(Node → Any communicating device in a network is called a node)
(link → it includes the type of connectivity (wired or wireless between the nodes)

classfellow
DATE : / 20
PAGE No

Network -

A network is a collection of devices connected to each other to allow the sharing of data.

→ for e.g - Internet (it connects the millions of people across the world)

→ for e.g (Real world) - Dominos has a network of 1232 branches across india.

Importance of Computer Network -

The internet is a network connecting all different network-enabled devices which enable data and information sharing between them and that makes computer networks a core part of our life.

→ for e.g - this online interview is also a part of computer network

Classification of Networks -

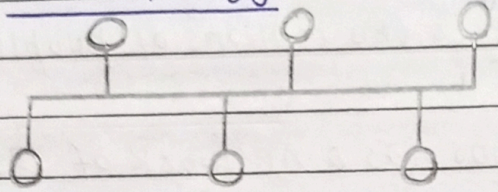
Distance ↓	Region ↓	
1m	square meter	→ Personal area network (bluetooth)
10m	Room	→ Local area network (wifi)
100m	Building	
1 Km	campus	
10 Km	city	→ Metropolitan area network (TV cable)
100 Km	country	→ wide area network (Internet)
1000 Km	Continent	
10000 Km	Planet	→ The internet (Global area network)

Network topology -

Network topology specifies the layout of a computer network. it shows how devices and cables are connected to each other.

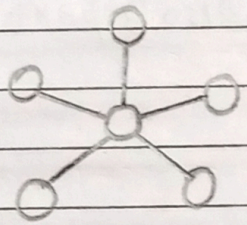
Types of topologies -

(a) Bus topology -



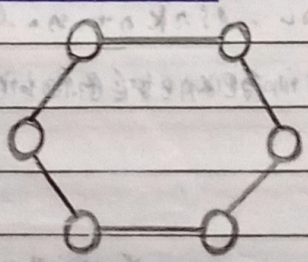
→ In bus topology, all the nodes are connected to a single cable known as a central cable or bus.
→ It is useful to connect a smaller no. of devices.
→ if the main cable gets damaged, it will damage the whole network.

(b) star topology -



→ In star topology, all the nodes are connected to a single device known as a central device.
→ star topology is commonly used in office and home networks.
→ if the central device is damaged, then the whole network fails.

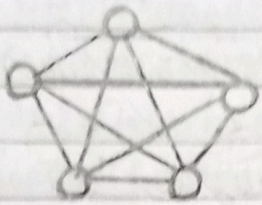
(c) Ring topology -



→ In ring topology, each node is connected to exactly two nodes forming a ring structure.
→ it is used very rarely as it is expensive and hard to install and manage.

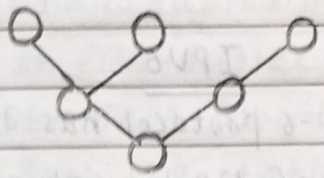
→ if one of the nodes are damaged, it will damage the whole network.

ⓓ Mesh topology -



→ In mesh topology, all the nodes are individually connected to other nodes.
→ Mesh topology is rarely used as installation and configuration are difficult.
→ it is a robust as a failure in one cable will only disconnect the specified Computer connected to this Cable.

ⓔ Tree topology -



→ A tree topology is a Combination of star and bus topology as all the smaller star networks are connected to a single bus.
→ if the main bus fails, the whole network is damaged.

∴ Mesh topology is best because if any link or node fails, then there will be another path that will allow network traffic to continue.

★ Factors affecting security of network → [unauthorized Access, Viruses]

★ Factors affecting reliability of network → [Frequency of failure, Recovery time of a network after a failure]

elements ← Protocols → set of rules governing exchange of information in an easy and secure way)
- syntax
- semantics
- Timing

DATE: / 20
PAGE No

★ factors affecting performance of network - large no. of users
- Transmission medium types
- Hardware
- software

★ Factors make network effective -
(a) Performance (transmit time and response time)
(b) Reliability (frequency of failure)
(c) Robustness (condition of being strong and in good condition)
(d) security (Protection of data from unauthorized access and viruses).

(Internet Protocol version)

IPV4 address -
→ An IP address is a 32-bit dynamic address of a node in the network.
→ An IPV4 address has 4 octets of 8-bit each with each number with a value up to 255.
→ There are five types of IPV4 classes which are classified as class A, B, C, D and E. (According to network coverage)

IPV4	IPV6
(a) IPV-4 protocol has address length of 32-bit represent in decimal format and it support manual configuration.	(a) IPV-6 protocol has address length of 128-bit represent in hexadecimal format and it support Auto configuration.
(b) It is less secure.	(b) It is more secure.
(c) Authentication facility not provided.	(c) Authentication facility is provided.
(d) Packet flow identification (PFI) is not available.	(d) Packet flow identification (PFI) is available.
(e) It has broadcast message transmission scheme.	(e) It has multicast message transmission scheme.

Transmission modes -

The way in which data is transmitted from one device to another device is known as transmission mode.
The transmission modes are divided into three categories -

ⓐ **simplex mode -**

→ In simplex mode, the communication is unidirectional i.e, the data flow in one direction.
→ A device can only send the data but cannot receive it or it can receive the data but cannot send the data.
(for e.g - keyboard and monitors. the keyboard can only give input and the monitor can only give the output)

ⓑ **Half-duplex mode -**

→ In half-duplex mode, direction can be reversed i.e, the station can transmit and receive the data as well.
→ Message flow in both the directions but not at the same time.
(for e.g - walkie-talkie. In which message is sent one at a time and messages are sent in both directions)

ⓒ **Full-duplex mode -**

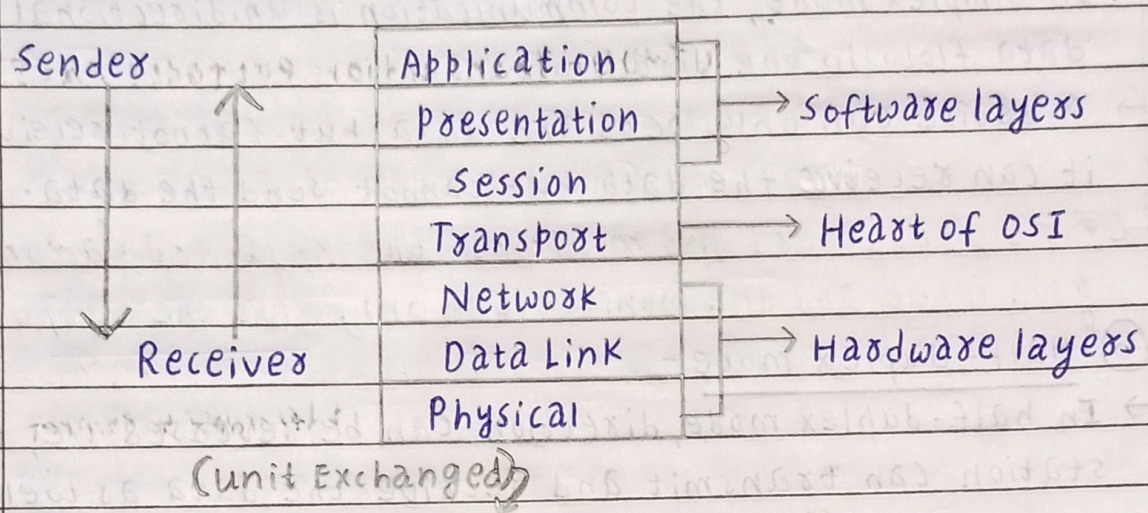
→ In full-duplex mode, the communication is bi-directional i.e, the data flow in both the directions.
→ Both the stations can send and receive the message simultaneously.
(for e.g - Telephone network. In which two persons can talk and listen at the same time)

OSI reference model -

(Open system Interconnections) model deals with connecting the systems that are open for communication with other systems.
The OSI model has seven layers. The principles used to arrive at the seven layers can be summerized below -
→ create a new layer if a different abstraction is needed.

→ Each layer should have a well-defined function.
→ The function of each layer is chosen based on internationally standardized protocols.

Seven layers -



1. Physical layer - (Bit)

→ it is concerned with transmitting raw bits over a communication channel.
→ The physical layer is mainly used for the physical connection between the devices.
→ It also chooses which type of transmission mode is to be selected for the transmission.

2. Data-link layer - (Frame)

→ it is used for transferring the data from one node to another node.
→ it receives the data from the network layer and converts the data into data frames and then attaches the physical address to these frames which are sent to the physical layer.
→ it enables the error-free transfer of data from one node to another node.

3. Network layer - (Packet)

→ Network layer converts the logical address into the physical address.

→ The routing concept means it determines the best route for the packet to travel from source to the destination.

4. Transport layer - (TPDU - Transaction Protocol data unit)

→ The basic functionality of this layer is to accept data from the above layers, split it up into smaller units if needed, pass these to the network layer and ensure that all the pieces arrive correctly at the other end.

→ The transport layer takes care of segmentation and Reassembly.
↳ (divides a computer network into smaller parts)

5. Session layer - (SPDU - Session Protocol data unit)

→ The main responsibility of the session layer is beginning, maintaining and ending the communication between the devices.

→ session layer also reports the error coming from the upper layers.

→ It establishes and maintains the session between the two users.

6. Presentation layer - (PPDU - Presentation Protocol data unit)

→ The presentation layer is also known as a translation layer as it translates the data from one format to another format.

→ At the sender side, this layer translates the data format used by the application layer to the common format and at the receiver side, this layer translates the common format into a format used by the application layer.

7. Application layer - (APDU - Application Protocol data unit)

→ It contains a variety of protocols that are commonly needed by users. (TELNET, EMAIL, FTP, WWW, HTTP, Bluetooth etc.)
↳ (File transfer Protocol, simple mail transfer Protocol etc.)

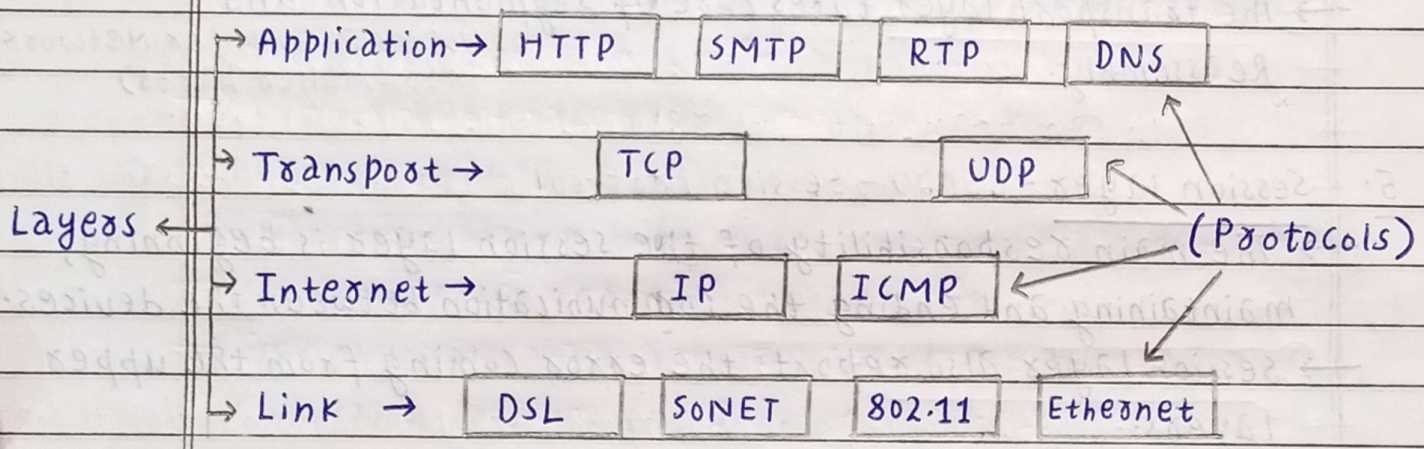
→ Application layer enables the user to access the network.

TCP/IP Reference Model -

→ It is a compressed version of the OSI model with only 4 layers.

→ The name of this model is based on two standard protocols used i.e, TCP (Transmission Control protocol) and IP (Internet protocol).

Four layers -



1. **Link layer -**
Decides which links such as serial lines or classic Ethernet must be used to meet the needs of the Connectionless internet layer.

2. **Internet layer -**
it delivers the IP packets where they are supposed to be delivered.

3. **Transport layer -**
its functionality is almost the same as the OSI transport layer. it enables peer entities on the network to carry on a conversation.

4. Application layer -
it contains all the higher-level protocols.

Difference between OSI and TCP/IP Reference models -

OSI Reference Model	TCP/IP Reference Model
(a) 7 layered architecture.	(a) 4 layered architecture.
(b) OSI Reference Model is less reliable.	(b) TCP/IP Reference Model is more reliable.
(c) OSI Model uses vertical approach.	(c) TCP/IP Model uses horizontal approach.
(d) It is acting as an interaction gateway between the network and the final user.	(d) It is a connection protocol that assigns the network of hosts over the internet.
(e) Transport layer is connection oriented.	(e) Transport layer is both connection oriented and connection less.

HTTP (HyperText Transfer protocol) -
→ It defines the set of rules and standards on how the information can be transmitted on the world wide web (www).
→ It helps the web browsers and web servers for communication.
→ it uses port 80 by default.

HTTPS (Hyper Text Transfer protocol secure or secure HTTP) -
→ It is an advanced and secured version of HTTP.
→ It enables secure transactions by encrypting the communication and also helps identify network servers securely.
→ it uses port 443 by default.

IP address → unique address that identifies a web page on the internet. (numerical label - e.g → 123.141.121.411)
(IP → Internet Protocol)

classfollow
DATE : / 20
PAGE No

DNS (Domain name system) -

→ It is a naming system for all the resources over the internet which includes physical nodes and applications.
→ It translates the domain names to their corresponding IPs. (e.g - interviewbit.com to 172.217.166.36)
→ without DNS, user musk know the IP address of the web page that he wanted to access.
(Domain name → IP address → web page)

TCP (Transmission Control Protocol) -

It is a set of rules that decides how a computer connects to the internet and how to transmit the data over the network.
→ Connection-oriented protocol
→ More Reliable
→ Slower transmission
→ offers error checking mechanism
→ Protocols like HTTP, FTP, TELNET, SMTP etc. use TCP at the transport layer.

UDP (user Datagram Protocol) -

It is also a set of rules that decides how a computer connects to the internet and how to transmit the data over the network.
→ Connectionless protocol
→ less Reliable
→ Faster transmission
→ No error checking mechanism
→ Protocols like DNS, RIP, SNMP etc. use UDP at the transport layer.

Some Protocols -

ICMP (Internet Control Message protocol) -

→ It is a network layer protocol used for error handling.
→ It is mainly used by network devices like routers for diagnosing the network connection issues and crucial for error reporting and testing.

DHCP (Dynamic Host Configuration Protocol) -

DHCP servers auto-assign the IPs and other network configurations to the devices individually which enable them to communicate over the IP network.

ARP (Address Resolution Protocol) -

It is a network level protocol used to convert the logical address i.e, IP address to the device's physical address i.e, MAC address. (MAC → Media Access Control)
(RARP → Reverse of Address Resolution Protocol)

FTP (File Transfer protocol) -

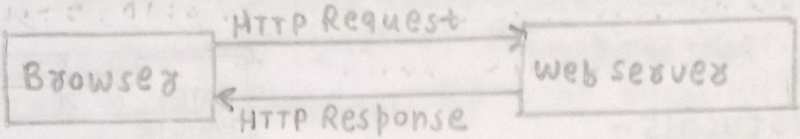
It is an application layer protocol used to transfer files and data reliably and efficiently between hosts.

Flow Control -

→ Flow control is meant only for the transmission of data from sender to Receiver.
→ It prevents the loss of data and avoid over running of receive buffers. (buffers → delay in process)

Error Control -

→ Error Control is meant for the transmission of error free data from sender to receiver.
→ it is used to detect and correct the error occured in the Code.



classfollow
DATE : / 20
PAGE No

Some Important definitions -

1. What happens when you enter google.com in the web browser?

→ (a) check the browser cache first if the content is fresh and present in cache display the same.

(b) if not, the browser checks if the IP of the URL is present in the cache, if not then request the OS to do a DNS lookup using UDP to get the corresponding IP address of the URL from the DNS server to establish a new TCP connection.

(c) A new TCP connection is set between the browser and the server.

(d) An HTTP request is sent to the server using the TCP connection.

(e) The web server handle the incoming HTTP request and send the HTTP response.

(f) The browser process the HTTP response sent by the server and may close the TCP connection or reuse the same for future requests.

(g) if the response data is cacheable then, browsers cache the same.

(h) Browser decodes the response and renders the content.

2. Bandwidth -

The maximum amount of data transmitted over an internet connection in a given amount of time. (Mbps)

3. Hub - (Network Connecting device)

→ A hub is a physical layer networking device which is used to connect multiple devices in a network.

→ Generally used to connect computers in a LAN.
(100 Mbps, less efficient as collisions present)

(Packets → Data sent over a network is divided into smaller segments called packets)

(firewall → security system from unauthorized servers)

classfollow
DATE : / 20
PAGE No

Switch - (Network connecting device) → used in multicasting

A switch is a data link layer networking device which is used for connection establishment and connection termination on the basis of need.
(1 GBPS, more efficient as the collisions can be avoided)

4. Router -

A router transfers information and data like web pages, emails, images, videos etc from source to destination in the form of packets.

Gateway -

Gateway acts as the entry-exit point for a network since all traffic that flows across the networks should pass through it.

★ Difference → A router sends the data between two similar networks while gateway sends the data between two dissimilar networks.

5. Bridge -

A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN.

6. Subnetting in IP -

When a bigger network is divided into smaller networks, in order to maintain security, then that is known as subnetting. so, maintenance is easier for smaller networks.

7. Unicasting -

if the message is sent to a single node from the source then, it is known as unicasting.
(e.g- when we click a hyperlink in a web browser, we are requesting HTTP data from the host)

UTP cable → unshielded twisted pair (used in LANs)
STP cable → shielded twisted pair (Also used in LANs)
↳ expensive

Anycasting-

if the message is sent to any of the nodes from the source then, it is known as anycasting.
(e.g - DNS (Domain name system))

Multicasting-

if the message is sent to a subset of nodes from the source then, it is known as Multicasting.
(e.g - watsapp group)

Broadcasting-

if the message is sent to all the nodes in a network from the source then, it is known as broadcasting.
(e.g - Radio and T.V)

8. **Cryptography-**

→ Cryptography is used to secure and protect data during communication. it is helpful to prevent unauthorized person from accessing any confidential data.

→ Encryption and decryption are the two essential functionalities of cryptography.

(Encryption - transforms the original information into an unrecognizable form)

(Decryption - Process of converting encrypted data in a form this is understood by a human or a computer)

9. **Switching techniques-**

→ The switching technique will decide the best route for data transmission.

→ Information may be switched as it travels through various communication channels.

(circuit switching, Packet switching, message switching)

(frame → data unit)

classfellow
DATE : / 20
PAGE No

10. **Stop-wait protocol-**

In stop and wait protocol, a sender after sending a frame waits for an acknowledgement of the frame and sends the next frame only when acknowledgement of the frame has received.