Computer Networks

↳ Why should know about computer networks and why we have to learn, why it is important?

1. Networking is everywhere.
2. Networks support the way we learn.
3. Network support the way we communicate.
4. Network support the way we work.
5. Network support the way we play.

Computer Network:

It is a set of nodes connected by communication links.

↳ Here nodes { computer, printer & any device }

↳ nodes that are capable of sending & receiving data.

↳ A communication link can be a wired link & wireless link:

↳ link carries the information.

End devices: ex: printer, PC, Tablet, phone

Intermediary devices: routers, & cell tower, modem

Internet cloud

↳ Basic characteristics of Computer Network.

1. Fault Tolerance
2. scalability
3. Quality of service.
4. security.

(1) Fault Tolerance:-

(i) Continue working without being effected by failure.

(ii) Ensure no loss in service.

(2) Scalability:-

(i) Grow based on the needs

(ii) Have good performance after growth.

Ex: Internet

(3) Quality of service:-

(i) set priorities for data packets.

(ii) Manage data traffic to reduce data loss delay etc.

(4) Security:-

(i) The ability to prevent unauthorized access misuse & forgery.

(ii) The ability to provide confidentiality Integrity, Availability.

Data Communication :

↳ Data communication are the exchange of data between two nodes via some form of link (transmission medium) such as a cable.

Data flow :

① simplex data flow :

↳ Communication is always unidirectional

↳ one device can transmit and the other device will receive.

↳ Ex: keyboards etc.

② Half Duplex data flow :

↳ Communication is in both directions but not at the same time.

↳ If one device is sending, the other can only receive, and vice versa.

Ex: walkie-Talkies

(3) Full Duplex (or) duplex data flow:

↳ Communication is in both directions simultaneously.

↳ Device can send and receive at the same time.

↳ Ex: Telephone line.

protocols

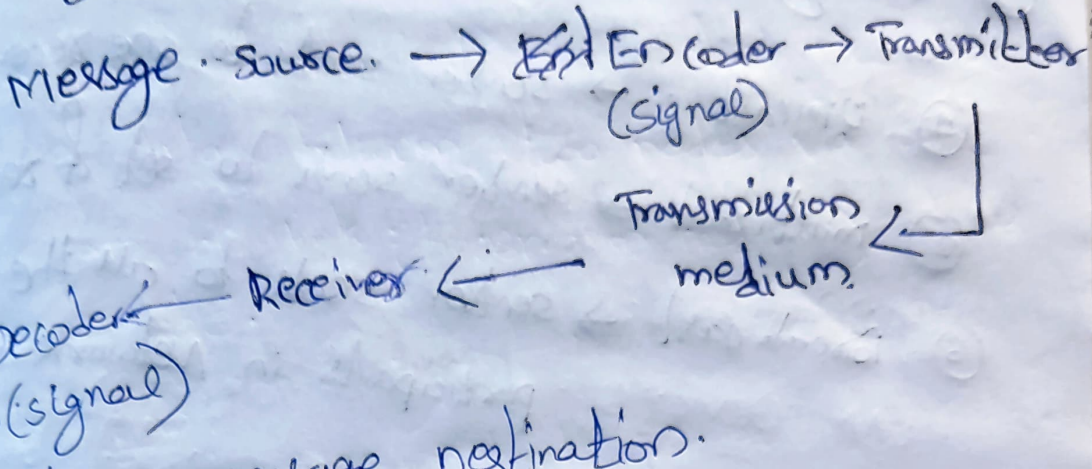
↳ protocols are the Rules that govern all methods of communication.

↳ schemes like (1) source (or) sender
(2) Destination (or) receiver.
(3) channel (or) media.

↳ protocols determine:-
(i) what is communicated in Network
(ii) How it is communicated in Network
(iii) when it is communicated in Network

↳ Elements of protocol are.
(1) Message encoding (4) message size
(2) Message formating and encapsulation
(3) message timing (5) message delivery options.

Message encoding :-



② Message Formatting and encapsulation :-

↳ Message should be in Agreed format.

↳ encapsulate the information to identify the sender and the receiver rightly.

③ Message size :-

↳ nodes break long messages into smaller parts or sentences.

④ Message timing :-

↳ protocol should control the flow between sender & receiver.

↳ Sender should wait for certain time to get acknowledgement from the receiver.

↳ protocal should also provide the response time.

(5) Message delivery options:

(1) Unicast → server sends to one receiver.

(2) multicast → server sends to set of receivers

(3) Broadcast → server sends to all the participants in Network.

peer to peer Network:

↳ All peers / devices are equal.

↳ No centralized Administration.

↳ Not scalable (no other devices are added to network)

client server Network:

↳ Centralized administration.

↳ It is Request-Response model.

↳ It is Scalable.

↳ But the server can be overloaded.

↳ peer to peer means → client to client.

↳ client-server may → client to server ⊙ vice versa.

Components of Computer network:

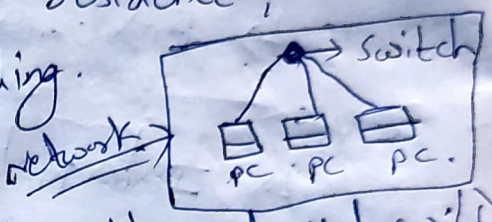
1. Nodes
   - ↳ End devices (pc, devices)
   - ↳ Intermediary nodes (router, modem)
2. Media
   - ↳ wired medium (guided medium)
   - ↳ wireless medium (unguided medium)
3. Services
   - ↳ e-mail ↳ online games ↳ voice over IP
   - ↳ storage services ↳ Video telephony ↳ file sharing
   - ↳ Instant messaging ↳ world wide web.

Classification of Computer networks

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide Area Network (WAN.

1) Local Area Network (LAN)

↳ A local Area Network (LAN) is a computer network that interconnects computers within a limited area such as residence, school laboratory or office building.



LAN Devices

↳ wired LAN (Example: Ethernet - Hub, switch)

↳ wireless LAN (Example: Wi-Fi)

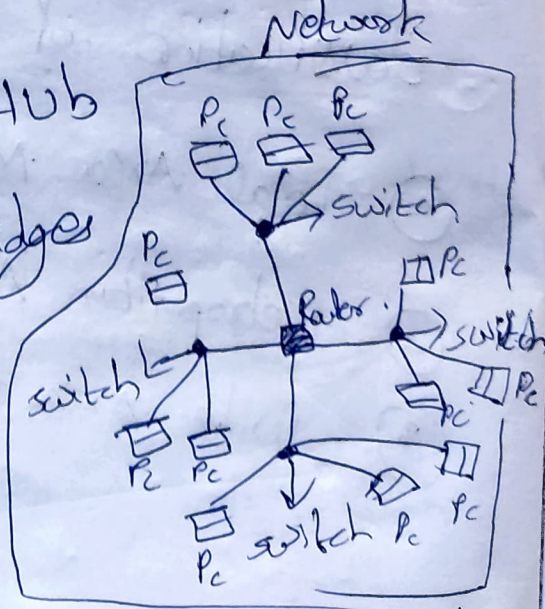
2) Metropolitan Area Network (MAN)

↳ A metropolitan area network (MAN) is a computer network that interconnects users with computers resources in a geographic region of the size of a metropolitan area (city)

MAN Devices

↳ Switches / Hub

↳ Routers / Bridges



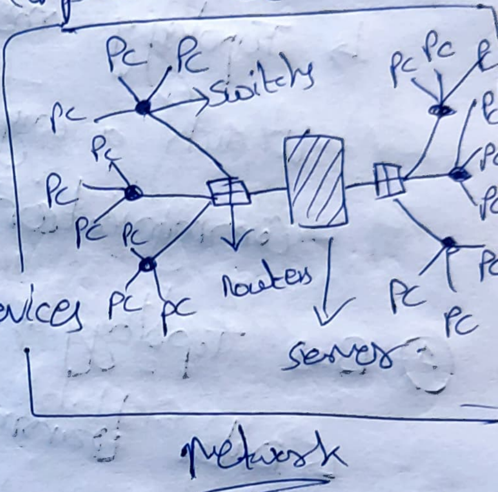
③ Wide Area Network (WAN)

↳ A wide area network (WAN) is a tele-communications network that extends over a large geographical area for the primary purpose of computer network.

WAN Devices

End devices &

Intermediary devices



④ The Internet (Wide wide Area networks)

↳ Country to Country / continent to continent.

⑤ Storage Area Network (SAN)

↳ Cloud computing

↳ It is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the users.

Network Topology

↳ Arrangement of nodes of a computer network.

↳ Topology = Layout.

↳ Topology means Arrangement of nodes in such a way that we have to make communication among all the nodes.

(1) Bus Topology :-

↳ Data transmitted between nodes in the network over the common transmission medium (or) Bus.

↳ Data can flow in both directions

↳ Advantages :-

↳ only one wire - less expensive.

↳ suited for temporary network

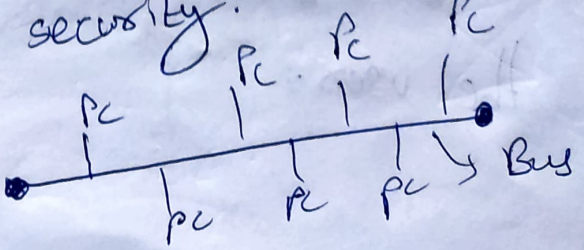
↳ Node failures does not effect others.

↳ disadvantages :-

↳ not a fault tolerant.

↳ limited cable length

↳ No security.



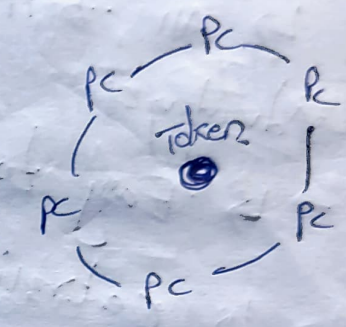
(2) Ring Topology

↳ It is a bus topology in a closed loop.

↳ peer-to-peer LAN topology.

↳ unidirectional.

↳ sending and receiving data take place with the help of TOKEN



↳ Here Token will be shifted from one pc to another; who ever has token theirs turn to send data..

↳ Advantages

↳ performance is better than Bus

↳ All nodes with equal access

↳ ~~dis~~Advantages

↳ unidirectional.

↳ If one node (or) link is failure then it will effect whole network.

↳ ↑ load → ↓ performance

↳ ~~AN~~ ~~node~~.

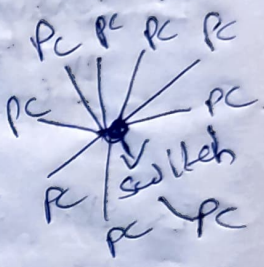
↳ No security.

3) Star Topology

↳ Every node is connected to a central node called a hub @ switch.

↳ centralized management

↳ All traffic must pass through switch @ hub.



↳ Advantages

↳ Easy to design.

↳ centralized administration

↳ scalable network.

↳ Disadvantages :

↳ switch is failed then network effects.

↳ switch is overloaded it will cause bouble.

↳ cost ↑ due to damaged switches.

4) Mesh Topology

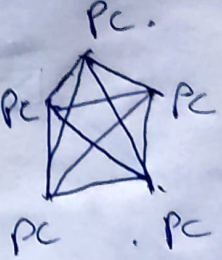
↳ Each node is directly connected to every other nodes in the network.

↳ Fault tolerant & reliable.

↳ Advantages :

↳ fault tolerant

↳ Reliable.



↳ Disadvantages

↳ Issues with Broadcasting.

↳ Expensive & Impractical for large networks

5) Hybrid Topology

↳ if there are one or more different topologies are their then it is called hybrid topology.

IP Address

↳ IP → Internet protocol

↳ Every node in the computer network is identified with the help of IP address.

↳ IP Address is a logical address because It can change based on the location of the device.

↳ Represented in decimal and it has 4 octents (X.X.X.X)

↳ 0.0.0.0 to 255.255.255.255 (32bits)

MAC addressing

↳ MAC → Media Access Control

↳ Every node in the LAN is identified with the help of MAC address.

↳ Ip Address → location of a person

↳ MAC Address → Name of the person.

↳ IP address are Router friendly.

↳ MAC address are switch friendly

↳ Switch identify the device using MAC address.

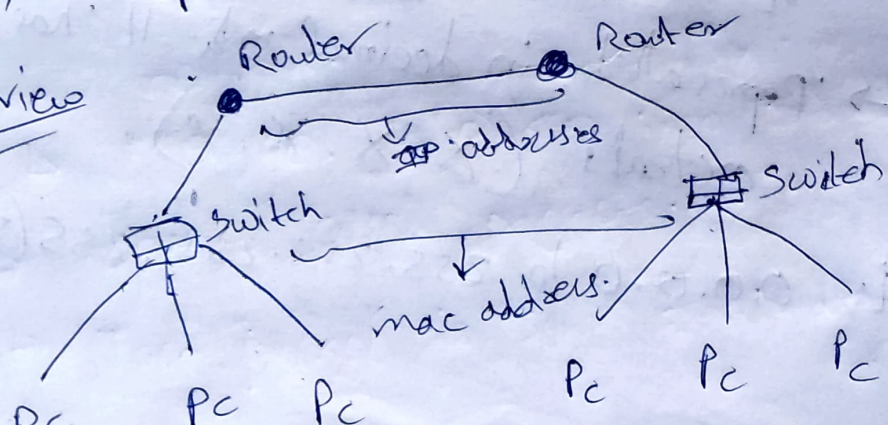
↳ MAC addresses are physical address because they cannot be changed.

↳ Assigned by the manufacturers.

↳ 70-20-84-00-ED-FC (48 bits)

↳ represented in hexadecimal.

overview



port number

↳ In a node many processes will be running.

↳ Data which are sent/recived must reach the right process.

↳ process is identified by port number.

↳ port → communication endpoint.

↳ Fixed port numbers → 25, 80, etc...

↳ Dynamic port numbers → (0, 65535)

switching

↳ switching in computer network helps in deciding the best route for data transmission if there are multiple paths in a larger network.

↳ one-to-one connection

1. circuit switching.
2. message switching
3. packet switching
   - ↳ Datagram approach
   - ↳ Virtual circuit Approach.

① circuit switching.

↳ A dedicated path is established between the sender and receiver.

↳ After that data transfer happens

↳ And After data transfer the dedicated path / connection is Disconnected.

② message switching.

↳ Store and forward mechanism

↳ Message is transferred as a complete unit and forwarded using store and forward mechanism at the intermediary node.

↳ Not suited for streaming media and real-time application.

③ packet switching.

↳ The Internet is a packet switched network.

↳ Message is broken into Individual chunks called packets.

↳ Each packet is sent Individually.

↳ Each packet will have source and destination IP address with sequence number.

↳ Sequence number will help the receiver to:
- ↳ Reorder the packets
- ↳ Detect missing packets
- ↳ Seeks acknowledgments.

↳ Datagram Approach

↳ Datagram packet switching is also known as Connectionless switching.

↳ Datagram Contain destination information and intermediary devices use this information to forward datagrams to right destination.

↳ Here path is not fixed.

↳ Intermediate nodes take the routing decisions to forward the packets.

↳ Virtual circuit Approach:

↳ It is also known as connection-oriented switching.

↳ A preplanned route is established before the messages are sent.

↳ Call request & call accept packets are used to establish the connection b/w sender & receiver.

↳ In this approach the path is fixed for the duration of a logical connection

Layers in Computer Networks

↳ We will decompose the network into more manageable components @ layers.

↳ It easy to understand.

↳ Easy to troubleshoot

↳ It provide more modular-design

↳ The protocols in each layer governs the activities of the data communication.

↳ Network edge:

↳ The network Interface that are accessible to end-users.

Ex:- Applications, skype, web etc.....

↳ Endsystems are nothing but host that are accessible to their own.

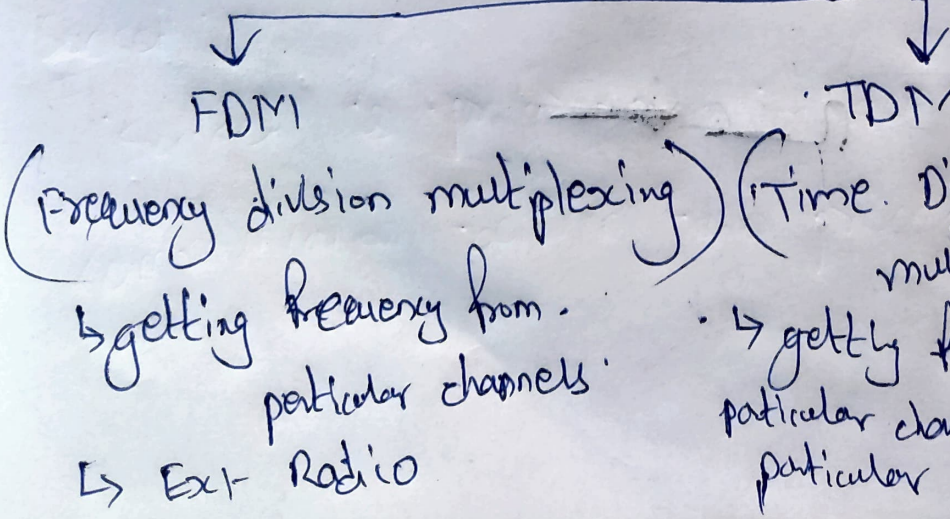
↳ Network Core:

↳ It is a collection of network hardware devices that provides the fundamental services for organization.

↳ This is done using

① circuit switching

② packet switching.



↳ How do loss and delay occur ?

① Transmission delay occur while router puts the packets in line @ air.

② queuing delay occur while queuing the packets in the line (waiting)

③ loss occur when the queue is full. then router will just drop the packets.

④ propagation delay is the short amount of time for a signal that will take access the medium.

⑤ processing delay the time that will take to find the address that packet will go.

⑥ Nodal delay

$$d_{nodal} = d_{process} + d_{queu} + d_{trans} + d_{prop}$$

↳ If average queuing delay increases then traffic intensity increases.

↳ Throughput is the rate (bits/unit time) at which bits transfered between sender & receiver. → (reality)

Malware

↳ Virus
↳ Worm
↳ Trojan Horse
↳ Spyware
↳ Botnet
↳ Denial of service Attack
↳ packet sniffing
↳ IP spoofing
↳ Record & playback attack.

Socket

Socket is programming interface for communication between two process.

Bandwidth (Capability)

↳ Maximum amount of data that can be transmitted per second.

(OR)

↳ The bandwidth of a network is given by the number of bits that can be transmitted over the network in a certain period of time.

Latency delay : (Nodal delay)

↳ The latency (OR) delay defines how long it takes for an entire message to completely arrive at the destination from the time, the first bit is sent out from the source.

Latency = Transmission delay + propagation delay + Queuing delay + processing delay.

$$\text{Trans.de} = \frac{\text{Message size}}{\text{Bandwidth}}$$

$$\text{prop.de} = \frac{\text{Distance}}{\text{propagation speed}}$$

Quede. = Traffic ↑ = Queue ↑

procede. = processing message time.

Round trip time = 2 × Tp.

OSI Model (open system Interconnection)

↳ It is a model of understanding and designing a network architecture that is flexible, robust and interoperable.

↳ It is a Reference model which will help to build the network architecture.

↳ OSI model was never fully implemented.

TCP/IP model (Transmission control protocol/Internet protocol)

↳ The TCP/IP protocol suite was developed before OSI model.

↳ TCP/IP is a hierarchical protocol made up of interactive modules.

purpose of OSI model

↳ The purpose of OSI model is to facilitate communication between different systems without requiring changes to the logic of the device hardware and software.

For Example if you want to send the password to another user, which should not know to any one.

↳ In OSI Reference model architecture

↳ Application layer → password will be sent

↳ presentation layer → password will be encrypted to some jumbled data.

↳ session layer → password will be changed according to syntax & scematics, sync

↳ Transport layer → TL Info + password (encrypted)

↳ Network layer → NL + TL + encrypted password.

↳ Data link layer → DL + NL + TL + encrypted password.

↳ physical layer → These all Info change binary bits (10 tool to 1110101---)

↳ It knows which medium it is connected to.

① Application layer :-

↳ It enables the user to access the network resources.

↳ like File transfer, Access management, mail services, Directory services - etc.

② presentation layer :-

↳ It is concerned with the syntax and semantics of the information exchanged b/w two systems.

↳ Translation → Converting data to Agreed format

↳ Encryption → encrypted syntax

↳ Compression → reduce the no of bits.

③ session layer :-

↳ It establishes, maintain and synchronize the interaction among communicating devices.

↳ Dialog control → It helps in process communication

↳ synchronization → It helps in the synchronization of data which transferring

(4) Transport layer:

↳ It is responsible for process to process delivery of the entire message.

↳ port addressing

↳ segmentation and reassembly.

↳ Connection control

↳ End-to End control

↳ Error control (in b/w two nodes)

(5) Network layer:

↳ It is responsible for delivery of data from the orginal source to the destination network.

↳ logical addressing / Ip addressing

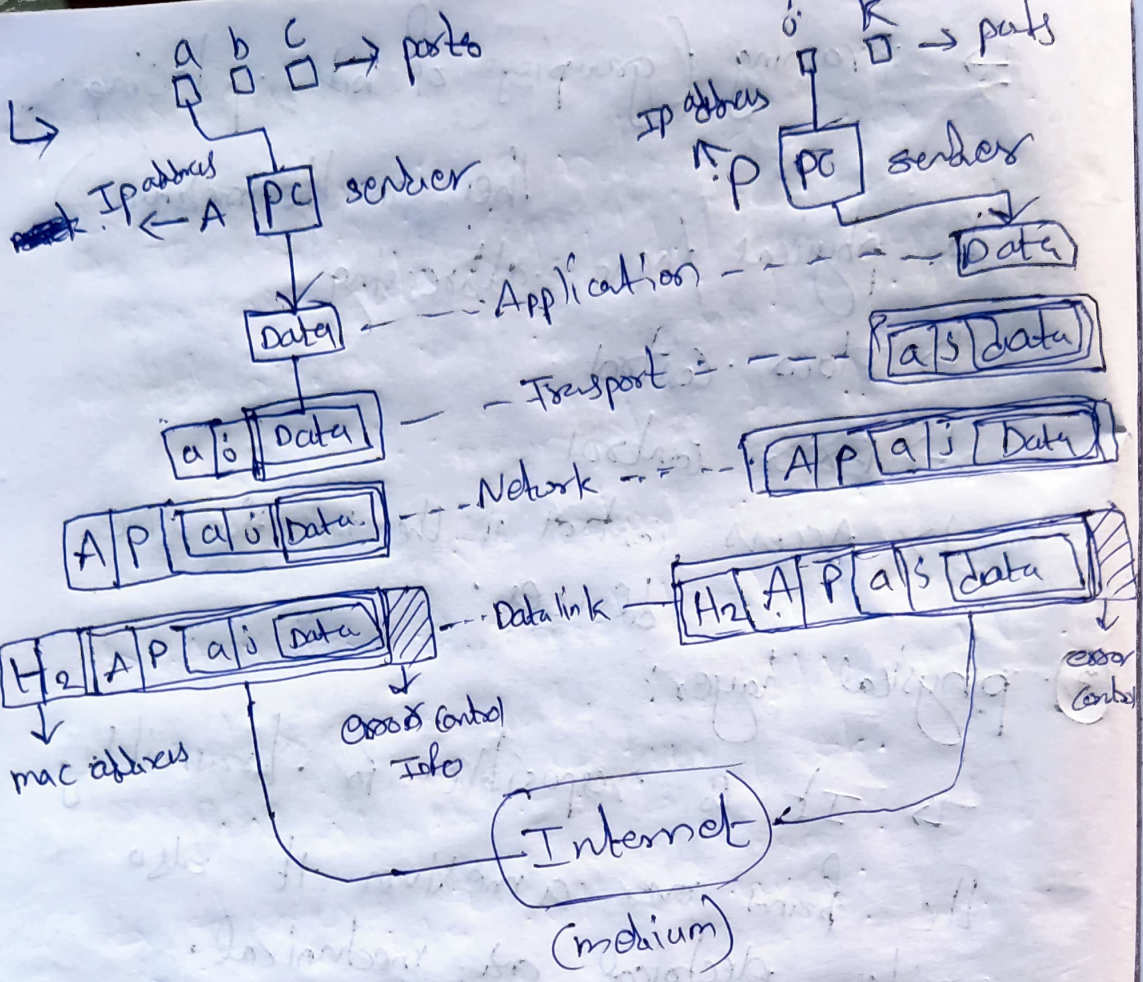
↳ Routing (Find the best route)

(6) Data link layer:

↳ It is responsible for moving data from one node to another node.

↳ Framing (grouping of bits & placing them in the medium)
↳ physical / MAC addressing
↳ Flow control
↳ Error control
↳ Access control if the more than one devices

⑦ physical layer:
↳ It is responsible for transmitting the frame over a medium it also provide electrical and mechanical.
↳ Defines the type of media.
↳ Representation of bits
↳ Data rate → no of bits per sec
↳ synchronization of bits (sender & reciver)
↳ Line configuration
↳ dedicated path to one node
↳ common path to multiple nodes
↳ physical topology.
↳ Defines how devices are connected over network.
↳ Transmission mode (simplex, half duplex, duplex)



↳ Application
presentation
session } → Application → HTTP, DNS, DHCP, FTP

Transport → Transport → TCP, UDP

Network → Internet → IPV4, IPV6.

Data link
physical } → network Access → PPP, frame Relay, Ethernet

protocol Data Unit (PDU)

↳ protocol Data unit (PDU's) are named according to the protocols of the TCP/IP model.

- ↳ Application layer → Data
- ↳ Transport layer → segment
- ↳ Network layer → packet
- ↳ Data link layer → Frame
- ↳ physical layer → Bits.

CMD - commands

↳ Ipconfig → view Ipaddress

↳ Ipconfig /All → view MAC addresses and other info

↳ Ping → we can send message to destination Ipaddress and get acknowledgement.

↳ Tracert → route from source node to destination node.

↳ nslookup → we can know the Ipaddress of the given website name.

Router :

↳ A router is a networking device that forwards data packets between computer network.

↳ like communication b/w two different local area networks works.

↳ A router is connected to at least two networks, commonly two LANS, WANS or LAN and its ISP's network.

↳ It is inter network layer.

Repeater :

↳ It regenerates the data between two switch, so that data can not be lost.

Bridge :

↳ It is also Repeater but the Functionality of reading MAC address is added.

↳ It is a layer 2 device.

Network Devices

↳ Repeater → layer 1 (physical) (regenerates)

↳ Hub → layer 1 (physical) (Broadcasting)

↳ switch → layer 2 (Datalink) (unicasting) (saves mac address)

↳ Bridge → layer 2 (Datalink) (Regenerates & Mac address)

↳ router → layer 3 (network) (works on Ip addresses)

↳ Multi-layer switch (layer 3 switch)

↳ works as layer 3

↳ also works as layer 2

↳ Brouter → combination Bridge & router.

↳ modem →

↳ modulator → digital info is carried by Analog signal

↳ demodulator → retrieves the info

↳ Firewall (security Device)

physical layer:

↳ The data is communicated b/w the nodes

↳ Here data will be converted into signals inorder to pass through the medium.

↳ These conversion of data is done physical layer of OSI (or) TCP/IP model.

principles of physical layer:-

↳ It moves data in the form of electro-magnetic signals across a transmission medium.

↳ The data is converted into the format that should be understandable for the medium.

↳ For ex:- Image must be changed to a for that transmission media can accept.

↳ signal:- It is a function represents the variation of physical quantity with respect to time.

① Analog signal:- All real-life signals are analog in nature.

(ii) Digital signal.

↳ In a given time if it take only finite values then it is Digital signal.

↳ Here In physical Layer the bits are converted to signals and transmitted thrugh signals.

↳ Their can be Wired media.

↳ Electrical signals through Copper cable.

↳ Light pulses fibre optic cable.

↳ wireless media.

↳ micro wave signals.

wired media → Copper cable.

→ Fiber optic cable.

wireless media → Antennae, Radia, NICs

Access points.

Data link layer :

↳ when network layer creates a packet it gives that packet to the data link layer inorder to add header & trailer. then network layer PDU converts to frame.

↳ Data link layer moves the frames from one node to another by encapsulating the physical address of the source and physical address of the destination in it.

↳ Framing
↳ physical Addressing
↳ Flow control
↳ Error control
↳ Access control.

Framing → grouping of bits into frames so that each frame is distinguishable from another.

physical Addressing :→ A frame is the encapsulation of header and trailer information with the packet.

↳ header contains (source & destination MAC address)

Flow Control :→

↳ Flow control will be end to end.

↳ speed matching mechanism.

↳ Flow control coordinates the amount of data that can be sent before receiving an acknowledgement.

Access Control :→ It controls the media between end to end.

Error Control :→

↳ Error detection.

↳ Error Correction.

↳ Data link layer

↳ logical link control (LLC)

↳ flow control → control info is added to packet.

↳ Media Access Control (MAC)

↳ framing, MAC addressing.

Error control, Access control

↳ Here Header & Trailer added.

↳ Framing is done between nodes. In two types.

① If sender and receiver knows the size of the frame.
   ↳ fixed size framing.

② The size of each frame to be transmitted may be different
   ↳ Variable size framing.
   ↳ Here we use additional mechanisms like we mask end & beginning of the frame and identify.

↳ These will be done in two ways

① Bit oriented approach.
   ↳ frame as a collection of bits.
   ↳ protocol :- HDLC
      (High-level Data link Control)

② Byte-oriented Approach.
   ↳ frame as a collection of bytes.

↳ protocol :-

① BISYNC.
(Binary synchronous communication protocol.)

② DDCMP.
(Digital data communication Message protocol)

③ PPP
(point-to-point protocol)

③. clock Based framing
↳ It is mainly for optical framing.
↳ protocol :- (SONET)
↳ (synchronous optical network)

HDLC protocol:-

↳ HDLC protocol is used in Bit oriented approach. It is very powerful protocol it has

because.

① Beginning & ending sequence (01111110)

② Header → Address & Control field

↓

tells type of frame

③ Body → payload (variable size)

④ CRC :→ cyclic Redundancy check.

↳ Error Detection.

↳ If the Beginning & ending sequence is present in body (data part) then receiver thinks that it is the ending sequence and leads to framing error.

↳ For that bit stuffing is needed. Here in bit stuffing when ever the sequence is found in body part it just keeps the '0' after '5' ones in the sequence. (01111110 → 011111010)

Bisync protocol:

↳ This protocol is used in Byte oriented approach it is very powerful protocol.

↳ It has cyclic Redundancy check for error detection.

↳ Here if framing error occur then Byte stuffing is involved.

PPP protocol:

↳ PPP is a WAN protocol and which is commonly run over Internet links.

↳ It is used in broadband communication having heavy loads and high speeds.

↳ Flag (1 byte) is used beginning and end of frame.

↳ protocol → tells type of data contained in
- Network layer pdu.

↳ checksum → It is used for error detection.

↳ Byte stuffing is need if framing error occurs.

DDCMP (protocol)

↳ It is a byte - counting approach.

↳ There will be a Count field in the frame. (That tells how many bytes or Container in the frame body.)

Error detection :

① Bit Error

↳ 1 bit in the data unit has been corrupted

② Burst error

↳ 2 or more bits in the data unit has been corrupted.

↳ To detect or correct errors, we need to send some extra bits with the data.

↳ The extra bits are called as redundant bits.

↳ If the redundancy bits are matched then receiver ~~acks~~ accepts it or ① it will ask to retransmit it. ② It can be corrected using error-corrected code.

Error detection techniques:-

(1) Vertical Redundancy check (VRC)
↳ It generates a parity bit.
↳ Even and odd ones → 0
↳ It is powerfull in Bit error
↳ It is not powerfull in Burst error.

(2) Logitudinal Redundag check (LRC)
↳ A block of bits is organized in rows & columns
↳ It generates a Two Dimensional parity
↳ The parity bit is calculated for each column and set along with the data.
↳ odd no → 1
↳ Even no → 0

↳ If two bits in one data units are damaged and two bits in exactly the same positions in another data unit are also damaged then LRC checker will not detect an error.

Ex:- 1 1 1 0 0 1 1 1
1 1 0 1 1 1 0 1
0 0 1 1 1 0 0 1
LRC 1 0 1 0 1 0 0 1
1 0 1 0 1 0 1 0

(3) Checksum → Receiver ⇒ 1's means no Errors.

↳ It will break the original message into 'k' number of blocks with 'n' bits in each block.

↳ It will sum all the 'k' data blocks.

↳ Add the carry to the sum if any.

↳ It will apply 1's complement to the sum = checksum.

↳ It is very powerful Algorithm.

(4) Cyclic Redundancy check (CRC)

↳ Find the length of the divisor = 'L'.

↳ Append 'L-1' bits to the original message.

↳ perform binary division operation

↳ Remainder of the division = CRC.

↳ If the receiver gets all 0's at the Remainder then that mean no error are present.

Flow Control

↳ speed should be matching b/w sender & receiver.

↳ It coordinates the amount of data that can be sent before receiving an acknowledgment

protocols

- noiseless channels
  1. simplest
  2. stop & wait
- Noisy channels
  1. stop & wait ARQ
  2. Go-Back-N ARQ
  3. selective Repeat ARQ

1. stop-And-wait protocol.

↳ After transmitting one frame, the sender waits for an acknowledgement before transmitting the next frame.

↳ problems:

↳ if a data is lost then network is useless.

↳ if a Acknowledgement is lost then next will not be sent.

↳ if the Acknowledgement is delayed then it considers as ack of some other packet.

② Stop-And-wait protocol (ARQ)

↳ if the acknowledgement does not arrive after a certain period of time, the sender times out and retransmits the original frame.

↳ Go-Back-N-ARQ & Selective Repeat ARQ are sliding window protocols.

③ Sliding window protocol

↳ drawbacks of stop-and-wait-ARQ

① one frame sent at a time.

② poor utilization of bandwidth.

③ poor performance.

↳ It sends multiple frames at a time.

↳ No of frames to be sent is based on window size.

↳ Each frame is numbered (sequence number)

Go-back-N-ARQ

↳ It is a sliding window protocol

↳ The number of frams that can be sent depends on the window size of the sender

↳ If the acknowledgment of a fram is not received with an agreed upon time period, all frams in the current window are transmitted.

Selective Repeat ARQ

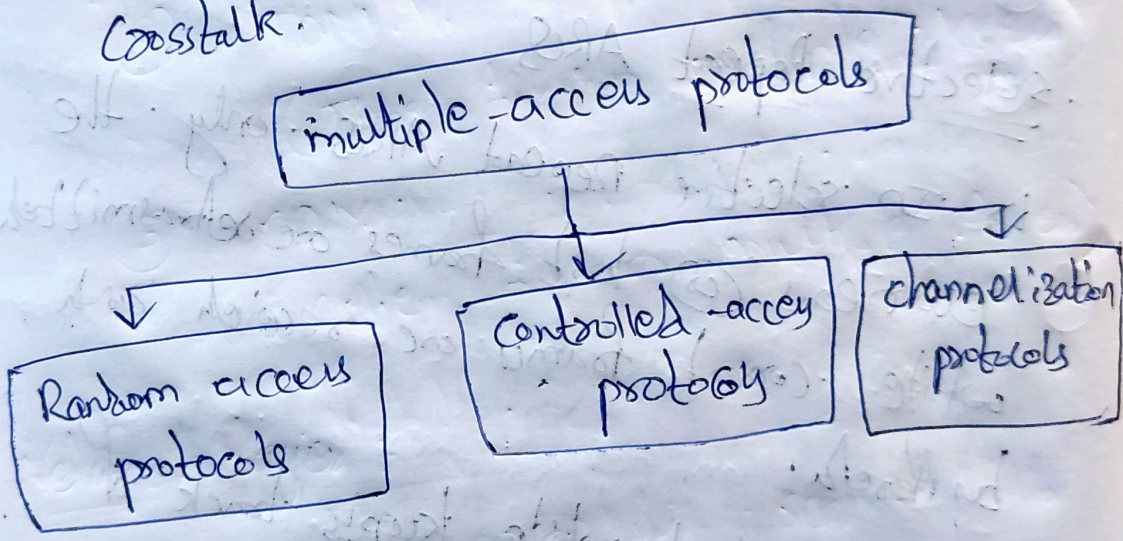
↳ In selective Repeat ARQ only the erroneous (or) lost frames are retransmitted while correct frams are received and buffered.

↳ The receiver while keeps track of sequence numbers, buffers the frams in memory and sends NAck for only fram which is missing (or) damaged.

Access protocols

↳ If there is a dedicated link b/w the sender and receiver then dat link control layer is sufficient but if there is no dedicated link present then multiple stations can access the channel simultaneously

↳ Hence multiple access protocols are required to decrese collision and avoid crosstalk.



Random access protocols

1. ALOHA
2. CSMA (Carrier sense multiple Access)
3. CSMA/CD (Carrier sense multiple Access with collision detection)
4. CSMA/CA (Carrier sense multiple Access with collision Avoidence)

↳ Here All the stations have same superiority that is, no station has more priority than another station. Any station can send data depending no medium's state.

↳ Here each station has the right to the medium without being controlled by any other station.

Controlled access protocols

↳ Here stations consult one another to find which stations has the right to send.

↳ A station cannot send unless it has been authorized by other stations.

(1) Reservation
(2) polling
(3) Token passing.

Channelization protocols

↳ In this method the available bandwidth of a link is shared in time, frequency (or) through code, between different stations.

(1) FDMA (Frequency division multiple Access)

(2) TDMA (Time division mutiple Access)

(3) CDMA (Code division multiple Access)

Network layer :-

↳ Here sender encapsulate segments into datagrams (or) packets.

↳ Here Network layer pdu is datagrams (or) packet.

↳ Network layer protocols are present in every host, router and servers.

↳ we have two network layer functions.

(1) Forwarding

(2) routing.

↳ Forwarding → moving packets from router's input to router output.

↳ routing → finding the route taken by packets from source to destination

↳ Routing Algorithm determines ends to ends path through network.

↳ Forwarding table determines local forwarding at the router.

↳ In Datagram forwarding table consists of destination ipaddress and route.

↳ packets forwarded using destination Ip address.

↳ (1) source Ip address

(2) destination Ip address.

↳ How Routers are deciding Ipaddresses and store them?

↳ There will be address ranges for every interface.

↳ In routers the packets will be forwarded using destination address and longest address prefix.

↳ First 21 bits will be match and last bits will decide the Ipaddresses.

↳ If the two Ipaddresses are same then longest address prefix will decide where should it go.

↳ Router Architecture

↳ Input ports → datagrams/packets Enter

↳ output ports → datagrams/packets exit.

↳ Routing determines the routing path. By routing Algorithms like RIP, OSPF, BGP etc.

↳ Forwarding datagrams from input to output ports by high-speed switching fabric.

↳ Here Routing processor will compute the routes and tells high speed switching fabric how to forward the packets from input to output port.

Working of Input ports

↳ In Input port line termination is done.

↳ In Input port link layer protocols are Active.

↳ In Input port queuing is done.

↳ Forwarding table works

↳ If line speed is ↑ and forwarding speed is ↓ then packets will drop

↳ Here comes switching fabric that transfers the packet from input port to output port.

↳ There are Three types of switching fabrics.

① memory ② Bus ③ crossbar.

① memory switching
↳ packets are copied to system memory and then moves to output port.
↳ Limited by memory bandwidth.

② Bus switching
↳ By shared Bus, it will transfers the packets.
↳ Here Bus Bandwidth is limited.

③ cross-bar switching.
↳ Fragmenting datagrams into fixed length cells and switches through fabric.
↳ cross bar bandwidth is limited.

Working of output ports
↳ Buffering is done when datagrams arrive from fabric.
↳ queuing is done if packets is loss.
↳ Head of the line Blocking may occur while queuing.

Ip datagram Format

1. Ip protocol version
2. Header length
3. time to live
4. datagram length
5. check sum
6. Source Ip address
7. destination Ip address

↳ If the datagram is large then the Ip datagram is divided into several datagrams and they will reassemble only at final destination. (MTU)

↳ Interphase is a connection b/w hosts & physical link.

↳ routers have multiple interphases

↳ hosts have one or two interphases

Transport layer

↳ Transport layer is providing a logical communication between process running on different hosts.

↳ It is a end to end protocol.

↳ In Transport layer we use TCP & UDP protocols are used.

↳ Transport layer is nothing but collects & Distribute to the users.

↳ This is done in two ways

① multiplexing → Taking data & pushing it to one channel.

② Demultiplexing → Taking data and pulling from one channel.

↳ Here port number is used to find the destination in the other host to send data.

↳ In transport layer of demultiplexing:

↳ Ip datagrams stores source IP Address and IP Address and segment.

destination

↳ segment will store source port number & destination port number.

Demultiplexing

↳ Here UDP (user datagram protocol) identifies the 2 things

① destination IP Address

② destination port number

↳ In UDP socket consists of dest IP address and port number as IF the UDP segment have same dest ipaddress and port number then segment will be directed to the same destination socket.

↳ we use checksum at data like layer but their is no gaurenty has reliable. so it can be (ossepted in router, so we used checksum at trasport layer also.

Application layer:-

- Message type.
- Message syntax
- Message semantics
- message Rules.
- protocols used in Application layer
  1. HTTP
  2. FTP
  3. SMTP
  4. Bit torrent.
- Application layer provides communication b/w two processes.
- DNS plays a vital role in Application layer.
  - Domain name system.
  - use map IP address and names.
  - It is Distributed everywhere.
  - Hierarchal distribution.
  - It is one type of database
  - port no is 53.

↳ DNS decrease the traffic volume.
↳ It could not be destroyed.
↳ It is Easy to mainten.
↳ one server goes down other may be work.
↳ DNS return the IpAddress to the hostname.
↳ DNS supports common names.
↳ DNS gives unique IP addresses and give different one.
↳ It can be accessed by TLD.
. TLD → Top level Domain. like com, org, net, edu --- etc.