead.
- Simple to configure and maintain.
- Secure as only defined routes can be accessed.

→ Disadvantage : Manually update routes after changing.
- Impractical on large network.

(ii) Dynamic Routing : Dynamic routing makes automatically updated the routing table periodically by using one of the dynamic routing protocol such as RIP, OSPF or BGP.

RIP : Routing information protocol (Distance vector)
OSPF : Open shortest path first (Link state)
BGP : Border gateway protocol (Path vector)

- Dynamic routing algorithm change their routing decision if there is change in topology, traffic.

- Each router continuously check the network status by communicating with neighbours. Thus change in network topology is eventually propogated to all the routers

→ Advantage: Simple to configure on large networks.
- Ability to load balance blw multiple links.
- will dynamically choose better route if a link goes down.

→ Disadvantage: Updates are shared between routers, thus consuming bandwith.
- Routing protocol puts additional-load on router cpu/RAM.

(iii) Default routing: This is the method where router is configured to send all packets towards single router.

It does not matter to which network packet belongs, It is forwarded out to the router which is configured for default routing.

It is genrally use with sub router. A sub router is a router that has only one route to reach all network.

(2) Explain Routing loop Problem.

→ It is a serious network problem which happens when a data packet is continually routed through the same router over and over. The data packet continue to be routed within the network in endless circle.

→ A routing loop can have a impact on a network, and in some case disable the network. Normally routing loop is a problem associated with distance vector protocol.

→ Routing loop can occure when inconsistent routing tables are not updated due to slow convergence in charging network.

* Routing loop may caused by,

- Incorrectly configured static routes.
- Incorrectly configured route redistribution.
- Slow convergence.
- Incorrectly configured discard routes.

* Routing loops can create following issues :

- Excess use of bandwith.
- CPU resources may be strained.
- Network convergence is degraded.

* Avoidance technique

- Maximum hop count.
- Split horizon
- Route poisoning
- Hold-down timers

(3) Differentiate Broadcast and Multicast.

→

Broadcast	Multicast.
It has one sender and multiple receivers.	It has multiple sender and receiver
It works on star and bus topology.	It works on star, mesh, tree and hybrid topology.
It scale well across network	It doesn't scale well accross network.
It's bandwith is wasted.	It utilize bandwith efficiently
It has one to all mapping.	It has one to many mapping
Hub is an example of broadcast.	Switch is an example of multicast.
Process is slow.	Process is fast.

(a) Explain DHCP protocol.

→ DHCP stand for dynamic host configuration protocol.

→ It is a network managment protocol that can dynamically assign an IP address to a denial device, or node, on network so they can connect using IP.

→ DHCP automates and centrally handles these configuration. There is no requirment to manually assign an IP address to the new devices.

→ DHCP decrease the chances of common bugs appearing when IP address are created manually. It also insure no two hosts can have similar IP addresses.

→ DHCP act as essential role in handling small web where mobile devices are used and needed IP addresses on a non-permanent support. The electronic allocation of IP enables mobile to share openly from one network to another.

→ These appears when addresses are authorized manually. DHCP decrease the risk of such IP address conflicts. IP change is found the DHCP server is upgraded with new data and data will be distributed to the new endpoints automatically.

→ The use of DHCP provide that DHCP client get efficient and timely IP configuration parameter including IP address, subnet mask, default gateway so on without customer interference.

* Working of DHCP

→ **DHCP Server**: A DHCP server can be a router or a server role as a host. This is a networked device implementing the DHCP service and influencing IP address and associated configuration data.

→ **DHCP client**: DHCP client is the endpoint that receives configuration data from a DHCP server. This can be any device like computer, laptop or anything else that needs connectivity to network.
Some device is configured to receive DHCP data by default.

→ DHCP relay : A router or host that accepts client messages being advertised on that network and then forward them to a configure server.

The server then sends response back to the relay agent that devlopes them along with the client.

This can be used to centerlized DHCP server rather than having a server on each subnet.

→ Lease : It is the length of time for which a DHCP clients influence the IP data. When lease ceases, client has to reopen it.

→ Subnet : IP networks are logically divided two or more segmant called subnet or sub networks. Therefore, they can be handled effectively.

(5) Explain NAT. [Network address translation]

→ Usually we used gateway router devices used for NAT configuration. One of the interface for that devices is connected to the LAN and one of the interface for this device connected to the outside network.

→ When we receive a request from our local machine it will hit the configuration pool and that public IP converted to private or vice versa.

→ Inside worldwide location : IP address that speaks to atleast one inside nearby IP delivers to the rest of world.

→ Outside residential area : This is the genuine IP address of the objective host in the nearby organization after interpretation.

→ Outside worldwide location : This is the external host as observed to structure the external organization. It is the IP address of the external objective host before interpretation.

* Example

- Usage included with windows work area working frameworks.
- Local bundle channel.
- windows third party implementation.

⟶ Consider you have ISP abc.

- So, they will give you connection to your modem. That connection we used to called WAN.
- This connection is always configured with a public address.
- Then your modem is converted public connection to private connection.
- That means your device is connected to network that receives private IP address.
- In simple word NAT is used to translate private IP to public IP address or vise versa.

(6) Distance vector routing.

→ DVR is the dynamic routing algorithm. It was designed mainly for small network topologies. DVR is sometimes called by other names, most commonly the distributed Bellman-Ford routing algorithm and the Ford-Fulkerson algorithm.

→ The term distance vector derives from the fact that the protocol includes its routing updates with a vector distance or hope count.

→ In this algorithm, each router maintains a routing table indexed by, and containing one entry for, each router in the subnet. This entry contain two parts.
(i) Prefered outgoing line to use for that destination.
(ii) An estimate of the time or distance to that destination.

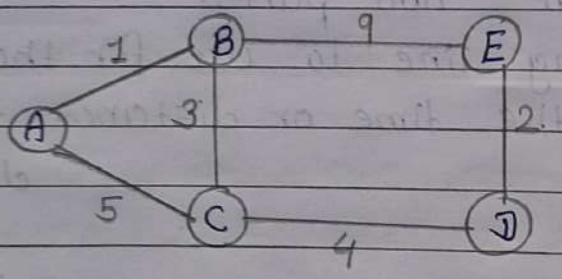
→ The metric used might be number of hopes, time delay in ms, total number of packets qued along the path.

→ Assume that delay is used as a metric and that the router knows the delay to each of it's neighbours. All nodes exchange information only with their neighbours nodes.
Nodes participating in the same local network are considered as neighbouring nodes.

-> Each router sends to each neighbour a list of it's estimated delay to each destination.
It also receives a similar list from each neighbour.

-> By performing calculation for each neighbour, a router can find out which estimate seems the best and use that estimate and the corresponding line in its new routing table.
Old routing table is not used in the calculation.

Ex. Write DVR table of B.



-> DVR table for B;

Destination	Cost	next
A	1	A
C	3	C
D	7	C
E	9	E

(7) Explain Link-State routing.

→ Link state routing is a second major class of intradomain routing protocol. It is dynamic type routing protocol.

→ The idea behind link state routing is simple and can be stated as five part.

(i) Learning about neighbours : When a router is booted, it sends a special HELLO packet on each point-to-point line. The router on the other end is expected to send back a replying telling who it is. When two or more routers are connected by a LAN, the LAN can be modeled as a node.

(ii) Measuring line cost : To determine the cost for a line, a router sends a special ECHO packet over the line that the other side is required to send back immediately. By measuring the round-trip time and dividing it by two, the sending router can get a reasonable estimate of the delay.

(iii) Building link state packet : State packets may be built periodically, or when some significant event occurs, such as a line or neighbour going down or coming back up again.

(iv) Distributing the link state packets :

- Each state packet contains a sequence number that is incremented for each new packet sent.
- Routers keep tracks of all the pairs they see.
- When a new link state packet comes in, it is cheked against the list of packets already seen.
  If it is new, it is forwarded on all lines except the one it arrived on.
  If it duplicate, it is discarded.

(v) Computing the new routers : Once a router has accumulated a full set of link state packets, it can construct the entire subnet graph. Then Dijkstra's algorithm can be run locally to construct the shortest path to all possible destinations.

- Link state routing protocol use event driven updates rather than periodic updates. Link state routing is widely used in actual network. OSPF protocol uses in a link state algorithm.

(8) Explain IPV4.

-> IP stands for Internet protocol and v4 stands for version 4.
IPV4 was the primary version brought into action for production within ARPANET in 1983.

-> IPV4 are 32-bits integers which will be expressed in decimal notation.
Ex. 192.0.2.126

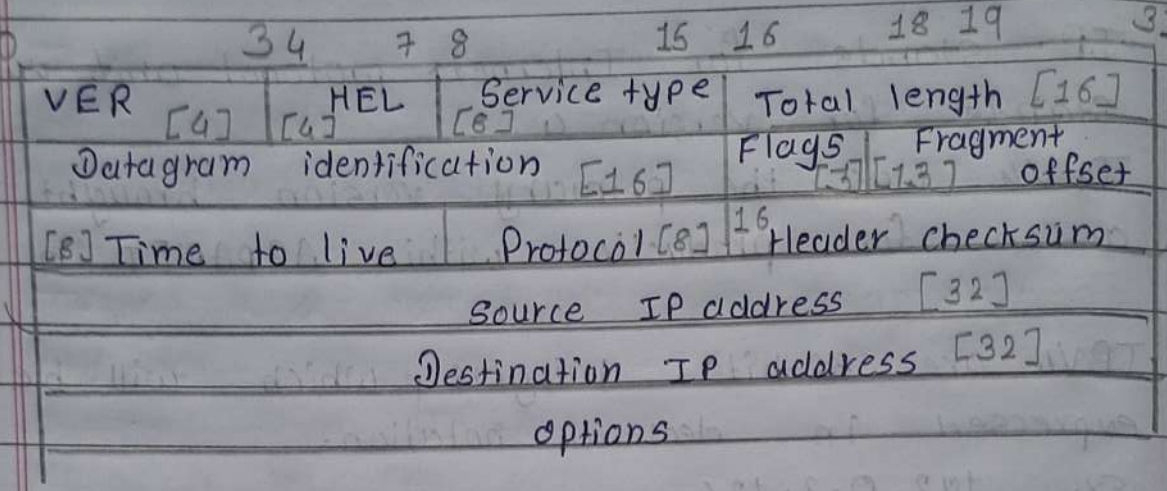
* Parts

-> Network Part : The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that assigned.

-> Host Part : The host part uniquely identifies the machine on your network. This part of the IPv4 address is assign to every host.
For each host on the network, the network part is the same, however the host half must vary.

-> Subnet Number : Local networks that have massive number of host are divided into subnet and subnet number

* Datagram



→ VER is a field that contains IP version.

→ HEL is the length of IP header in multiplies of 32 bits without the data field. Minimum value of correct header is 5, and maximum value is 15.

→ Service type is the indication of quality of service requested for this IP datagram.

→ Total length specifies the total length of datagram

→ Identification is a unique number assigned by the sender used with fragmantation.

→ Flag contain control flags
- 1st bit is reserved and must be zero.
- 2nd bit is : DF [Do not fragment]
- 3rd bit is MF [More fragment]

-> Fragment offset is used to reassemble the full datagram.

-> TTL (time to travel) specifies the time (in second) that datagram is allowed to travel.

-> Protocol number indicates the higher level protocol to which IP should deliver the data in this datagram.

-> Header checksum is a checksum for the information contained in the header. If the header checksum does not match the content of the datagram is discarded.

-> Source / destination IP addresses are 32-bit. Source / destination IP addresses.

(q) Explain IPv6.

→ IPv6 was devloped by internet engineering task force to deal with the problem of IPv4 exhaustion.

→ IPv6 is a 128-bits address having an address space of $(2)^{128}$, which is way bigger than IPv4.

→ In IPv6 we use colon hexa representation. There are 8 groups and each group represent 2 bytes.

→ We have three addressing method

(i) Unicast : Identifies a single network interface. A packet sent to a unicast address is delivered to the interface identified by that address.

(ii) Multicast : It is used by multiple host, called as group, acquires a multicast destination address. These host need not be geographically together. If any packet is sent to this multicast address, it will be distributed to all interface corresponding to that multicast address.

(iii) Any Cast : It is assigned to a group of interfaces. Any packet sent to an anycast address will be deliverd to only one member interface.

* Advantage

- Larger address space.
- Better header format.
- Security capabilities.
- Support for resource allocation.
- Allowance for extension.

-> IPv6 addresses are 128 bit in length. Addresses are assigned to individual interface on nodes, not to the node themselves. A single interface may have multiple unique unicast addresses.

-> The first field of any IPv6 address is the variable length format prefix, which identifies various categories of addresses.

(10) Compare b/w Distance and link state vector.

	Distance vector	Link-State vector
→	Bellan-ford algorithm is used to find shortest path.	Dijsktra algorithm is used to find shortest path.
→	Send message to their neighbours	Send message to every other node in network.
→	It is decenterlized routing algorithm.	It is centerlized global routing algorithm.
→	Sends larger update to only neighbour ~~node~~ routers.	Send small update everywhere.
→	Protocol example: RIP	Protocol example: OSPF
→	less CPU power require	More CPU power require.
→	less memory space needed	More memor space needed.
→	Simple to implement and support.	Expensive to implement and support.

(11) Compare IPv4 and IPv6.

	IPv4	IPv6
→	Header size is 32 bits.	Header size is 128 bits.
→	Can not support autoconfiguration.	Supports autoconfiguration.
→	Can not support real time application.	Support real time application.
→	No security at network layer.	Provide security at network layer.
→	Throughput and delay is more.	Throughput and delay is less.
→	It has a limited number of IP address.	It has large number of IP address
→	The IP address is represented in decimal.	The IP address is represented in hexadecimal.
→	Checksum field is avalaible in IPv4.	Checksum field is not avalaible in IPv6.
→	It doesn't provide encryption and authentication.	It provides encrytion and authentication.
→	IPv4 is broadcasting.	IPv6 is multicasting.

Chapter : 5

The Link Layer and LAN

(1) Disucuss the parity checks for error detection.

→ When data is transmitted from one device to another device the system does not guarantee wheather the data is received by the device is identical to the data transmitted by another device.

→ An error is a situation when the message received at the receiver end is not identical to the message transmitted.

→ There are two types of error.
(i) Single bit error
(ii) Burst error

(i) Singlebit error : It does not appear more likely in serial data transmission. For ex, Sender sends data at 10 MbPs, this means that bit lasts only for 1s and for a single bit error to occurred, a noise must be more than 1s.

-> Single bit error mainly occurs in parallel data transmission.

Ex; If 8 wires are used to send 8 bits of a byte, if one of the wire is noisy then single bit is corrupted per byte.

(ii) Burst Error : The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst error.

The burst error is determined from the first corrupted bit to last corrupted bit.

The duration of noise in burs error is more than the duration of noise in single bit.

Burst error are more likley to occure in serial data transmission.

The number of affected bits depends on the duration of the noise and date rate.

(2) Explain Random access and Slotted ALOHA.

-> Access to the medium from many entry point is called contention. It is controlled with a contention protocol.

-> In a random access method each station has the right to the medium without being controlled by other station. If one or more station tries to send, there is an access conflict, collision and frame will be either destroyed or modified.

* Slotted ALOHA

-> In this, the channel time is divided into time slots and the station are allowed to transmit at specific instance of time. These time slots are exactly equal to the packet transmission time.

-> All users are taken synchronized to these time slots, so that whenever user genrate a packet it must synchronized exactly with the next possible channel slot.

-> Transmission attemps for four network user and random retransmission delays for colliding packets in slotted ALOHA.

* Assumptions :

- All frames are of same size.
- Time is divided into equal size slot.
- Nodes start to transmit frames only at beginning of slot.
- Nodes are synchronized.

* Advantage

- Single active node can continuously transmit at full rate of channel.
- Highly decenterlized, each node independently decide when to retransmit.
- Simple to implement.

* Disadvantage

- Collision waste slot.
- Idle slot.

→ Throughput : $(S) = G \times e^{-G}$

Pure ALOHA	Slotted ALOHA
-> Frames are transmitted at arbitary time	Time is divided up into discrete slot, the frame is sent at the start of slot.
-> $S = G \times e^{-2G}$	Throughput (S) = $G \times e^{-G}$
-> Vulnereble time is 2 times the frame transmission time.	Vulnerable time is one half that of pure ALOHA.
-> Maximum utilization is 18.4 %.	Maximum utilization is 36.8 %.
-> Global time is not required.	Require global time for synchronization.
-> Simple to implement.	Implement is complex.
-> Can not used for Satalite, due to low utilization.	It is used in broadcast satelites.

(3) Explain Ethernet Frame Structure.

→ Basic frame format which is required for all MAC implementation is defined in IEEE 802.3 standard.

→ Ethernet frame start with preamble and SFD, both works at physical layer.

→ Ethernet header contain both source and destination MAC address, after which the payload of frame is present.

→ The last field CRC which is used to detect error.

Preamble	SFD	Destination address	Source address	Length or type	Data & padding	CRC

→ Preamble : A 7-byte pattern of alternating 0s and 1s used by the receiver to establish bit synchronization. Each frame contains the bit pattern 10101010. The pattern provides only alter and timing pulse.

-> SFD : SFD stands for start frame delimiter.
- The sequence 10101011, which indicates the physical actual start of the frame and enables the receiver to locate the first bit of the rest of frame.

-> DA : The DA field is 6-byte and specifies the station for which the frame is intended.
- It may be unique physical address, group address and global address.

-> SA : The SA field is 6-byte and contains the physical address of the sender of the packet.

-> Length : It is 2-byte field which indicates the length of entire frame.

-> Data : Data unit supplied by LLC. It is a minimum of 46 bytes and a maximum of 1500 bytes.

-> CRC : It contains error detection information

(4) Explain Functionality of Hub, Switch, Router, Gateway.

-> Hub : A hub is basically a multiport repeater. A hub connects multiple wire coming from different branches. For example, the connector in star topology which connects different stations.

Hubs can not filter data, so data packet are sent to all connected devices. In other words the collision domain of all host connected through hum remains one.

-> Switch : A switch is multiport bridge with a buffer and design that can boost its efficiency and performance.

A switch is data link layer device.

- The switch can perform error checking before forwarding data, which makes it very efficient.

- In other words the switch divides the collision domain of hosts but broadcast domain remains the same.

→ Routers : A Router is a device like a switch that routes data packet based on their IP adresses.
A Router is mainly a network layer device.
- Router normally connect LAN and WAN together and have a dynamically updating routing table based on which they make decision on routing the data packets.

→ Gateway : A gateway as name suggest is a passage to connect two networks together that may work upon different networking models.
- They basically work as the messenger aggents that take data from one system interpret it, and transfer it another system. Gateway are also called protocol converters and ~~enter~~ can operate at any network layer. These are genrally more complex than switches or routers.

→ Repeater : A repeater operates at physical layer. Its job is to regenirate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.

Repeaters do not amplify the signals.

[CRC]

(5) Explain Cyclic Reludancy check.

→ Parity method only detect odd number of errors. To overcome this weakness polynomial codes error detection method is used. Polynomial codes involve genrating check bits in the form of CRC.

→ The theory of polynomial code is derived from a branch of mathamatics called algebra theory. The theory of CRC checksum is devloped by using algebra and polynomials.
These polynomials are equations which have the form of power of x.

→ Polynomial codes are used with frame transmission ~~error~~ scheme. A single set of check digit is genrated for each frame transmitted, based on content of farme and is appeand by transmitter to the tail of the frame.

→ The receiver then perform a similar computation on a complete frame and check digit. If different answere is found that indicates an error.

→ Conversion polynomial to binary:

$x^7 + x^4 + x^3 + x^0 = 10011101$

→ The polynomial which represent data bit is called message polynomial, Usually shown as G(x).
There is second polynomial called genrator polynomial P(x).

Combine two polynomial P(x) and G(x) to produce CRC checksum polynomial F(x).

Ex. Genrate the CRC code for message 1101010101. Given $g(x) = x^4 + x^2 + 1$

~~$x^4 + x^2 + x + 1 = 10100$~~

→ $x^4 + x^2 + 1 = 10101$

```
10101 ) 11010101010000
        10101
        011110
         10101
         010111
           10101
           000100100
                10101
                0011100
                  10101
                  010010
                   10101
                   00111
```

Ex. Genrate the CRC code for message 1101010101. Given $g(x) = x^4 + x^2 + 1$

→ $g(x) = x^4 + x^2 + 1 = 10101$

```
10101 | 1 1 0 1 0 1 0 1 0 1 0 0 0 0
        1 0 1 0 1
        ---------
        0 1 1 1 1 1
          1 0 1 0 1
          ---------
          0 1 0 1 0 0
            1 0 1 0 1
            ---------
            0 0 0 0 1 1 0 1 0
                  1 0 1 0 1
                  ---------
                  0 1 1 1 1 0
                    1 0 1 0 1
                    ---------
                    0 1 0 1 1 0
                      1 0 1 0 1
                      ---------
                      0 0 0 1 1 0
```

Reminder : 0110

→ Message transmit :

```
  1 1 0 1 0 1 0 1 0 1 0 0 0 0
+                   0 1 1 0
-----------------------------
  1 1 0 1 0 1 0 1 0 0 1 1 0
```

(6) Explain CSMA/CD.

→ CSMA/CD stands for Carrier Sense multiple Acess / collision detection.

→ It is a media access control method that was widely used in early ethrnet technology (LAN) when there used to be shared bus topology and each computer were connected by table.

→ Consider a scenerio where there are 'n' station on a link and all are waiting to transfer data through that channel. In this case all 'n' stations would want to access the link to transfer their on data.

→ Problem aries when more then one station transmits the data at the moment. in this case there will be collision in data from different station.

→ CSMA/CD is one such technique where different station that follow this protocol agree on some terms and collision detection measure for effective transmission. This protocol decides which station will transmit when so the data reaches the destination without corruption.

* Working

Step 1: Check if sender is ready for transmiting data packets.

Step 2: Check if transmission link is ideal?
Sender has to keep on checking if transmission link is idle. For this it continuesly sense transmission from other nodes. Sender sends dummy data on link. If it does not receive any collision signal, this mean the link is idle at the moment.
If it senses that the carrier is free and there are no collision it sends the data.

Step 3: Transmit the data and check collision.
Sender transmits its data on link.
It doesn't use an acknowledgment system.
It checks for succesful and unsuccessful transmission through collison signal.
During transmission if collision signal is received by node, transmission is stoped.
The station then transmit the Jam signal onto the data link and wait for random time intervals before it resends the frame.

Step 4: If no collision was detected in propogation, the sender completes its frame transmission and reset the counter.