* Network

- Network is the collection of two or more system that are connected to each other through a transmission media.
- Computers are connected to each other through a network so that they can communicate with each other.
- ~~They are~~ The network is essential between the computer ~~to~~ in order to share resources (such as printer and CDs), exchange file or allow electronic communication.
- The computer on a network can be linked through cables, telephone lines, radiowaves, satellite or infrared light beam.
- Network can be private or public.

→ Advantage of Ad Network

1. Easy Communication

It is very easy to communicate through network. We ~~people~~ can communicate efficiently using a network with many users. We can enjoy the benefits of emails, instant messaging, telephony, chat, etc.

2. Ability to share file, data and information.

We can find and share data and information

ROUGH

- because of networking.

3. Sharing Hardware

- Network provide ability to share hardware. for ex- a printer can be share among the user in a network so that there is no need to have individual printers for each and every computer in a company.

4. Sharing Software

- User can share software within the network easily.

5 flexibility

6 Reliablity (believable)

7. Security

- Sensitive files and program are password protected. Then those file cannot only be access by the authorized users.

8. Speed

- Sharing and transferring files within network is very rapid, depending upon the type of network.
- This will save time.

9 Data is easy to backup as all the data ~~are~~ is stored in file server.

⇒ Disadvantage of Networking

1. Expensive to build
- Purchasing the network cabling and file server can be expensive
2. Prone to Virus, hacker
- Virus can spread to other computer through out a computer network. and there is also a danger of hacking with wide area network.
3. Security threats
- It is always create problem ~~in~~ with large network.
- There are hacker who are trying to steal valuable data of large companies for their own benefits. So it is necessary to take care of security
4. Cable may break:
- when cables are breakdown, it can stop the entire network.

* Peer to Peer Network/Architecture

- Peer to Peer ~~Net~~ is a network which is suitable for small networks having less than 10 computers
- In Peer to Peer network, strictly security is

is not necessary
- All computer have the same status. There is no master or controller in this computer network.
- Each computer act as independent workstation and maintaining its own security that shares data on its own disk but can share it with all other computer on Network.

Advantage

1. Easy to set up
2. less expensive and easy to install
3. Doesnot require any server
4. Since each computer is master of its own, they are ~~independent~~ not depend on other computer for their operation
5. Doesnot require strict Security.

* Client Server Network/Architecture
- It is a computer networking model which is designed for end user - client to access resources from a central computer - Server
- Client can retrieve data that are stored on the server
- Server is a specialized computer that control the network resources and provide services to all other computer in the

network.

- A server perform all the major operation like security and network management.
- All the client communicate with each other through server. for ex 1
- If client 1 wants to send data to client 2, it first send request to server to seek permission for it. The server then send signal to client 1 allowing it to initiate the communication.
- A server is also responsible for managing all the network resources such as file, applications and shared device like printer etc.
- So if any client wants to access these services, it first seek permission from the server by sending a request.

Advantage

1. Possibility of Back-up and recovery.
2. Have security
3. Performance - use of dedicated server, improve the performance of the whole network.
4. All files are stored in central location
5. Upgradation - changes can be made easily by just upgrade the server

*-Network classification

* Diff btw Peer-Peer Ntwk and Client Server Netw

Peer to Peer Network	Client Sever Netwo
1 Easy to set-up	1. Difficult to set-up
2. less expensive to install	2 More expensive to install
3. Very low level of security.	3. High level of Security
4. less than 10 computer is suitable	4. No limit to the no. of computer
5 Doesnot require server	5. Require a server

* Classification of Network

There are various classification of Network

1. PAN

- PAN stands for Personal Area Network.
- Personal Area network is a computer netwo used for transforming data such as computer, telephones, printer in very shorter distance that are located to single person. or in a single building
- PAN has connectivity range up to 10 metres

- Example

Internet hotspot which may connect up to 8 devices connected with a single hotspot

Advantage

- Efficient, cost-effective and ~~convite~~ convenient.
- Security because it is controlled by single person.

Disadvantage

- Shorter distance upto 10 m only.
- Data rate is low upto other network

2 MAN.

- MAN stands for Metropolitan area network.
- MAN is a network that interconnects users with computer resources in large area like city.
- MAN has connectivity range upto 100 metre.
- MAN cover area less than WAN but more than PAN.
- ~~for example~~

Advantage

3 ~~WAN~~ . wider area than PAN.

. Information can be transfer widely and rapidly

Disadvantage

. Cost is higher than LAN

ROUGH

- Difficult to manage

3. MAN
- MAN stands for wide area network

3. LAN
- LAN stands for local area network
- LAN is a network that interconnect ~~computer~~ users with computer resources is small area like buildings or group of buildings in same office etc.
- It is widely used to connect personal computer and workstation in company offices.

Advantages
- lower in cost
- Sharing resources
- High speed
- Security.

Disadvantage
- Area is limited
- when no. of nodes increases then performance become decreases.

4. WAN
- WAN stands for wide area network.
- A WAN is a network used to transmit

data and information over large geographical distance which may even entire countries and continents.

- A WAN may contain multiple smaller network such as LANs or MANs.

Advantage

- have large geographical area

Disadvantage

- Complex and complicated
- High cost
- Require high performance device
- low security

* Transmission Media

- Transmission media is a pathway through which data can be transmitted from sender to receiver.
- Transmission media is a physical media through which communication take place in computer network
- Transmission media is of 2 type

1. ~~Wir~~ Guided transmission Media

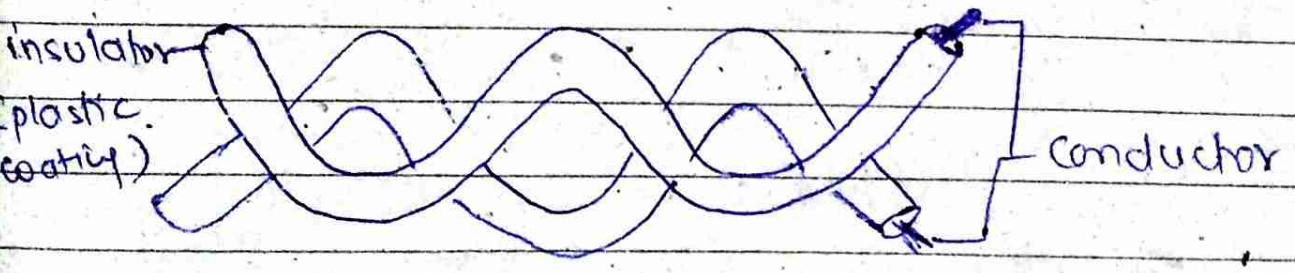
- It is also known as wired or bounded transmission media.
- In Guided media, cables or wire are

are used to connect computer to transfer information.
- Electromagnetic signals travel through this physical media to communicate the computer.

→ Type of Guided transmission media.

1. Twisted pair wire

- A twisted pair wire consist of two conductor (normally copper), each with its plastic insulation, twisted together.
- This twisted pair decrease the crosstalk (unwanted signal) inteface.
- This cable is most commonly used in telecommun ication.
- It is lightweight, cheap, easy to install, and support many diff type of network.



- Twisted pair is of two type

(a) Shielded twisted pair

- This cable have has a metal foil or fine wire mesh covering surrounded the wire to protect the transmission.
- It can improve the signal rate and reduce crosstalk.

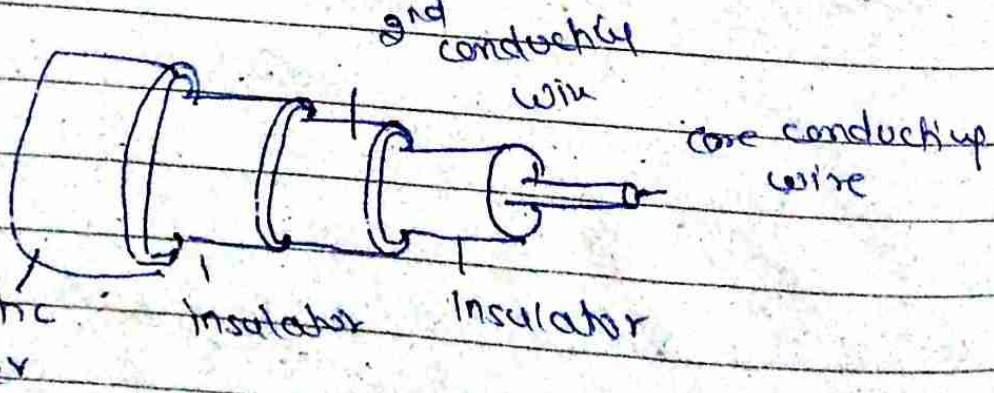
ROUGH

① Unshielded twisted pair (UTP)

- It does not contain any metal coating outside the wire
- UTP is the copper media inherit from telephony which is being used for telephony increasing higher data rates.

② Co-axial wire/cable

- Coaxial cable has two wires of copper. The core wire lies in the center and it is made of solid conductor. The core is enclosed in an insulated sheath.
- The second wire is wrapped over the sheath that shield against noise. This wire is also enclosed in an insulated sheath.
- The whole cable then covered by a plastic cover



- This cables carries high frequency range

3. Optical fibre

- Optical fibre works on the properties of light.
- The core of optical fibre cable is made of high quality glass or plastic.
- from one end of it light is emitted, it travels through it and at other hand light detector detect light stream and converts it to electric data.
- It has highest mode of speed. It comes in 2 mode
  - (a) Single mode - which can carry a single ray of light
  - (b) multimode - it is capable of carrying multiple beams of light.
- To connect and access optical fibre cable, Spectal type of connectors are used ie SC- Subscriber Channel, Straight tip (ST) or MT-RJ.

(2) Unguided transmission media

- It is also called wireless communication.
- It doesnot require any medium to transmit electromagnetic signals.
- In unguided media, the electromagnetic signals are transmitted through broadcasting through

air to everyone.
- It is also known as unbounded media as it doesnot have any border limitation.
- The unguided media allows the user to connect all the time as the communication is wireless.

→ Types of Unguided transmission media

1 Radiowave Unguided Transmission Media
- Transmission making use of radio frequencies is called radio wave transmission
- Any radio setup has two part
  ① Transmitter
  ② Receiver
- The transmitter takes some sort of messages encoded it onto a sine wave and transmit it with radio wave.
- The receiver receives the radiowave and decode the message from the sine wave it receives.
- Both the transmitter and receiver use antenna to radiate and capture the radio signal.

2 Microwave
- Microwave uses high frequency band of a radio broadcasting transmission to transmit the data.

- It uses ~~dise~~ a dish shape antenna for sending and receiving the data.
- Microwave are also called line-of-sight because the microwave signal cannot bend around the surface of the earth.
- Hence, transmitter and reciver of a microwave mounted on a very high tower in a line of sight.
- This type of Communication is not possible in longer distance. Whenever it is used for longer distance, a separate device called repeater is used to amplify the signal.
- Installing cost is high

3 Infrared

- Infrared uses red light to transmit information.
- ~~The wireless remote controls used with appliances such as TV etc with Infrared~~
- the common appliances of it is in television and VCR's with a remote control.
- Infrared is used to connect the local area network in the same room.

* Diff btw Guided and Unguided Media

Guided Media	Unguided Media
• IEEE standard for ethernate network is 802.3	• IEEE standard for unguided network is 802.11
• Devices are connected physically, through cables or wires.	• Devices are not connect physically
• The signal require physical path for transmission.	• Signal is broadcasted through air.
• It provide direction to signal for travelling	• It does not provide any direction.
• More Secure	• less Secure
• Difficult to manage	• Easy to manage
• Provide high speed data transfer	• Provide less speed data transfer.

* Network topology

• Network topology is the arrangement of a network including its nodes and connecting lines.

• Network topology defines the layout, virtual shape or structure of Network.

- The Network topology determines the way in which various systems are connected and communicated with each other.

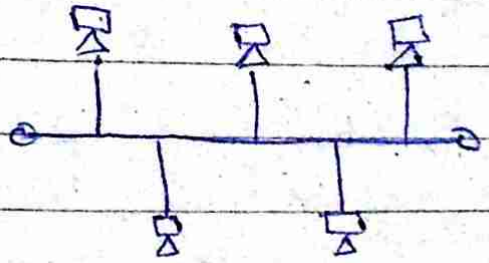
Various type of topology

1. Bus topology

- In bus topology, every computer or network devices is connected to a single cable called a trunk.
- Bus must be terminated at both end to eliminate signal bounce.
- Data is sent to all computers on the trunk.
- Every computer examine every packets on the wire to determine who the packet is for and accept only messages addressed to them.
- Repeater can be used to regenerate signals

Advantage

- It is cost effective
- It is easy to understand
- Easy to Expand
- less no. of Cable required
- Use in Small network



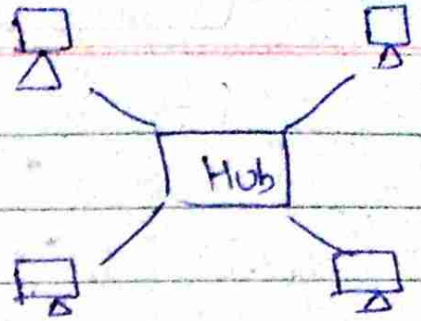
ROUGH

Disadvantage

- Cables fails then whole network fails.
- become slow by heavy network traffic.
- Cable has limited stength.
- Difficult to troubleshoot a bus because cable break or loose connector will cause reflection and bring clown the whole network.

2. Star topology

- In star topology all the computers are connected through a centralized device ie. Switch or hub.
- Hub is the central node and all other nodes are connected to the central node
- Hub act as a repeater for data flow
- Signals travels through hub to all other computer.
- If hub goes down, entire network goes down.
- But if a computer goes down, the network function normally.
- The Hub receives the data and then transfer it to the destination.



Advantage

- Easy to setup and modify
- Easy to troubleshoot
- Hub can be upgraded easily.
- Only that node is affected that fails, rest of the node work smoothly.
- fast performance with few nodes and low network traffic

Disadvantage

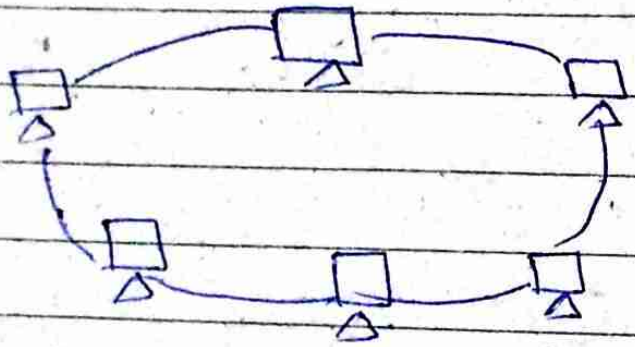
- Cost of installation is high
- Expensive to use
- Performance is based on Hub.
- If the Hub fail, whole network ~~failed~~ stopped because all the nodes depend upon the hub.

3 Ring topology

- In Ring topology all the devices are connected to each other through point to point configuration making a ring.
- No termination is required because it is a ring.
- Each workstation is connected to two other components on either side and they communicates with these two adjacent neighbors.
- Sending and receiving of data take place by the help of TOKEN.

ROUGH

• Token passing :- Token contain a piece of inform
that is send by the source computer.
This token then pass to next node, which che
if the signal is intended (belong) to it. If yes, it
receives it ~~and passes~~ ; otherwise pass token
to next node. This process is continue until
the signal reaches its intended destination.



Advantage

1. Data flow in one direction, reducing the chance of packet collisions.
2. Cheap and easy to install.
3. Data can transfer btw workstation at high speed.
3. Additional workstation can be added without impacting performance of the network.

Disadvantage

1 The entire network will be impacted, if one workstation shutdown or fails.
2 Adding or deleting the computer disturb the network activity.

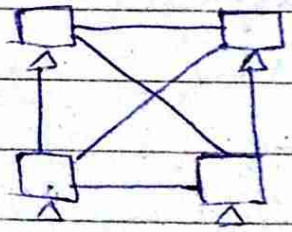
In full Mesh topology
no. of Cables = $\frac{n(n-1)}{2}$
no. of ports = n-1

- Hardware needed to connect each computer to the network is more expensive.
- Difficult to troubleshoot.

4. ~~Mc~~

4. MESH Topology

- In mesh topology, all the devices connected to each other devices
- In mesh topology, each of the devices are interconnected with one-another.
- All nodes cooperate to distribute data among each other.
- Every node not only send data but also receives data from other nodes.
- Each nodes are directly connected to all other nodes.



Advantage

1. Provide security and privacy.
2. Easy to troubleshoot
3. It is robust (strong)
4. failure of one computer, doesnot affect other computer

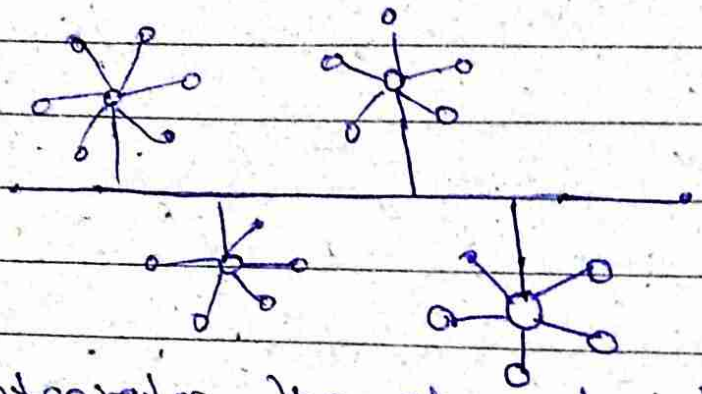
Disadvantage

1. Bulk of wiring is required.
2. Implement cost is higher than other.
3. high chances of redundancy.

ROUGH

5 Tree topology (hierarchical)

- Tree topology is the combination of star network topology and bus topology.
- In this, nodes of bus network, are replaced with star topology



- It integrates the characteristic of both star and bus topology.

Advantage

1. Easy to expand
2. Error detection
3. Easy to maintain
4. If one segment is damaged, other segment is not affected

Disadvantage

1. It relies heavily on ~~bus~~ main bus cable, it break whole network is ~~fail~~ failed.
2. Costly
3. Required many cables

6 Hybrid topology

- It is a mixture of two or more topologies.
- Hybrid topology is always produced when two different basic network topologies are connected.

Advantage

- Reliable and easy to detect the failure System.
- Easy to troubleshoot
- Include both wired or wireless network
- Expandable network

Disadvantage

- Difficult to understand its design.
- Designing cost is high
- lots of Cables are used.

* OSI Model

- OSI stands for Open System Interconnection.
- This model was created by ISO (International Standard Organization) to help standardize communication between computer System.
- OSI model is a model by which several different computer from different manufacturer can communicate easily.

- It divide communication into seven different layer.
- When one computer system communicate with another, whatever whether it is local network or Internet, data travel through these seven layers.
- It provide a description of how network hardware and software work together in a layered fashion to make communication possible

7 different layers

1. Physical layer

- It is the first layer of the OSI model, which is responsible for the transmission of digital data bit (bit stream) from the physical layer of the ~~sender to the physical layer of the~~ sending device to the physical layer of the receiving device.
- The physical layer defines the connector, interface specification, as well as transmission medium requirement.
- Ethernet cables, Token ring network topology technology all function at the physical layer of OSI model.
- Hubs and repeaters are the standard network devices that ~~are~~ function at this layer.
- At this layer, data are transmitted using the type of signalling i.e electric voltage, radio frequencies, or pulses of infrared or ordinary light, supported by the physical medium.

Protocol for physical layer

Bluetooth, ~~wifi~~, Ethernet, DSL, ISDN, 802.11

EEE 802, IEEE 802.2, ISDN

2. Data link layer (flow control)

function

- It provide the capability of error-detection, access control
- Allow devices to access the network to send and receive message.
- It also offer physical address such as Mac. MAC address so a device's data can be sent on the network.
- It convert the bit steam into frames. (fram
- Device like switch work at this layer
- NIC and Bridge are also used.

→ Protocol

ARP, ATM, CDP, FDDI, PPP, STP, Token Ring switches

3. Network layer

- It provide logical address i.e IP address to the packets so that packets of c

→ function

- It creates logical path between two hosts across the world wide web called as virtual circuit
- It convert the data into packets.
- It provide logical address i.e IP address to the packets so that packets has reached to its final destination.

(control the flow of packets).

Routing

- Routers works at this layer
- Routers communicate with one another using routers routing protocol to learn the other network and to calculate the best way (path) to send the info (packets)

→ Protocol

TCP/IP, IPX, RIP, IPv4, IPv6, ICMP, IGMP IPsec.

4. Transport layer

- Transport layer is responsible for the transparent transfer of data between end System.
- It breakdown the data into various segments called Segmentation.
- It is responsible for end-to-end error detection and flow control, connection control.
- Realignment of Segmented data in the correct order on the receiving side.
- Reassembly of data (in another system)

→ Protocol

TCP, UDP, SPX

ROUGH

5 Session layer

function

- Synchronization (kind of refresh or update) of data flow control
- It control dialogue. (half duplex or full duplex)
- ~~It is responsible for establishment~~, no
- It is responsible to establish, manage and terminate a day dialogue throw a network
- Acknowledgment of data receiving during a session.
- Retransmission of data if it is not received by a device.

→ Protocol

SQL, SCP, ZIP, NFS, NetBIOS, PAP, P

6. Presentation layer

- Encryption and decryption of a message for security
- Compression and expansion of a message so that it travel efficiently.
- Content translation.
- Graphic formatting

→ Protocol

JPEG, TIFF, GIF, ASCII, EBCDIC

MPEG

7 Application layer

- Application layer supports applications, apps, and end-user processes.
- It is responsible for application services for file transfer, email and other network software services.

⇒ Protocol

FTP, HTTP, DNS, NTP, Telnet

ROUGH

* Network Devices

1. Hub (work in half-duplex mode)

- Hub is the most basic network devices that connect multiple computer or other network devices together.
- Hub is used to transfer the data ~~in the form of~~.
- The data is transformed in the form of packet on a computer network.
- When a hub receives a packets of data from a connected device, it copies the data packets and broadcast that data packets to all other connected devices without knowing to whom that packet is to be belong.
- Hub is not secure and safe.
- Moreover, copying the data packets on all the interface or port make it slower.
- They transmit the packet regardless of the fact that ~~the~~ if data (packet) is destinated for the device or not.
- There are 2 type of Hub

a) Active Hub.

- Active Hub amplify or regenerate the information signal.
- This is also known as multiport Repeater

- It can upgrade the properties if incoming signal before sending to them to destination.

⑥ Passive Hub

- It works like a Simple Bridge.
- It is used for just creating a connection between Various device.
- It does not have the ability to amplify or regenerate any incoming signal.
- It receives signal and then forward it to multiple devices.

8. Switch (works in full-duplex)

- Switch is the network device that connect multiple, computer or other network together.
- Switches are connected to the devices through twisted pair Cabling.
- When Switch receives a packet, it transfer it to only on that computer to the intended receiver. (i.e Unicast)
- It doesnot broadcast the packet to all computer. i.e (prevent loop Generation)
- So the bandwidth is not shared and make the network much efficient.
- Switches operates in full-duplex mode where devices can send and receive data from

the switch at simultaneously.
- Speed of transfering data is high as does not broadcast the data.
- Switches are used in LAN connectivity device

3 Router (Connect ~~that have same protocol~~)
- Router is a network device that are used to connect two or more networks
- Routers are located at gateways, the place where two or more networks connect.
- Router uses networks header and forwarding table to determine the best path for forwarding the packets.
- when a router receives the data, it determines the destination address by reading the header of the packets.
- Once the address is determine, it searches in its routing table to know how to reach to the destination and then forward the packets to the best and easy path.
- Router works also works on different -different Protocol.
- Router is also used in different Subnet connectivity.
- Router works on the 3rd layer of OSI ie network

4. Bridges (Data Link layer device of OSI)

- Bridges is used to communicate two different network that uses the same protocol.
- Bridge works at the data link layer of OSI model.
- Sometimes it is necessary to divide network into subnets to reduce the amount of traffic. ~~On each large~~ Once divided, the bridge is used to connect the two subnets and manage the traffic flow between them.
- (But it is now replaced by Switch)
- The function of Bridge is to blocking or forwarding data, based on the destination MAC address written in each frame of data.
- If the destination address is on other side from which the data ~~is~~ ~~was sending~~ was sended, it can forward the data to other network to which it is connected.
- If the address is not on the other side of the bridge, the data is blocked from passing.
- It has single input and single output port thus making it 2 port devices.

ROUGH

⑤ Repeater

- Repeater is a device which is used to regenerate and retransmit the data as it is in its original state.
- When data is transfer in layer area the signal become weak rese and also the speed of transfering data is reduced. To overcome this we use repeater. that amplify the weak signal to regain its original quality.
- Repeater it classified as layer 1 devices in the OSI model because they act only on the bit level.
- Purpose

To generate and strengthen the signal at the bit level to allow them to travel a longer distan on the media.

6 Modem

- Modem means modulator or demodulator
- Modem is a device that enables the a compu to transmit data over telephone line or cables lines.
- Computer information is stored digitally, whereas information transmitted over telephone line is transmitted in the analogue wave fo

with the help of modem
- Modem provide relatively slow method of communi-cation.

(7) Gateway

- Any device that translate one data format into another data format is called gateway
- ~~Example~~ Key point about gateway is that only the data ~~is transm~~ format is translated, not the data itself.
- for example- many company uses an email system such as Microsoft exchange or novel Grop wise. These system transmit mail internally in a certain format. when mail needs to be sent across Internet to users using different email system, the email must be computing converting to another format. usually to SMTP (Simple mail transfer protocol).

(8) NIC

- NIC stands for Network interface card. It is also known as LAN card, ethernet card, ethernet connector, network adaptor, networ interface controller.
- NIC is a computer hardware component that allow a computer to connect ~~with~~

ROUGH

to a network.

- NIC may use both wired or wireless connection
  - → In wired → a computer is connected to network through cables that uses RJ-45 connectors.
  - → In wireless → Computer are connected to network through Infrared radiation.
- It is specially designed for LAN transmission technology.
- The old 'Combo' NIC accept both BNC (co-axial) and RJ-45 (UTP) connector.
- NIC support transfer rate of 10, 100 or 1000 Megabit per second.

⑨ ADSL

- ADSL stands for Asymmetric digital Subscriber line
- ADSL is a type of DSL, which is a method of transferring data over copper telephone lines.
- ADSL has different maximum data transfer rate for uploading and downloading data. while SDSL (Symmetrical DSL) upload and download data at same speed

* Network Terms

① DNS (Domain Name System)

- The Domain Name System (DNS) is a hierarchical and decentralized naming system for computer, services or other resources connected to the Internet or a private network.
- It associates various information with domain names assigned to each of the participating entities.
- It translates more readily memorized domain names to the numerical ~~memorized~~ IP addresses needed for located and identifying computer services and devices with the underlying network protocol
- The Domain Name System also specifies the technical functionality of the database service that is at its core.

② URL (uniform resource locator)

- A URL is the address of a resource on the internet.
- A URL indicate the location of the resource as well as the protocol used to access it.
- It is a type of URI (uniform resource identifier)
- URL is an address that send user to a specific resource.

Components of URL

1. Protocol

- The protocol declares how our web ~~server~~ browser communicates with a web server when sending and fetching a web page or document

⟹

(3) Protocols

- A protocol is a set of rules and guidelines for communicating data.
- Rules are defined for each step and process during communication between two or more computer.
- Protocol specify the standard for communication and provide detailed information on process involved in data transmission.

1. Hypertext Transfer Protocol (HTTP)

- Hypertext ~~Transport~~ Transfer protocol (HTTP) is an application-layer protocol used primarily on the world wide web.
- HTTP defines how message are formated and transmitted.
- HTTP uses a client-server model where the web server browser is a client and

communicates with the webserver that hosts the website.

- The browser uses http, which is named over TCP/IP to communicate to the server and retrieve web content for the host.
- HTTP is widely used protocol and has been rapidly adopted over the internet because of its simplicity.

2. ~~Hypertext transfer protocol~~ Secure (HTTPS)

- HTTPS is the same things as HTTP, but uses a secure socket layer (SSL) or transport layer Security (TLS) for security purpose.
- Therefore, secure website uses the HTTPS protocol to encrypt the data being send back and forth with SSL encryption.
- Example of sites ~~are~~ that uses https are banking and investment website, e-commerce websites etc
- By viewing the URL in the address field of our web browser, we can know that this website is secure.
- Most browser also display lock icon somewhere along the edge of the window to indicate the website we visited is secure.

- HTTPS enables encrypted communication and secure connection between a remote user and the primary web server.

3 FTP (file transfer Protocol)

- FTP is a client-server protocol used for transfering files to or exchange file with the host computer.
- FTP uses Internet's TCP/IP protocol to enable the data transfer.
- It may be authenticated with user name or password.
- But Any Anonymous FTP allows user to access file, program and other data from the internet without the need of userId or password.
- publicly available files are often found in a directory called pub.

4. SMTP (Simple Mail transfer Protocol)

- SMTP is a protocol used for sending e-mails over the network.
- SMTP is a set of commands that authenticate and direct the transfer of electronic mail.
- Most e-mail system that sending mail over the internet use SMTP to send message from one

server to another, the email client uses either pop(postoffice protocol) or IMAP(Internet message access protocol) to ~~retrieve~~ retrieve the mail.

- SMTP is generally used to send message from mail client to a mail server. This is why we need to specify both the POP or IMAP server and SMTP server when we configure our e-mail application.
- It works on port 25 and uses TCP/IP protocol for sending and receiving protocol

5 TCP/IP (Connection Oriented Protocol)

- TCP/IP means Transmission control protocol and internet protocol.
- TCP/IP is the backbone of all communication
- TCP/IP defines how to establish communication so that the programmer exchange the data
- These protocol describe the movement of data packets of between the source and destination
- If the packets of data is lost ~~tcp~~ ask the source to resend it.

Example:-

If a server wants to send the html file to client, it will send it via http protocol. So the http layer ask the tcp layer

to setup the connection. The TCP break the file into packets and no. them and ask the IP protocol to get the destination address. The TCP then deliver the packets which ultimately combines up at the target (destination point) to retrieve a original html file.

- It guarented the receiver receives the packets

(6) UDP (User datagram protocol) (Connectionless pr

- It is similar to TCP but it is used if small data is involved.
- If the UDP protocol is used, the packets of data are called datagram.
- It is not that efficient in data connection as the TCP does.
- It is also used along with IP protocol as UDP/IP.
- Commonly used in video game, video conferen where the loss of data is tolerable
- If the packets of data is lost, UDP does not ask for those packets again from HTTP.
- It is used which faster speed is required and error correction is not necessary.
- working

when an app uses UDP packets are just send to the receiver. The sender doesn't wait to make sure the receiver receives the message - it just continue to send the next package. If the receiver misses few UDP packets Sender will not ask send them back.

* Component of URL

2. Subdomain
   - Subdomain is the division of the main domain name.

3. Domain name
   - It is a unique reference that identifies a web site on the internet.
   - Domain name always include TLD (top level domain) Ex - doepud.co.uk , uk is TLD. and .co.uk is second level domain (SLD).

4. Port
   - The port no. is rarely visible in URL, but always required.
   - when declared it comes after the TLD (top level domain), separated by a colon.
   - for http. port → 80 and for https (secure) → port = 443

5. Path
   - The path refers to the file or directory on the web server
   - Sometimes the file name is not specified. eg. https://doepud.co.uk/blog/ so the web server automatically look inside the /blog/ for a file called index or default.

6. Query

- A query is commonly found in a URL of dynamic pages. and is represented by question mark followed by one or more parameters.
- The query ~~followed by~~ directly follows the domain name, path or port number.

- http://www.google.co.uk/search?q=url&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-GB:officials&client=firefox-a.

Query pair

?q=.....utf-

8&aq ——— mozilla:en

GB:—— firfox a

7 Parameter

- Parameter are the information found in the query string of the URL.
- Parameter follows the question mark and are separated by an ampersand(&) character.

- q=url
- ie=utf-8
- oe=utf-8
- aq=t etc.

⑧ Fragment

- It is an internal page reference, sometimes called a anchor.
- It usually appear at the end of the URL and begins with hash (#) character followed by an identifier.
- It refers to the section within the page

---

* MAC Address

→ MAC stands for Media Access Control address.
→ MAC is our machine address.
→ This address will never change
- It is also known as hardware address.
- MAC address operates at the data link layer of the OSI model.
- It is of 12 digit hexadecimal number (48 bit no). It is made up of number 0-9 and or a letter A-f. separated by colon
  ex - 00:0d:83:b1:c0:8e
- It is a unique machine address given to our device.
- Our device communicate with the local area network using this network Address

ROUGH

* Data communication

- communication
- Data communication means data or inform
- is transmitted from one location to anoth
- through transmission media.
- Data communication is the process of computing and communication technologies
- to transfer data from one place to another
- It enables the movement of digital data between two or more nodes, regardless of geographical areas, technologies medium or data contents

- → Key elements or components of Data communication.

1. Message
- The message is the information or data that is communicated.
- It may consist of text, numbers, images, audio, videos. etc
- Text is converted to binary and image is converted to pixels. etc.

2. Sender

- The computer or any other device that sends the data or message is called sender.
- A sender may be computer, workstation, telephone, video camera etc.

3. Receiver

- The device that receives the data is called receiver.
- Receiver is also known as sink.
- Receiver can be a computer, workstation, printer or fax machine.

4. Medium (communication channel)

- The physical path through which a data or message travels from sender to receiver
- If the receiver and sender are within a same building - a wire may be the medium
- If they are located at different location, the media may be the telephones line, fibre optics, satellite or microwave

5. Encoder | Decoder

Encoder

- computer works with digital signal and the communication channel (medium) use analog signals
- Therefore, to send data through a comm. channel (medium), the digital signals are encoded (converted) into analog signal. This is called encoding.
- The device that convert digital signals into analog signal is called encoder.

Decoder

- computer works ~~or~~ with digital signals and the ~~transmit~~ comm. channel (medium) usually use analog signal.
- Therefore, a receive data from a comm. channel ~~are~~ coded analog signal are converted back to digital signal. This is called decoding.
- The device that convert analog to digital signal is called decoder.

Data communication modes

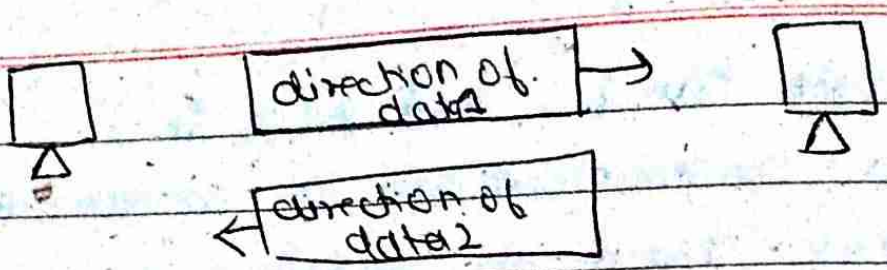
There are 3 types of modes

1. Simplex mode

- In this mode, data can be send only in one direction. i.e communication is unidirectional.
- A device either send or receive a data
- device that behave as sender, we can not send a back message back to the sender.
- Unidirectional comm. is done in Simplex Systems
- Example :- loudspeaker, television broadcasting, television and remote, keyboard and monitor etc.

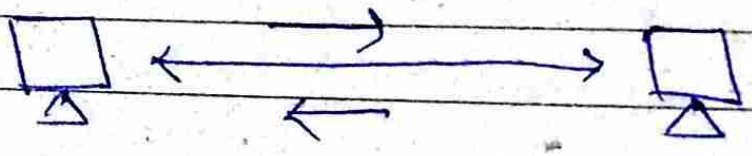
2 Half duplex

- In half duplex mode data can be transmit in both direction but only in one direction at a time. Means both the connecting
- device can transmit data and receive but not simultaneously.
- A device that send data cannot receive data at that time.
- It receives data after the data is sending to the receiver.
- Hub works as an half-duplex mode



3. Full duplex mode

- In full duplex mode, data can be sent in both directional simultaneously.
- A device can send or receive data simultaneously.
- Switch works on full duplex mode.



* Key elements of Protocol.

1. Syntax

- Syntax refers to the structure or format of the data, meaning the order in which they are presented.
- for ex:- a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bit to be the receiver's address and rest of the stream to be the message itself.

2 Semantics

- Semantics refers to the meaning of each section of bits.
- How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation?
- for ex - does an address identify the route to or final destination of the message?

3. Timing

- Timing refers two characteristic
  - → first when data should be send.
  - → second - how fast they can be sent.
- for ex - if a sender produce data of at 100Mbps but the receiver can process data at 1Mbps, the transmission will overload the receiver and some data will be lost.

* Difference btw TCP and UDP

TCP	UDP
1. TCP stands for Transmission control protocol	1. UDP stands for User Datagram Protocol
2. It is connection oriented protocol.	2. It is connection less protocol.
3. TCP is more reliable	3. It is less reliable
4. TCP is slower for data sending	4. UDP is faster for data sending
5. It controls the flow of data	5. It does not have an option for flow control
6. TCP makes error checking and also report them	6. UDP makes error checking but not reporting
7. Header size of TCP is 20 byte.	7. Header Size of UDP is 8 byte.
8. TCP is used in application in which fast transmission of data is not required.	8. UDP is used in application in which app. have the priority of sending the data on time and on faster rates
9. TCP is heavy weight	UDP is light weight

as it needs three packets to set up a connection.	due to no ordering of message.
10. It rearrange data packets in the order specified	10. No order ;

* Remote logging

- Remote logging is Unix-like computer operating system command that allows user to login to another UNIX machi comp. (host) on a network and to interact as if the user were physically present at the host computer
- Once logged in to the host, the user can do anything that the host has given permission for - such as read, edit, delete files etc.
- It uses TCP port 513.
- Remote login considered ~~no~~ useful for simple logins that don't require a lot of control over the client/host interaction.
- Benefits of Remote login is the ability to use a file called .rhosts that resides on the host machine and maintains a list of terminals allows to login without a password.

ROUGH

* function of Transport layer

- Transport layer is the fourth layer of OSI model.
- It respond to service request from session layer and issues service request to Network layer.
- Transport layer is responsible for delivering messages between hosts.
- In transport layer, data travels in the form of segments.
- Transport layer is responsible for creating an end to end connection between source IP and the destination IP
- Transport layer is using two major protocols TCP and UDP.
- TCP is connection oriented protocol where UDP is connection less protocol.
- So by using TCP we can create an end to end reliable connection btw source and destination hosts.
- Transport layer is called host-to-host transport layer in TCP/IP model.

Responsibilities / Duties of Transport layer

1. Creating end-to-end connection between hosts

in different network.

2. Error control

3. flow control

4. Ensure complete data transfer in TCP

5. Congestion Avoidance.

6. Connection Control

* Internet Protocol

- Internet protocol is the set of rules for exchanging messages between computers across a single network or a series of interconnected networks, using the Internet Protocol Suite (often referred to TCP/IP).
- Messages are exchange as datagram, also known as data packets or packets.
- IP allows devices (running on diff. platform) to communicate with each other as long as they are connected to the Internet.
- The main purpose and task of IP is the delivery of datagram from the source host to the destination host based on their address.
- To achieve this, IP includes methods and structures for putting tags (address info., which is part of metadata) within data gram. This process of putting these tags on datagrams is called encapsulation

ICMP (Internet Control Message protocol)

- ICMP is a TCP/IP network layer protocol that provides troubleshooting, control and error message services.
- It provide error message to the source IP address when network problems prevents delivery of IP packets.
- Any IP network device has the capability to send, receive or process ICMP messages.
- An ICMP message is encapsulated directly within a single IP datagram and reports errors in the processing of datagrams.
- An ICMP header begins ~~with~~ after the IPv4 header.
- An ICMP packet has an eight byte header, followed by a variable-sized data section.
- The first 4 bytes of the header are fixed.
  - (a) ICMP type
  - (b) ICMP code
  - (c) checksum of the entire ICMP message
  - (d) "
- The remaining four bytes of the header vary, based on the ICMP type and code.

- ICMP for Internet protocol version 4 is called ICMPv4 and for Internet protocol version 6 is called ICMPv6.

* ARP

- ARP stands for "Address Resolution Protocol".
- ARP is a protocol used for mapping an IP address to a computer connecting to a local network LAN.
- Since each computer has a unique physical address called a MAC address, the ARP converts the IP to the MAC address.
- This ensures each computer has a unique network identification.
- It is used when info sent to the network arrives at the gateway, which serves as the entrance point to the network.
- The gateway uses the ARP to locate the MAC address of the comp. based on the IP address the data is being sent to.
- ~~The ARP~~
The ARP look up this info. in a table called the "ARP cache".
- If the address is found, the information relayed to the gateway, which will send the data to appropriate machine.

ROUGH