COMPUTER NETWORKS

Computer Network:

→ A computer Network is a set of devices connected through links. In simple terms computers connected together

■ Network: A network is a set of devices that are connected with a physical media link. In a network, two or more nodes are connected by a physical link or two or more networks are connected by one or more nodes. A node can be any devices which is capable of sending or receiving the data. The links connecting the nodes are known as communication channels.
In simple term, network is a collection of devices connected to each other to allows sharing of data.

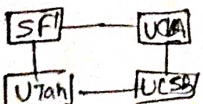
Brief History:

- In 1969, ARPANET (Advanced Research Project Agency Network) becomes the first connected computer Network.
  - It implemented the TCP/IP protocal, which later become the Internet.
- ARPANET was developed by Advanced Research Project Agency (ARPA), a subset of US Department of defence (DoD).

? Why did the DoD need to develop network computers?

→ Because of the cold war betⁿ US & USSR (Union Sovict Socialist Republics). The goal of ARPANET was to keep lines of communication open if the USA and the USSR decied to Exchang nuclear devices.

- ARPANET revolutionized communications by using packet-switching instead of direct connection. Data that is communicated through a packet-switching system is formated into packets with an address of destination machine. and sent onto the network and pick up by the next machine. The address in protocal tells the machine where to send the packets. This way the info. will reach its intended destination, even if there isn't a direct connection betⁿ two machines.
- While it changed the need for these to be direct connections between machines to communicate, the ARPANET relies on phone lines. It was originally a four-node network between university computers of Stanford, the University of Utah, UCLA (University of California LA) and UCSB (University of California, Santa Barbara).

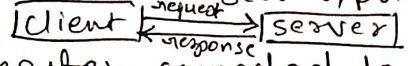


~~# Bits~~

Basic Terms in Computer Network :-

1. **Client** :- A client is a computer Hardware device or software that acessess a service made available by a server. The server is often (but not always) located on a separate physical comp.

2. **Server** :- A server is a physical computer dedicated to run services to serve the needs of other computers. Depending on the services that is running, it could be a file server, database server, home media server, print server, web server.



3. **Host** :- A host is a computer, connected to other computers for which it provides data or services over the network. In theory, every computer connected to a network act as a host to other peers on the network

4. **Peer** :- A Peer is a node that provides the same functionality as another. Eg two computers in network are peers, but a computer and a server are not peers as they perform different operations.
A peer is something or someone that is an equal member of group, where there's some kind of relationship beth the members of the group.

5. **Bandwidth** : Network bandwith is a measurement indicating the maximum capacity of a wired or wireless communication link to transmit data over a network connection in a given amount of time. Typically, bandwidth is represented in the numbers of bits, kilobits, megabits or gigabits. that can be transmitted in 1 second. ~~Synchro~~ Synonymous with capacity bandwidth describes data transfer rate.

- **Speed** : Speed refers to rate at which data can be transmitted while the bandwith is the capacity for that speed.

1 gbps = 10^9 bits/s

1 mbps = 1000000 bits/s

1 kbps = 1000 bits/s

16 **Jitter**:- Information is transported from your data packets across the internet. They are usually set at regular intervals and take a set amount of time. Jitter is when there is a time delay in the sending of these data packets over your network connection. This is often caused by network congestion, and some times route changes.
The longer data pkts take to arrive, the more jitter can negatively impact the video and audio quality.

17 **Packets**:- A packet is a small segment of a larger message. Data sent over computer network such as internet, is divided into packets. These packets are then recombined by the computers or device that recieves them.

- **Packet Header** :- A packet Header is a "label" of sort, which provides information about the packets contents, origin, destination.

Packets consist of two portions: the Header & the payload.
The Header contains info about the packet, such as origin, destination IP address etc. while the payload is actual data.

18 **Segments** :- If the Tranport protocal is TCP, the unit of data sent from TCP to network layer is called segments.

19 **Frame** :- A frame is also a unit of data, it is a protocal Data Unit of a Data link layer.

NOTE
- The PDU of Transport layer is called as Segments
- The PDU of Network layer is called as Packets
- The PDU of Data Link layer is called as Frames.

10 **Local Host** :- local host is your own computer. Local host can be seen as server that is used on your own computer. Local Hast has the IP Add : 127.0.0.1.

11 **Bit-Rate**: **Line coding**:- The procers of turning binary data into a time-based signal is known as line coding.
Bit Rate :- Network connections can send bits very fast. We measure that speed using Bit-rate. The number of bits of data that are sent each second.

12 **Latency** :- Latency measures how late the bits arrive.
Latency is the time between the sending of data msg and recieving of that msg, measured in milliseconds.

13 NOISE :- Noise is any undesired signal in communication circuit. Noise is a unwanted disturbance superimposed or a useful signal, which tends to obscure its information content.

Types :- Thermal, Intermodulation, Crosstalk and impulse noise.

14 Attenuation :- Attenuation means lass of signal strength in networking cables or connections. This is measured in decibels(dB) or voltage. and can occur due to varity of factors, It may cause signals to become distorted or indiscernible Ex :- is wifi signal, strength. is weaker than the routes.

Distortion :- interruption of transmitting signals that causes an unclear reception.

What is WEB and what's the Difference bet^n web & internet?

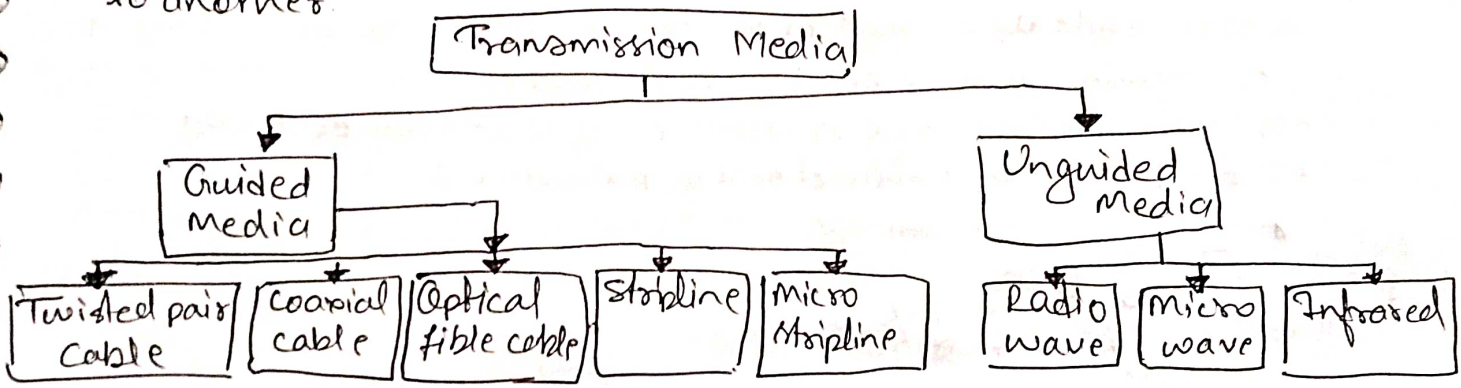
→ The internet is a global network of networks while the web or World Wide Web (www) is a collection of information that is accessed via the internet.

◆ The internet is infrastructure while the web is served on top of that infrastructure.

• Web applications uses HTTP protocal which is a layer over TCP protocal, whereas internet applications can either use TCP or UDP protocal.

Transmission Media :.

→ A Transmission Media a path between transmitter & Receiver. i.e. it is the channel through which data is sent from one place to another.



1. Guided Media :- Wired or Bounded ~~Gui~~ transmission Media.
- Signals being transmitted via physical link.

Features –
- High speed
- Secure
- Used for shorter distance.

Types →

(i) Twisted Pair Cable :- consist of 2 separatly insulated conductor wires wound about each other. Several such pairs are bundled together in protective sheath. Two types

- Unshielded Twisted Pair (UTP)
→ Consist of two insulated copper wire. twisted around each other.
→ ability to block interference and doesn't depend on physical shield.
→ Used in the telephonic Application
• Least Expensive • Easy to install • High Speed
• Short distance transmission due to Attenuation.

- Shielded Twisted Pair
→ Consist of special jacket (copper braid covering or foil shild) to block external interference
→ Used in fast data rate Ethernet.
• More Expensive • Bulky • diff. to install
• Better performance.

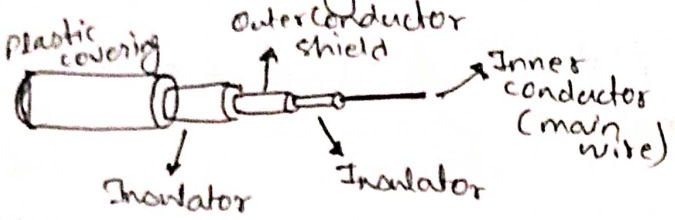
(ii) Coaxial Cable :- It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having separated insulated protection cover.

→ Transmit information in two modes:

① Baseband mode : dedicated cable Bandwith

② Broad band mode: cable bandwith is split into separate ranges.

→ Cables TVs and analog TV network uses coaxial cables



Advantages:

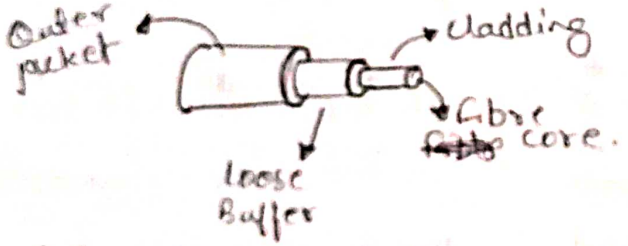
- High Bandwidth
- Better Noise Immunity
- Easy to install and Expand
- Inexpensive

Disadvantages:-

- Single cable failure can disrupt the entire network.

(iii) Optical Fiber Cable :- It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic called cladding.

- This is used for large transmission of large volumes of data.
- The cable can be unidirectional or bidirectional.



Advantages

- Increased capacity & Bandwidth
- Lightweight
- Less Signal Attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials.

Disadvantages

- Diff. to install & maintain
- High cost
- Fragile

(iv) Stripline :- It is a transvers Electromagnetic transmission line medium invented by Robert M. Barrett in 1950's.

- Stripline is the earliest form of planar transmission line
- Uses a conducting material to transmit high frequency wave.
- In this, the conducting material is sandwiched b/w two layer of ground plane which are usually shorted to provide EMI immunity.

(v) Microstripline :-

- In this, the conducting material is separated from the ground plane by a layer of dielectric.

2 Unguided Media :- also refered as Wireless or Unbounded transmission media

→ No. physical medium is required.

Features- • The signal is Broadcasted through air.
• Less Secure
• Used for large distances.

Types :-

(i) Radio Waves :- • easy to generate
• can penetrate through buildings.
• Sending & Recieving antennas need not be aligned.
• Range : 3 KHz – 1 GHz.
• AM & FM radios and cordless phones uses Radio waves.

(ii) Microwaves :- • Sending and Recieving antennas need to be properly aligned with each other.
• Distance covered by signals is directly proportional to height of antenna.
• Fre. Range : 1 GHz – 300 GHz.
• Mainly used for mobile phone communication & Television Distribution

(iii) Infrared :- • Used for short distance communication.
• cannot penetrate through obstacles
• Fre. Range : 300 GHz – 400 THz.
• Used in TV Remote, wireless mouse etc.

Computer Network Devices :-

1 Hub :- • Works at physical layer and hence connect devices physically
• It uses Twisted pair cables to connect devices.
• They are designed to transmit the packets to other appended devices without alternating any of the transmitted packets recieved.
• They transmit the info regardless of the fact if data packet is destined for the device connected or not.

Two Categories :-

(i) Active Hub (Repeaters) :- • Smarter than the passive Hub, They provide path for signals also they regenerate, concentrate and strengthen the signal before sending to destination. It is also called as "Repeaters".

(ii) Passive Hub :- They more like a point contact for the wires to built in the physical Network. They have nothing to do with modifing the signals.

2 Ethernet Hub :- It is a device connecting multiple Ethernet devices together and make them perform like the functions as a single unit.
- They vary in terms of speed.
- It communicates in half-duplex mode where chance of data collision are inevitable most of the time.

3 Switches : Switches are the linkage points of an Ethernet network.
- Devices in swiches are connected through twisted pair cables.
- Switches transfer data packets only to that port which is connected to destination devices. A swiches does so by having a built-in learning of MAC address of devices connected to it.
- Since transmission of data signals are well defined in a switch hence the network performance enhanced.
- Switches Operates in full duplex mode where devices send & received data simultaneously.

4 Modem :- Modulator-Demodulator (Modem) is a device which converts computer-generated digital signals to analog signals, and also capable of again converting analog signals to digital signals at receiving end.

Common types include:- half-duplex modem, full-duplex modem, 2 wire modem, 4-wire modem, synchronous and Asynchronous modem.

Modem stands for Modulator-Demodulator device assists computer in transferring data and information over telephone lines.
It act as modulator when it converts digital data into analog signal and it act as demodulator when it converts analog into digital signal.

5 Gateways :- A Gateway is not a hardware device itself, it is a software firmware which save configuration settings of the device mostly the gateway address in routers is 192.168.0.1 or 192.168.1.1.
It acts as a 'gate' between two networks. It may be routers, firewall, server or other devices that enables traffic to flow in and out of the network, while a gateway protects the nodes within network it also a node itself.

6 Wifi Routers :- Similar like modem is also Modulator and Demodulator the additional feature is wireless connectivity, which is called as Wifi. It has 4-ethernet ports and its having routing, DHCP so that connect 240 pc and devices modem internet with wired & wireless.

7 **Routers**:- When a device in LAN needs to communicate with a device on another ~~LAN~~ LAN, it must send traffic to a specialized device connected to the LAN called a Router. whose purpose is to find the best path for the message to take to arrive at the intended target device, and to send the message along its way following that path.

- Routers are Network layer devices and are particularly identified as Layer-3 devices of the OSI Model.
- They process logical addressing information in the Network ~~add~~ header of the packet such as IP Address.
- It has the ability to connect dissimilar LAN on the same protocol.

Functionality:-

- When a Router receives the data, it determines the destination addr by reading the header of the packet. Ones the address is determined, it searches in its Routing table to get know how to reach the destination and then forwards the packet to the nigher hop on the route. The hop could be the final destination or another routers.

Routing table:- It plays a very pivotal role in letting the router makes a decision. Thus a routing table is ought to be updated and complete. The ways through which a router can recieve information are:-

(i) **Static Routing**:- The routing information is fed into the routing table manally, It does not becomes a time-taking but gets prone to errors as well. Static Routing is feasible for tinniest environment with minimum of one or two Routers.

(ii) **Dynamic Routing**:- For larger environment of Dynamic Routing proves to be the practical solution. The process involves use of peculiar routing protocals to hold communication. The purpose of these protocal is to enable the other routers to transfer information about other routers. So that the other routers can built their own routing tables.

8 **Repeater**:- ~~Repeat~~ Repeater is used to extend the range of radio signal so that the signal can cover longer distances, a repeater is an electronic device that recieves a signal and re-transmits it. Repeaters is used for wired medium as well as wireless medium.

Types of Repeaters

- Analog Repeater
- Digital Repeater
- Microwave Repeater
- Satellite Repeater
- Wifi Repeater/WLAN Repeater
- LTE Repeater
- Optical Repeater.

9 **Bridges:-** A network bridge device is primarily used in LAN's because they can potentially flood and clog a large network thanks to their ability to broadcast data to all the nodes if they dont know the destination nodes MAC Address.

A bridge is a type of network device that provides interconnection with other bridge networks that uses the same protocal.

A bridge is a computer network device that builds the connection with other bridge network that uses the same protocal.

It works at the Data link layer of the OSI model and connects different networks together and develops communication between them.

Bridges are similar to repeater & Hubs in that they broadcast data to every node, However Bridge maintain the Media Access Control (MAC) address table as soon as they discover new segments, so subsequent transmissions are sent to only to the desired recipient.

A bridge uses database to ascertain where to pass, transmit or discard the data frame.

(1) If the frame received by the bridge is meant for a segment that resides on the same host network, it will pass the frame to that node and the receiving bridge will then discard it.

(2) If the bridge receives a frame whose node MAC Address is of the connected network, it will forward the frame toward it.

Types:- Transparent Bridge (2) Source Route Bridge (3) Translation Bridge.

10 **Brouters:-** Brouters are the combination of both the bridge and routers. They take up the functionality of the both networking devices serving as a bridge when forwarding data between networks, and serving as a router when routing data to individual systems.

Brouters functions as a filter that allows some data into the local network and redirects unknown data to the other network.

Brouters operate at both the network layer for routable protocals and at the data link layer for non-routable protocals. As network continue to become more complex a mix of both routable and non routable protocals has led to the need of the combined features of Bridge and routers.

Brouters handle both routable and non routable features by acting as routers for routable protocals and bridges for non-routable protocal.

11 **Network Card** :- also known as Network Interface Card (NICs) are hardware devices that connects a computer with the network.

- It is installed on the mother board
- They are responsible for developing a physical connection between the network and the computer.
  Computer data is translated into electrical signals send to the network via Network Interface Card.
- They also mange some important data-conversion function.

12 **Network Protocol** : Network protocols define a language of instruction and conventions for communication between the network devices. It is essential that a networked computer must have one or more protocol drivers. Usually for two computers to interconnect on a network, they must use identical protocols. At a time, computers are designed to use multiple protocols. Network protocols like HTTP, TCP/IP offer a basis on which much of internet stands.

13 **Integrated Services Digital Network (ISDN)** :- ISDN are used to send over graphical or audio data files. It is a WAN Technology that can be used in place of a dial up link.
It surely prodives higher speed than a modem and has the capability to pick up the line and drop it considerably at a faster rate.

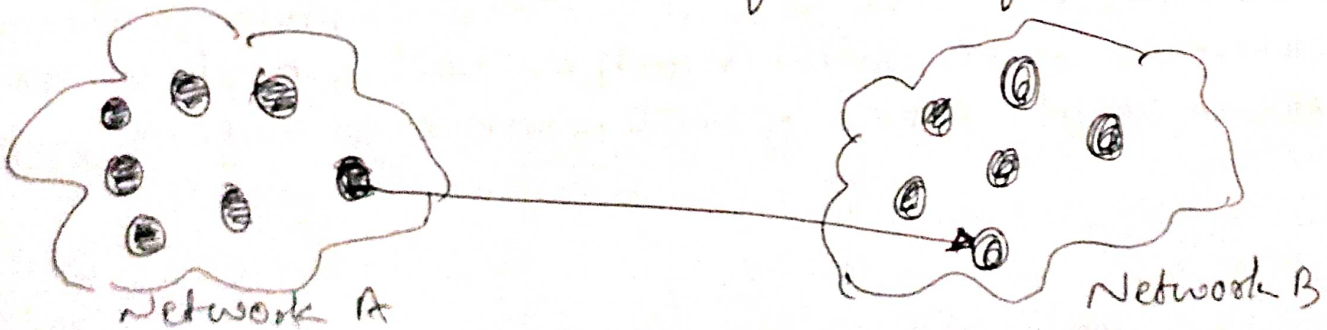
Unicast, Broadcast & Multicast

Cast :- cast term signifies some data (stream of packets) is being transmitted to the recipient from client.

1 **Unicast**:- • One-to-One transmission

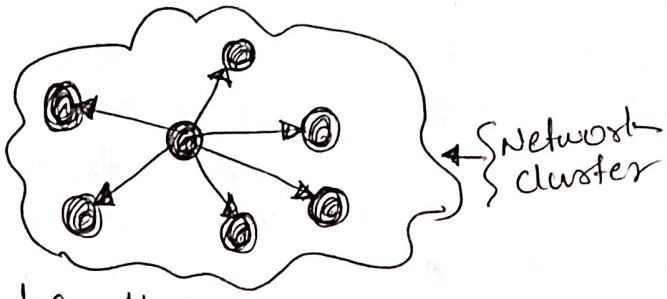
- This type of information transfer is useful when there is participation of single sender and single recipient.

For Example : a device having IP address 10.1.2.0. in a network wants to send the traffic stream (data packets) to the device with IP address 20.12.4.2 in other network, then unicast comes into picture.
This is the most common form of data transfer over the Network.

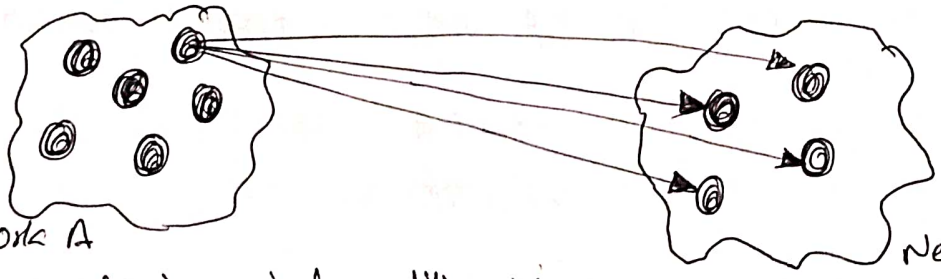


[2] Broadcast : Broadcasting transfer (one-to-all) techniques can be classified into two types.!-

(i) Limited Broadcasting :- Suppose you have to send stream of packets to all devices over the network that you reside, this Broadcasting comes handy. For this to achieve, it will append 255.255.255.255 (i.e. all the 32 bits of IP address set to 1) called as Limited Broadcast Address in the destination address of datagram(packet) header which is reserved for information transfer to all the recipients from a single client (sender over a Network).



(ii) Direct Broad Casting :- This is useful when a device in one network wants to transfer packet stream to all the Devices over the other network. This is achieved by translating all the Host ID part bits of destination Address to 1, reffered as Direct Broadcasting Address in datagram Header for information transfer.



— This mode is mainly utilized by television network for video & Audio distribution.

— One important protocol of this class in computer Network is Address Resolution Protocol (ARP) that is used for Resolving IP Address into physical Address which is necessary for underlying communication

[3] Multicast :- In multicast one/more senders and one/more recipients participate in data transfer traffic. ~~For this~~, Multicast lets server's direct single copies of data stream that are then simulated and routed to hosts that request it.

IP multicast requires support of some other protocols like IGMP (Internet Group Management Protocol), Multicast routing for its working. Also in classful IP Addressing Class D is reserved for multicast group.

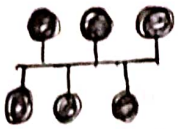
Topologies :

→ Network Topologies describe the methods in which all the elements of network are mapped, Network Topology specifies the layout of a computer network. It shows how devices and cables are connected to each other.

1 Point to Point (P-2-P)

→ In this method, the network consist of direct link bet^n two computers.
→ Fastes & highly reliable than other types, since there is direct connect^n
→ No need for network Operating System
→ No need of an expensive server as individual workstations are used to access the files.
→ You cant backup files.
→ Used for small areas only where computers are in close proximity.
→ No security.

2 Bus Topology :-

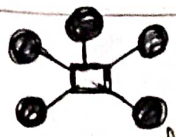


→ Bus Topology is a network topology in which all nodes are connected to a single cable known as central cable or bus
→ It acts as shared communication medium i.e. If any device wants to send the data to other devices, then it will send the data over the bus which in turn sends the data to all attached devices.
→ Useful for small numbes of devices.
→ As if the bus is damaged then the whole network fails.

3 Ring Topology :-

→ Ring topology is a network topology in which nodes are exactly connected to neighboring devices for communication purpose. and thus forming a single continuous path for transmission. It is called a ring topology as its formation is like a ring.
→ Does not need any central server to control the ~~cont~~ connectivity amoung the nodes.
→ If single node is damaged, whole network fails.
→ Ex. SONET network, SDH network etc.

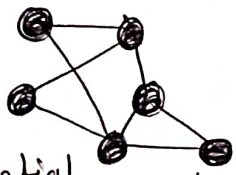
4 Star Topology :-



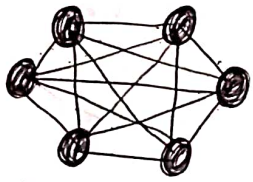
→ In this, all nodes are connected to a single device known as a central device.
→ Requires more cables as compaire to other topologies. Therefore it is more robust as a failure in one cable will only disconnect a specific computer connected to that cable.
→ If the central device falls, whole network fails.
→ Easy to install, manage and troubleshoot. used in home & office

5 Mesh Topology :-

→ In this, all the nodes are individually connected to other nodes
→ Does not need any central hub or switch.
→ It is robust as a failure in one cable will only disconnect the specific computer. connected to this cable.
→ Offers a high level of redundancy, so even if one network cable fails, still has alternative path for data to reach the destination.
→ two types :-
① Partial Mesh Topology :- In this, all nodes are not connected to each other
② Full Mesh Topology :- all nodes are connected to each other.



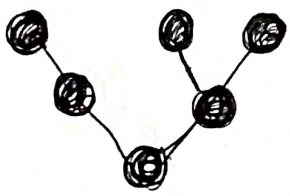
Partial Mesh



Full Mesh

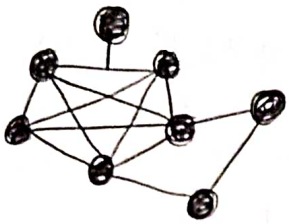
6 Tree Topology :-

→ Tree topology have a root node, and all the other nodes are connected which form a hierarchical topology.
→ In this, All the star networks are connected to a single bus.
→ In this the whole network is divided into segments known as star networks which can be easily maintained. If one segment is damaged there is no effect on other segments.
→ Tree topology depends on the main bus and if it breaks, then the whole network gets damaged



4 Hybrid Topology :-

→ A Hybrid Topology is a combination of different topologies.
→ For example if star topology is connected with different topology, then it becomes a Hybrid topology.
→ It provides flexibility as it can be implemented in a different network environment.
→ The design of Hybrid topology is complex.



Different Types of Networks :-

→ Network can be divided on the basis of area of distribution :-

1 LAN (Local Area Network)

→ It is a group of network devices that allow communication between various connected devices. Private ownership has control over LAN rather than public
→ LAN ~~has~~ has short propagation delay than MAN and WAN.
→ Used for small geographical location like office, shool etc.

2 MAN (Metropolitan Area Network)

→ It covers a larger area than LAN such as small towns, cities etc.
→ MAN connects two or more computers that reside within the same or completely different cities.
→ MAN is expensive and should or might not be owned by one organizat^{n}.

3 WAN (Wide Area Network)

→ Covers larger area than LAN and MAN such as country
→ PSTN or satellite medium is used for wide area network.
→ WAN also might not be owned by one organization.
→ Transmission speed is low.

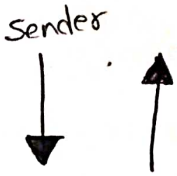
Other than that -

- PAN (Personal Area Network) :- Range is limited upto 10 meter, Created for personal use, Generally personal Devices are connected to this network.
- CAN (Campus Area Network) :- It is a connection of devices within campus area which links to other departments of organizat^{n} within some campus
- GAN (Global Area Network) :- It uses satellites to connect devices over the global area.

OSI Model

OSI Model :- OSI stands for Open System Interconnection Model is a conceptual framework used to describe the functions of a networking system. developed by International Organization for Standardization (ISO) in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

7 layers Are :-



① Application Layer
② Presentation Layer
③ Session Layer
} Software Layer

④ Transport Layer
⑤ Network layer
⑥ Data Link layer
⑦ Physical Layer.
} Hardware Layer

Brief Explanation of All Layers :-

1. Physical Layer [Layer 1] :-

→ The lowest layer of OSI model is physical layer
→ It is responsible for the actual physical connection between the devices
→ The physical layer contains information in the form of bits.
→ It is responsible for transmitting individual bits from one node to other. when receiving data, this layer will get the signal received and converts it into 0's and 1's and send them to the Data link layer, which will put the frame back together.
→ Function of physical layer :-

(i) Bit Synchronization :- The physical layer provides the synchronization of bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.

(ii) Bit rate control :- The physical layer also defines transmission rate, i.e. the number of bits sent per second.

(iii) Physical topologies : Physical layer specifies the way in which the devices/nodes are arranged or connected in a network. i.e. bus, star, or mesh etc. topology.

(iv) Transmission Mode :- Physical layer also defines the way in which data flows between two connected device. The various transmission modes possible are Simplex, Half-duplex, full duplex.

NOTE :- Hub, Repeater, Modem, Cables are Physical Layer Devices

- Network layer, Data link layer, and Physical layers are also known as Lower Layer or Hardware Layers.

2. Data Link Layer [Layer2]

→ Data Link Layer is responsible for the node-to-node delivery of the message.

→ The main function of this Layer is to make sure data transfer is error-free from one node to another, over the physical layer.

→ When a packet is arrived in a network, it is the responsibility of Data link Layer to transmit it to Host using its MAC Address.

→ Data Link Layer is divided into two sublayers.

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

→ The packet received from the Network layer is further divided into frames depending on the size of NIC (Network Interface card)

DLL also encapsulates Sender's and Receiver's MAC address in the Header

→ The receiver's MAC Address is obtained by placing an ARP (Address Resolution Protocol) request onto the wire asking "Who has that IP Address?" and the destination Host will reply with its MAC Address.

→ Functions of DLL Are :-

(i) Framing :- Framing is a function of DLL. It provides a way for a sender to transmit a set of bits that are meaning full to the receiver. This can be accomplished by attaching special bit patters to the beginning and end of the frame (AKA. Header & Footer)

(ii) Physical Addressing :- After creating frames, DLL adds physical address (MAC Address) of sender and/or receiver in the Header of each frame.

(iii) Error Control :- Data Link Layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.

(iv) Flow Control : The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving acknowledgement.

(v) Access Control : when a single communication channel is shared by multiple devices, the MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

NOTE : Packets in Data Link Layer is refered as **Frames**.

- Data Link Layer is handled by the NIC (Network Interface Card) and device drivers of Host machine.
- Switch & Bridge are Data Link Layer devices.

3. Network Layer [Layer3] :

→ Network layer works for the transmission of data from one host to the other located in different network.
→ It also takes care of packet routing i.e. selection of shortest path from one host to other host to transmit the packet, from the number of routers available (Hop-By-Hop routing).
→ The Sender & Receiver's IP addresses are placed in the header by network layer.
→ Functions of Network Layer :-

(i) Routing :- The network layer protocols determine which route is suitable from source to destination. This function of Network layer is called Routing.

(ii) Logical Addressing : In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme. The Sender's & Receiver's IP addresses are placed in the Header by the network layer. Such an address distinguishes each devices uniquely and universally.

NOTE : Packets in Network layer is refered as ~~Segments~~ **Packets**.
- Network layer is implemented by networking devices such as routers.

4. Transport Layer [Layer4]

→ Transport layer provides services to the application layer and takes services from the network layer.
→ Data in Transport Layer is refered as **Segments**.
→ It is responsible for End-to-End Delivery of the complete message. The transport layer also provides the acknowledgement of successful data transmission and retransmit the data if an error is found.

(i) At Sender's side :-

→ This layer receives data from upper layer and perfor segmentation and also implements Flow & Error control. to ensure proper data transmission.
→ It also adds source & destination port number in the Header and then forward it to Network layer.
Generally, this destination port no. is configured either by default or manually.

NOTE :- The Sender need to know the port No. assosiated with the receiver's requested Application.

(iii) At Receiver's Side :

→ Transport Layer reads the port Number from its Header and forward the Data which it has received to the respective application. Also perform sequencing and reassembling of the segmented data.

Functions of Transport Layer :

(i) Segmentation & Reassembly : This layer accepts the message from the session layer, breaks the message into smaller units. Each of the segments produced has a header associated with it. Transport layer at destination station reassemble the message.

(ii) Service Point Addressing (SPA) :- In order to deliver the message to correct process, the transport layer header includes a type of address called service point Address or Port Address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

Services provided by the Transport Layer :

(i) Connection-Oriented Services :- It is a three-phase process (or 3-way or 3-way Hand Shake that includes :-

- Connection Establisment
- Data Transfer
- Termination / Disconnection.

■ In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

(ii) Connectionless Service :- It is a one-phase process and includes Data transfer. In this type of transmission, the receivers does not acknowledge receipt of a packet. This approach allows for faster communication between devices.

NOTE : Data in Transport layer is called segments.

- Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application layer by making the system calls.
- Transport Layer is called as Heart of OSI Model.

Session Layer [Layer 5]

→ This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensure security.

→ Functions of session Layer are :-

(i) Session Establishment, maintenance and termination :- This layer allows the two processes to establish, use and terminate a connection.

(ii) Synchronization :- This layer allows the process to add checkpoints which are considered as synchonization points into the data. These synchronization points helps to identify the errors so that the data is re-synchronized properly, and ends of the message are not cut prematurely so that the data loss is avoided.

(iii) Dialog Controller :- The session layer allows two systems to start communication with each other in half duplex or full duplex.

NOTE : Implementation of these 3 layers (session, Presentation & Application) is done by the network application itself. These are known as Software layers.

6 Presentation Layer [Layer6] :-

→ Presentation Layer also called as Translation layer.
→ The Data from the application layer is extracted here and manipulated as per the required formate to transmit over the network.
→ Functions of the Presentation Layer.

(i) Translation : For Ex. ASCII to EBCDIC. [Extended Binary Code Decimal Interchange Code]

(ii) Encryption/Decryption :- • Encrypts the data or decrypts the data.
• The encrypted data is known as cipertext and decrypted data is known as plain text. A key value is used for encrypting and decrypting the data.

(iii) Compression :- Reduces the number of bits that need to be transmitted on the network.

7 Application Layer [Layer7]

→ Application Layer is implemented by the network Applications. These applicatn produce the data, which has to be transmitted/Transfered over the Network.
→ This app layer also serves as a window for the application services to access the network and for displaying the received information to User.
Ex. Application like Browsers, messenger etc.

NOTE : Application layer is also known as Desktop layer.

→ Functions of Application layer.

(i) Network Virtual Terminal
(ii) FTAM - File Transfer Access and Management
(iii) Mail Services
(iv) Directory Services.

" OSI Model acts as a reference Model and its not implemented on Internet. TCP/IP Model is being Used "

TCP/IP Model

#TCP/IP Model : The TCP/IP model was designed and developed by Department of Defense(DoD) in 1960's and is based on standard protocols. It stands for Transmission Control Protocol/ Internet Protocol.
The TCP/IP model is a concise version of OSI model. It contains four layers, unlike ~~7~~ 7 layers in OSI model. The layers are :-

1. Process/Application Layer
2. Host-To-Host Layer/Transport Layer
3. Internet Layer
4. Network Access/Link Layer.

- The first layer Process layer is on the behalf of sender and Network Access layer on the behalf of Receiver.

#Explanation of layers :-

1. Network Access Layer

→ This layer corresponds to the combination of Data link layer & physical layer in OSI model.
→ It looks out for Hardware addressing and the protocols present in this layer allows for the physical transmission of Data.

2. Internet Layer (Network Layer)

→ This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of Data over the network.
Main Protocal residing at this layer :-

(i) IP (Internet Protocol) :- Responsible for delivering packets from source host to destination host by looking at the IP addresses in the Header. two versions :- IPv4 & IPv6. IPv4 is the one that most of the websites are using currently but IPv6 is growing as IPv4 is limited.

(ii) ICMP (Internet Control Message Protocol) :- It is encapsulated within IP datagram and is responsible for providing hosts with Info. about network problems

(iii) ARP (Address Resolution Protocol) : Its job is to find Hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP, Inverse ARP.

3 Host-to-Host Layer (Transport Layer)

→ This layer is similar to Transport Layer of OSI model.
→ It is responsible for End-to-End communication and Error-free delivery of data.
→ It shields the upper layer applications from complexities of data.
→ Main Protocol Presents are :-

(i) Transmission Control Protocol : It is known to provide reliable and Error-free communication between end systems. It performs sequencing and segmentation of data.
It also has acknowledgement features and controls the flow of data through flow control mechanism.
It is very effective protocol but has alot of overhead due to such feature. Increased overhead leads to increase cost.

(ii) User Datagram Protocol : It does not provides such features like TCP. It is the go-to protocol. if the application does not require reliable transport as it is very cost effective. Unlike TCP, which is connection-Oriented protocol, UDP is connectionless.

4 Application Layer

→ This layer performs the functions of top three levels of OSI model i.e. Application Layer, Presentation and Session Layer
→ It is responsible for node-to-node communication and controls user-interface specifications.
→ Some important protocols in Application Layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, NTP, DNS, DHCP, NFS, X window, LPD.
Some of them are :-

(i) HTTP and HTTPS :- stands for HyperText Transfer protocol. It is used by world wide web to manage communication betⁿ web browsers and servers. while HTTPS stands for HTTP-Secure. it is a combination of HTTP with SSL (Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign-in, authenticate and carries bank transactions.

(ii) SSH : stands for Secure Shell. It is a terminal emulations software like Telnet. The reason SSH is more preferred because of its ability to maintain encrypted connection. It sets up a secure session over a TCP/IP connection.

(iii) NTP :- Stands for Network Time Protocol. It is used to synchronize the clock on our computer to one Standard Time Source. It is very useful in situation like bank transactions. Assum a situation without NTP, suppose you carry out a transaction where your computer reads the time 2:00 PM while Server records it 2:30 PM. The Server can crash very badly if its out of sync.

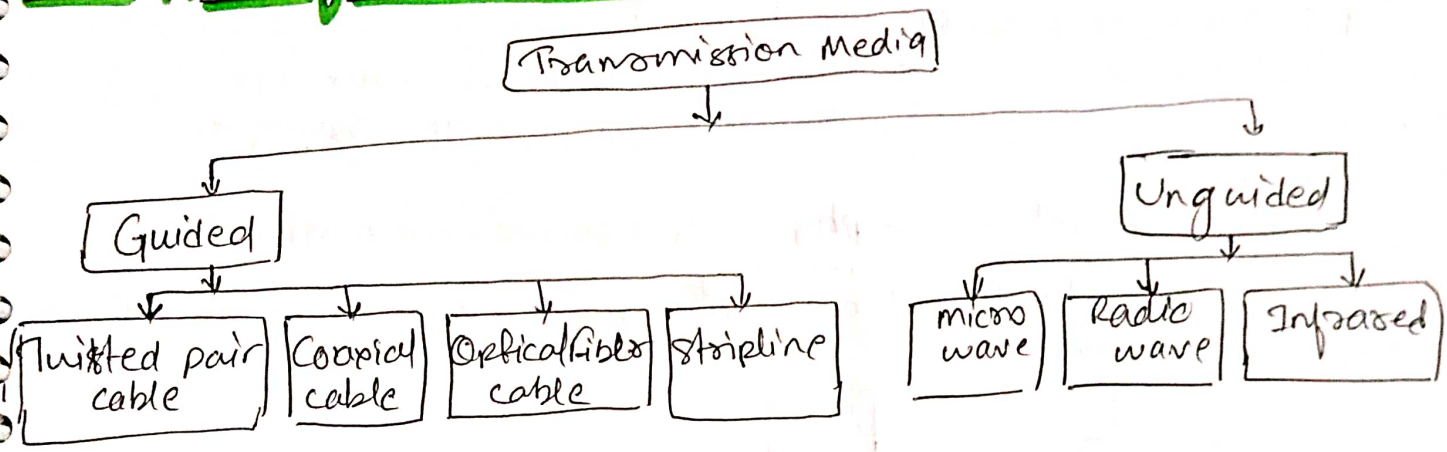
1. Physical Layer

Networking Devices:

- HUB, Switches, Routers, Gateway, Brouters, NICs etc.

** Already Covered **

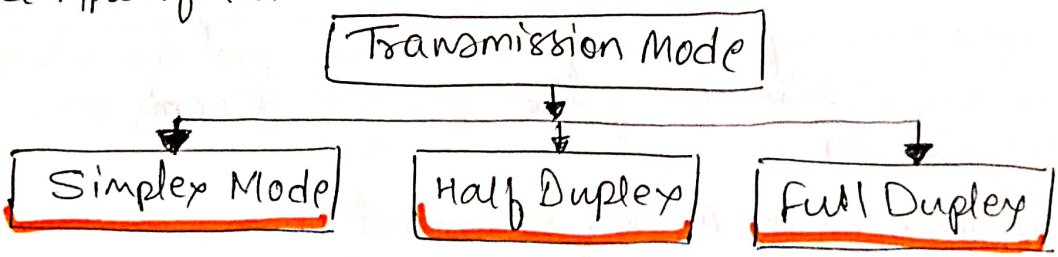
Types of Transmission Media



** Already Covered **

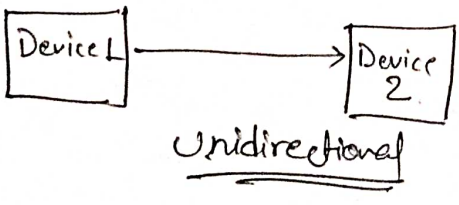
Transmission Modes in Computes Network

→ It means transferring data between two devices. It is also known as communication mode.
→ Three types of Transmission mode.



1. Simplex Mode :-

→ Communication is unidirectional.
→ The simplex mode can uses the entire capacity of the channel to send data in one direction.
Eg Keyboard only input and monitor only output.

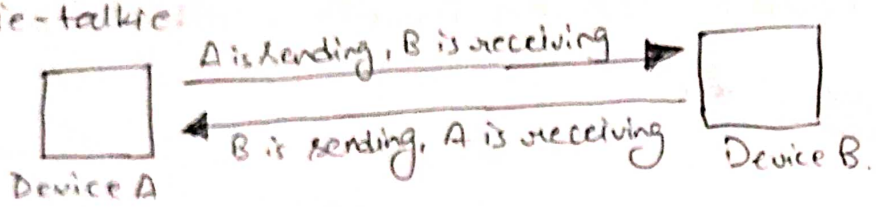


2 Half Duplex :

→ In Half Duplex, each station can both transmit and receives, but not at the same time. When one device is sending, other can only receive at that time. and vice versa,

→ The entire capacity of channel can be utilized for each direction

Ex Walkie-talkie



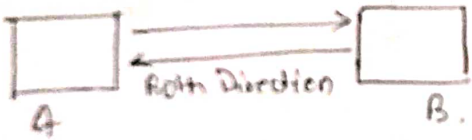
3 Full Duplex :

→ Full Duplex mode, both station can transmit and receive simultaneously.

→ In full Duplex mode, signal going in one direction share the capacity of the link with signal going in another direction. This sharing occurs in two ways :

- Either the link contain two physically separate transmission path, one for sending, one for receiving
- Or the capacity is divided between signals travelling in both direction

Ex Telephone Network



Analog to Digital

Digital Signal : A digital signal is a signal that represents data as a sequence of discrete values; at any given time, it can only take on one of a finite numbers of values.

Analog Signal : An analog signal is any continuous signal for which the time varying feature of signal represents of some other time varying quantity.

Following Technique used for Analog to Digital

1. Pulse code Modulation
   - (i) Sampling
   - (ii) Quantization
   - (iii) Encoding
2. Delta Modulation
3. Adaptive Delta Modulation.

1. **Pulse Code Modulation** : It is a common technique to change analog to digital. It has three process:

(i) **Sampling** : It is a process of measurement of ~~the~~ amplitude of continuous-time signal at discrete instants, and converting the continuous-signal into discreate signal three sampling method.

(a) Ideal sampling (b) Natural sampling (c) Flat top sampling.

(ii) **Quantization**: The digization digitization of analog signals involves the rounding off ~~the~~ of the values which are approximately equal to analog values. The method of sampling chooses a few points to the analog signal, then this points are joined to round off value to a near stabilized value. Such a process is called Quantization.

Quantization introduces various types of sources of errors in your algo. such as rounding errors, underflow or Overflow.

(iii) **Encoding** : After each sample is quantized and the number of bits per sample is decided, each sample can be changed to an n bit code.

Encoding also minimize bandwidth used.

2. **Delta Modulation** : since PCM is very complex technique, other techniques have been developed. The simplest is delta modulation.

→ Delta Modulation finds the change from previous value.

Modulator: It is used at sender site to create a stream of bits from analog signal.

→ The process records small positive change called delta.

If delta is positive process records 1 otherwise 0.

3. **Adaptive Delta Modulation** : The performance of delta modulation can be improved by making step size of modulation assume a time varing form.

Digital to Analog Conversion

→ Techniques are :-

1. **Amplitude data keying** :- In this carrier signal is analog and data to be modulated is digital. The amplitude of analog signal is modified to reflecting binary data.

~~2 Frequency key shi~~

2. **Frequency shift keying** : In this modulation the frequency of analog carrier signal is modified to reflect binary data.

3. **Phase Shift keying** : In this modulation the phase of the analog carrier signal is modified to reflect binary data. The The amplitude and fre. of carrier signal remains same.

Design Issues in Physical Layer

- The physical layer is basically concerned with transmitting raw bits over a communication channel.
- Mainly the design issues here deal with electrical, mechanical, timing interface, and physical transmission medium, which lies in it.
- Design issue has to do with making sure that when 1 bit send from one side it is received 1 bit by other side also not as a 0 bit.

2 Data Link Layer

Multiple Access Protocols:

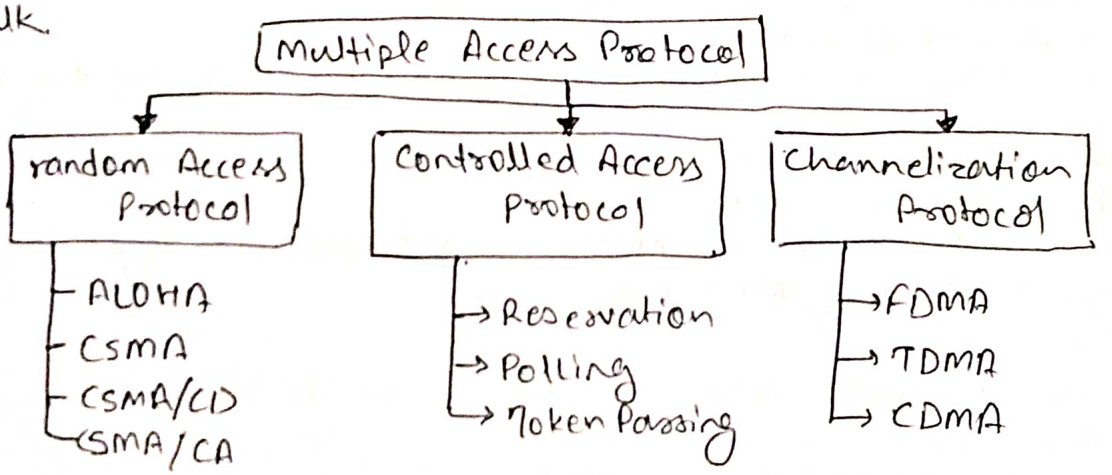
→ The Data Link Layer is responsible for transmission of data between two nodes. its main functions are:-
(i) Data Link Control
(ii) Multiple Access Control.

[1] Data Link Control:

→ The data link control is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control and flow control
→ DLC used to provide reliable data transfer over physical medium. Data link layer provides the coordination among the devices so that no collision occurs.

[2] Multiple Access Control:

→ If there is a dedicated link between the sender and the receiver then data link control layer is insufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple Access protocols are required to decrease collision and crosstalk.



(1) Random Access Protocol: All stations have same priority. Any station can send data depending upon medium's state.

(2) Controlled Access Protocol: The data is send by that station which is approved by other stations.

(3) Channelization: In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

NOTE: MAC addresses are used in this sublayer of DLL (i.e. Multiple Access Control)

Peer-to-Peer (P2P) File Sharing

→ P2P is a file sharing technology, allowing the users to access mainly the multimedia files like videos, music, games etc. The individual users in this network are refered to as peers. The peers request files from other peers by establishing a TCP or UDP connection.

How P2P works :-

→ A P2P networks allows computer hardware and software to communicate without the need for a server. Unlike client-server architecture.

→ The peers directly interact with one another without the requirement of a central server.

→ Now, when one peer makes a request, it is possible that multiple peers have a copy of that requested object. Now the problem is how to get the ip address of all those peers. This is decided by the underlying Architecture supported by the P2P systems.
By means of one of these method client-peer can get to know about all other peers which have the requested object/file and the file transfer take place directly between these two peers.

→ Three such architectures are :-

1. Centralized Directory
2. Query flooding
3. Exploiting Heterogeneity.

1 Centralized Directory :-

→ It is similar to client-server architecture as it also maintains a huge central server to provide directory service.

→ All the peers inform this central server of their IP Address and files they have for sharing.

→ The server queries the peers at regular interval to make sure that peers are still connected or not.

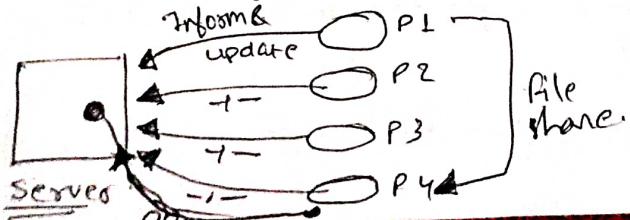
→ So basically this server maintains a huge database regarding which file is present at which IP address.

WORKING :-

- Whenever a request peer comes in, it sends its query to server.
- Since the server have all the information of its peer, so it returns the IP address of all peer having requested file to the client peer.
- Now file transfer takes place between two peers.

Problem :-

- The main problem with this architecture is that there is a single point of failure. If the server crashes, the whole P2P network also crashes.
Also since all the processing is to be done by single server so a huge amount of database has to be maintained and regularly updated.



[2] Query Flooding :-

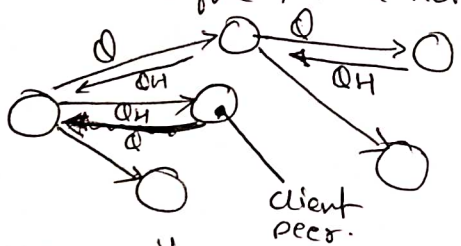
→ Unlike Centralized approach, this method makes use of distributed systems.
→ In this, the peers are supposed to be connected to an overlay network. It means if a connection/path exist from one peer to another it is a part of this overlay network
→ In this overlay network, peers are called nodes, and connection between peers is called an edge between the nodes. Thus resulting in graph like structure.

WORKING :-

- when client peer request for some file. this request is sent to all the neighbouring nodes i.e. to all nodes which are connected to this node. If those nodes dont have the required file they passes the query their neighbours and so on. This is called Query Flooring.
- when the peer with the requested file is found (referred to as query hit) the query flooding stops and it sends back the file name and file size to the client, thus following the reverse path.
- If there are multiple query hits, the client selects from one of these peers.

Disadvantage :-

→ The query has to be sent to all the neighbouring peers unless a match is found. This increase the traffic in the network.



Q = Query
QH = Query Hit.

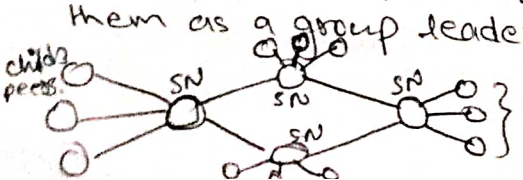
[3] Exploiting Heterogeneity :-

→ This P2P architecture uses of both the above-discussed system.
→ It resembles with Gnutella (distributed system like Gnutella because there is no central server for query processing.
→ But unlike Gnutella, it does not treat all it peer equally. The peer with higher bandwidth and network connectivity are at higher priority and are called group leaders / supernodes. The rest of the peers are assigned to these supernodes.
→ These supernodes are interconnected and the peers under these, inform their respective leaders about their connectivity, IP address, and files available for sharing.

WORKING :-

- This structure can process the queries in two ways :-

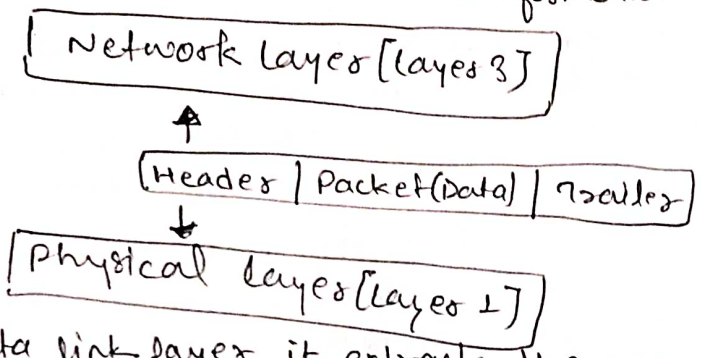
(i) the supernodes could contact other super nodes and merge their database with their own database. Thus this supernodes now has information of a large numbers of peers.
(ii) Another approach is that when a query comes in, it is forwarded to the neighbouring super nodes unit a match is found, just like in Gnutella. Thus query flooding exist with limited scope as each supernodes has many child peers. Hence such a system exploits the heterogeneity of the peers by designating some of them as a group leader and other as their child peer.



SN = Supernodes.

Framing in Data Link layer

- Frames are the Protocol Data Unit (PDU) in Data Link layer
- Framing is a point-to-point connection between two computers consists of a wise in which data is transmitted as a stream of bits. However these bits must be framed into discernible blocks of information.
- It provides a way for a sender to transmit a set of bits that are meaningful to the receiver.
- Frames have headers that contains information such as error-checking codes.



- At the data link layer, it extracts the message from the sender and provides it to the receiver by providing the sender's and receiver's addresses. The advantage of using frames is that data is broken up into recoverable chunks that can easily be checked for corruption.

Types of framing :- (two types):

① Fixed size ② Variable size.

Ethernet:

- Ethernet is the most widely used LAN Technology, which defined under IEEE standards 802.3. The reason behind its wide usability is Ethernet is easy to understand, implement, maintain, and allows low-cost network implementation.
- Ethernet generally uses Bus topology
- Ethernet operates in two layers of OSI model, Physical layer, and Data link layer. For ethernet protocol data unit is frame since we mainly deal with DLL.
- In order to control collision, the access control mechanism used in ethernet is CSMA/CD
- Manchester encoding used in Ethernet

Carrier Sense Multiple Access (CSMA)

- This method was developed to decrease the ~~collision~~ chances of collision when two or more stations start sending their signals over DLL. CSMA requires that each station first check the state of medium befor sending

Error Detection

Error:

A condition when the receiver's information does not ~~math~~ match with the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or 1 bit may change to 0.

Error Detecting Code (implemented in DLL or Transport Layer)

→ When a msg is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this we uses error detection code.

→ Basis approach used for error detection is the use of redundancy bits. where addition bits are added to facilitate detection of errors.

→ Some popular techniques are :-

1. Simple Parity Check
2. Two-dimensional Parity Check
3. Checksum
4. Cyclic Redundancy check

Introduction of MAC Address

→ Media Access Control Address is a physical address which works at Data Link Layer.

MAC Address :- MAC Address are unique 48 bits hardware number of a computer, which is embedded into NIC during the time of manufacturing. MAC address is also known as physical address of a network device.

MAC address is used in ~~M~~ Med. multiple Access control (sublayer of DLL)
MAC address is worldwide unique, since millions of network devices exists.

Formate of MAC Address :-

→ MAC address is a 12 digit hexadecimal number (6-Byte Binary number) which is mostly represented by Colon-Hexadecimal notation.

→ First 6-digit of MAC address identifies the manufacturer. called as OUI (i.e. Organizational Unique Identifier), IEEE Registration Authority Committee assign these MAC prefixes to its registered vendors.

Ex 3C:5A:B4 ⟶ google, Inc.
CC:46:D6 ⟶ Cisco

→ The rightmost six digit represents the Network Interface controller which is assign by manufacturer.

→ Representation (3 ways) :-

1. 00-0a-83-b1-c0-8e
2. 00:0a:83:b1:c0:8e
3. 000.a83.b1c.08e

Types of MAC Address

1) Unicast
2) Multicast
3) Broadcast.

Types of Switches :

→ Switches are connectivity points of an Ethernet network. These are small devices that can receive data from multiple input ports and send it to the specific output port that takes data to its intended destination in the network.

Types of switches :-

1 Unmanged Switches :

→ These are the switches that are mostly used in home networks and small businesses as they plug in and instantly start doing their job and such switches do not need to be watched or configured.
These requires only small cable connections.
It allows devices on a network to connect with each other such as computer to a computer or a computer to a printer.
They are least expensive switches.

2 Managed Switches :

→ These type of switches have many features like the highest level of ~~requ~~ security precision control, full mangement of the network. These are used in organizations containing a large network and can be customized to enhance the functionality of certain network.
These are costly options but their scalability makes them an ideal option for a network that is growing.
They are achieved by setting Simple Network Management Protocal (SNMP)
They are of two types :-

(i) Smart switches
- → offers basic management features with ability to create some level of security
- → also called as partial managed switches,
- → mostly used in fast & constant LAN

(ii) Enterprise Managed Switches
- → features like ability to fix, copy, transfer and display diff. network configuration along with web interface SNMP and command line interface
- → fully manged switches, more expensive,
- → used in organization with large number of ports, switches and nodes.

3 LAN Switches :

→ These are also known as ethernet switches or data switches and are used to reduce network congestion or bottleneck by ~~disturbing~~ distributing a package of data only to its intended recipient. These are used to connect points on LANs.

4 PoE switches

→ These switches used in PoE technology which stands for Power over Ethernet that is a technology that integrates data and power on the same cable allowing power devices to receive data in parallel to power. Thus these switches provide greater flexibility by simplifying the cabling process.

3. Network Layer

Introduction :

→ Network layer is the 3rd layer of OSI model.
→ The network layer is concerned with the delivery of packets across multiple network.
It selects and manges the best logical path for data transfer between nodes.
→ This layer contains hardware devices such as routers, bridges, firewall and switches but it actually creates a logical image of the most efficient communication route and implements it with a physical medium.
→ Network layer protocols exist in every host or router. The router examine the header fields of all the IP packets that pass through it.
Internet protocal and netware IPX/SPX are most common ## Protocals in network layer.
→ The network layer responds to requests from the layer above it (transport layer) and issues requests to the layer below it (data link layer).

■ Responsibilities of Network layer :-

Packet Forwarding / Routing of packets : Relaying of data packets from one network segment to another by nodes in computer network.

Connectionless Communication (IP) : A data transmission method used in packet-switched networks in which each data unit is separately addressed and routed based on information carried by it.

Fragmentation of Data : Splitting of data packets that are too longe to be transmitted on the network.

Difference between Internet, Intranet and Extranet :-

[1] Internet

→ The network formed by the co-operative interconnection of millions of computers, linked together is called Internet.

[2] Intranet

→ It is an internal private network built within an organization using Internet and world wide web standards and products that allows employees of an organization to gain access to corporate information.

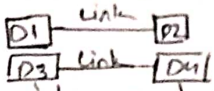
[3] Extranet

→ It is the type of network that allows users from outside to access the ~~Intranet~~ intranet of an organization.
It's a network of internetwork that's restricted in scope to one organization or entity bigger than intranet.

Line Configuration in Computer Network

→ A network is a two or more devices connected through a link. A link is a communication pathway that transfer data from one device to another. Devices can be computer, printer etc. or any other devices that is capable of receiving and sending of data.
For communication occurs, two devices must be connected in some ways to the same link at the same time, There are two possible ways of connections:-
① Point-to-point connection
② Multiple point Connection OR Multipoint connection.

1 Point-to-point connection:-



- A point-to-point connection provides a dedicated link between two devices
- The entire capacity of the link is reserved for transmission between those two devices.
- Most point-to-point connection use an actual path length of wire or cable to connect two ends, but other options like microwave or satellite links also possible.
- Point to Point network topology is considered to be one of the easiest and conventional network topology.
- It is also simplest to establish and understand.

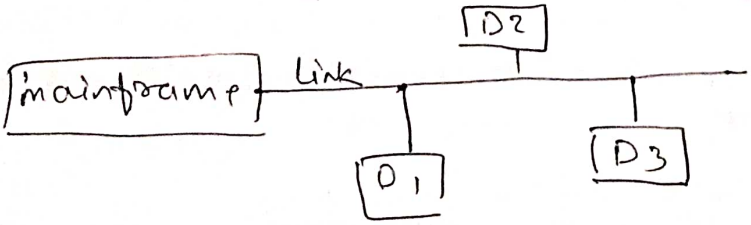
Ex Remote control and T.V. is ex. of P2P connection.

2 Multipoint Connection:

→ Also called as multidrop connection. In this connection two or more devices share a single link.
- More than two devices share the link that is the capacity of the channel is shared now. With shared capacity, there can be two possibilities in a multipoint Line Configuration.

(i) Spatial sharing: If several devices can share the link simultaneously its called Spatial shared Line Configuration

(ii) Temporal (Time) sharing: If users must take turns using the link, then it is called Temporally shared or Time shared Line Config



Difference Between Unicast, Multicast, and Broadcast

Unicast : One-to-One transmission

Broadcast : One-to-all transmission

Multicast : One/more Sender to One/more Recipients.

** Already Covered **

Collision Domain and Broadcast Domain in Computer Network

1 Collision Domain

→ A Collision Domain is a Scenario in which when a device sends out a message to the network, all other devices which are included in its collision Domain have to pay attention to it, no matter if it was designed them or not. This causes the problem because, in a situation where two devices send out their messages simultaneously, a collision will occur leading them to wait and re-transmit their respective messages one at a time.

** Remember, it happens only in the case of a half-duplex mode.

2 Broadcast Domain

→ A Broadcast Domain is a ~~Sce~~ Scenario in which when a device sends out a broadcast message, all the devices present in broadcast domain have to pay attention to it.
This creates alot of congestion in network. (commonly called LAN congestion) which affects the bandwidth of the users present in that network.
From this we can realize that the more the number of collision domains and the more the number of broadcast domains, the more efficient is the network providing better bandwidth to all its users.

So which devices break CollisionDomain and which breaks Broadcast Domain

(i) HUB :-

- It neighter breaks the collisionDomain nor a Broadcast Domain i.e. a Hub is neither a collision domain separator nor a Broadcast Domain Separator. All devices connected to a hub are in a single collision and single broadcast domain. ~~Remains~~
Remember Hubs do not segments a network, they just connect network segments.

(ii) Switches :-

- Every port on a switch is in a different collision domain, i.e. a switch is a collision domain separator. So msg that comes from a devices connected to different port never experience a collision.
This helps us during designing networkes but there is still a problem with switches
- They never breaks a broadcast domain, it means it is not a broadcast domain Separator
- All the ports on the switches are still in a single broadcast domain. If a device sends a broadcast message it will still cause congestion

(iii) Routers :-

- Routers not only breaks collision domain but also breaks broadcast domain which means it is both broadcast as well as collision domain Separator
- A router creates a connection between two networks
  A broadcast message from one network will never reach the other one as the router will never let it pass.

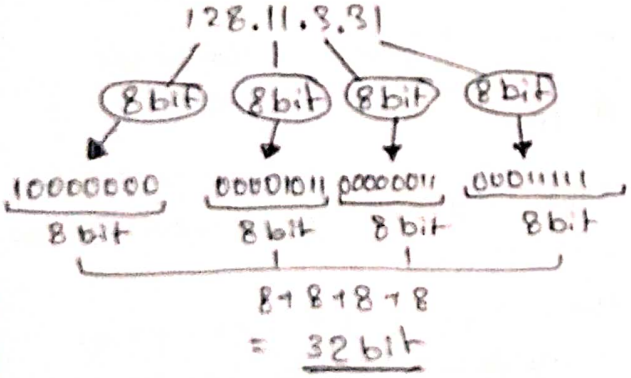
Also as repeaters and bridges differ from hubs and switches only in terms of the number of ports, a repeater does not breaks collision and broadcast domain while a bridge breaks only collision domain.

#Introduction of IP Addressing

■ Introduction :-

→ To communicate with each other within a network IP Addresses are used.
→ The participants in a network have their own unique addresses.
→ The Internet Protocol is responsible for allowing the IP address and subnet mask
→ The allocation of IP addresses is regulated by an international Organization i.e. Internet Corporation for Assigned Names and Numbers (ICANN).
  • ICANN is also responsible for allocation of DNS.
→ Certain IP address ranges are reserved for special purpose like range from 127.0.0.0 to 127.255.255.255. There is no reliable information on why that range was chosen.
→ IPv4 is a 32 bit (having 4 parts) unique address having an address space of 2^{32}.
→ Two notation in which IP address can be written.

① Dotted Decimal Notation :



② Hexadecimal Notation

8 bit	8 bit	8 bit	8 bit
01110101	00011101	10010101	11101010
75	1D	95	EA

0x751D95EA

Some points to be noted about Dotted Notation.

① The value of any segment (byte) is between 0 to 255 (both included)
② There are no zeroes preceding the value in any segment (i.e. 054 is wrong 54 is correct)

Types of IP address :-

1 IPv4 Address :-

→ 32 bit number with 4 words, each having 8-bit with value upto 255.
OR we can say IPv4 address has 4 octets of 8-bit with each number with a value upto 255.
→ IPv4 classes are differentiated based on the number of host it supports on the network.
→ Types of classes :-

IPv4 Class	IPv4 Start Address	IPv4 End Address	Usage.
A	0.0.0.0	127.255.255.255	Used for large Networks
B	128.0.0.0	191.255.255.255	Used for Medium Size Network
C	192.0.0.0	223.255.255.255	Used for Local Area Network
D	224.0.0.0	239.255.255.255	Reserved for Multicasting
E	240.0.0.0	255.255.255.255	Study & R&D

→ IPv4 uses a 32-bit address scheme to store 2^{32} address which is more than 4 billion address.
→ It is considered the Primary Internet Protocol and carries 94% of Internet Traffic.

2 IPv6 Address

→ IPv6 is the most recent version of Internet Protocol.
→ This new IP address version is being deployed to fulfil the need of for more Internet address.
→ IPv6 is a 128 bit, allowing 340 undecillion ($2^{128} \approx 3.4 \times 10^{38}$) unique address.

Features of IPv6 :

- Hierarchical addressing and routing ~~configuration~~ infrastructure.
- Stateful and stateless configuration.
- Support for Quality of Services (QoS).
- An ideal protocol for neighbouring node interaction.

Network transmission techniques :-

Circuit Switches vs Packet-Switch :-

→ In circuit switched network, a sig. single path is designated for transmission of all the data packets whereas in case of packet switched network, each packet may be sent through a different path to reach the destination.
In circuit switched network, the data packets are received in orders whereas in a packet switched network the data packet may be received out of order.
Packet-Switching is further divided into Virtual Circuit & Datagram.

■ IPv4 : IPv4 is a connectionless protocol used for packet-switched networks.

■ IPv4 Datagram Header : Size of the header is 20 to 60 bytes.

IPv4 Datagram fragmentation & Delay

Why IPv4 Datagram fragmentation required?

→ Different networks may have different Maximum Transmission Unit (MTU) for example due to difference in LAN technology. When one network wants to transmit datagrams to a network with smaller MTU, the router on path may fragment and reassemble datagrams.

How is fragmentation done?

→ When a packet is received at router, destination address and MTU is determined. If size of packet is bigger than MTU, and the 'Do not fragment' (DF) bit is set to 0 in header, then the packet is fragmented into parts and sent one by one. The maximum size of each fragment is the MTU minus the IP header size (IP Header size : min 20byte to max 60byte)

Each fragment is converted into a packet and the following changes happens in the datagram header.

(1.) The total length field is changed to the size of the fragmet.
(2.) The more fragment bit (MF bit) is set for all the fragment packets except the last one.
(3.) The fragment offset field is set, based on the number of fragment that is being set and the MTU.
(4.) Header Checksum is re-calculated.

Delays :

4 types of Delays happens :-

(1). Processing Delay : Time taken by the routers to process the data Packt head

(2). Queuing Delay : Time taken by the data packet in routing queues.

(3). Transmission Delay : Time taken to load a data packet onto the transmission channel.

(4). Propagation Delay : Time taken by the data packet to reach from source to destination.

Fragmentation at Network Layer

Fragmentation:

→ Fragmentation is done by the network layer when the maximum size of datagram is greater than the maximum size of data that can be held in a frame. i.e. MTU. The network layer divides the Datagram received from the Transport Layer into fragments so that data flow is not disrupted.

- Since there are 16 bits for total length in IP header, so max. size of IP datagram = $2^{16}-1 = 65535$ bytes
- It is done by network layer at the destination side and done at routers.
- Source side does not require fragmentation due to good segmentation by transport layer. i.e. instead of doing segmentation at transport layer and fragmentation at network layer, the transport layer looks at datagram data limit and frame data limit and does segmentation in such a way that resulting data can easily fit in a frame without need of fragmentation.
- Receiver identifies the frames with the identification (16 bits) field in the IP header. Each fragments of frame has the same identification number
- Receiver identifies the sequence of frame by fragment offset field in the IP header.
- Overhead at the network layer is present due to extra header introduced due to fragmentation.

Fields in IP header for fragmentation

① Identification (16 bits) - use to identify fragments of the same frame

② fragment offset (13 bits) - use to identify sequence of the fragments in frame

③ More Fragment (MF: 1 bit) - tells if more fragments are ahead of this
i.e. if MF = 1, more fragments are ahead of this fragment
if MF = 0, it is the last fragment.

④ Don't fragment (DF: 1 bit) :- if we don't want the packet to be fragmented then DF is set i.e. DF = 1.

Reassembly of fragments:

→ It takes place only at the destination and not at routers since packets take an independented path (datagram packet switching), so all may not meet at a router and hence a need of fragmentation arise again. The fragments may arrive out of order also.

Rules for Assigning Host ID & Network ID

1 Rules for Assigning Host ID :

→ ~~Host ID's are assigned within a network~~

→ Host ID's are used to identify a Host within a network. The following are the rules for Assigning Host ID.

- Within a network, the host ID must be unique to that network.
- Host ID in which all bits are set to 0 cannot be assigned because this ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this Host ID is now reserved as Broadcast address to send packets to all the Host present on that particular network.

2 Rules for Assigning Network ID :

→ Hosts that are located on the same ~~network~~ physical network are identified by network ID's, as all the Host on the same physical network are assigned the same network ID. The network ID is assigned on the basis of :-

- The network ID cannot starts with 127 because 127 ~~is reserved~~ belongs to class A address and is reserved for internal loop-back function.
- All bits of network ID set to 1 are reserved for IP Broadcasting therefore it cannot be used.

II IP Addressing / Classless Addressing :-

1 Network Address : It identifies a network on internet. Using this, we can find range of addresses in the network and total possible number of hosts in the network

2 mask : It is a 32-bit binary number that gives the network address in the address block when AND operation is bitwise applied on the mask and any IP address of the block.

The default mask in different classes are :-

Class A – 255.0.0.0 Class C – 255.255.255.0

Class B – 255.255.0.0

3 Subnetting : Dividing a large block of address into several contiguous ~~sub-blocks~~ sub-blocks and assigning these sub-blocks to different smaller networks is called Subnetting

4 Subnet mask : It is a 32 bit number used to differentiate the network component of an IP address by dividing the IP address into a network address and host address.

5 Classless Addressing

→ We use host ID-bits as net ID bits of a classful IP address. We give the IP address and define the no. of bits for mask along with it (followed by "/" symbol) like, 192.168.1.1/28. Here subnet mask is found by putting the given number of bits of out of 32 as 1

6 Default Gateway: It serves as an Access point or IP router that a networked computer used to send information to a computer in another network or over the internet.
The default simply means that it is used by default until an unless an application specifies another gateway. with without it, a network is isolated from outside.

7 Supernetting

→ It is the opposite of Subnetting. In subnetting a big network is divided into multiple smaller subnetworks. In subernetting multiple networks are combined into a bigger network termed as Supernetwork, or Supesnet.

Longest Prefix Matching in Routers :

1 Forwarding: Forwarding is moving incoming packets to the appropriate interface. Routes uses a forwarding to decide which incoming packets should be forwarded for the next hop.

2 IP Prefix: IP Prefix is ~~an IP~~ a prefix of IP address. All computers on one network have the same IP Prefix. For ex. 192.24.0.0/18, 18 is the length of the prefix and the prefix is the first 18 bits of the address.

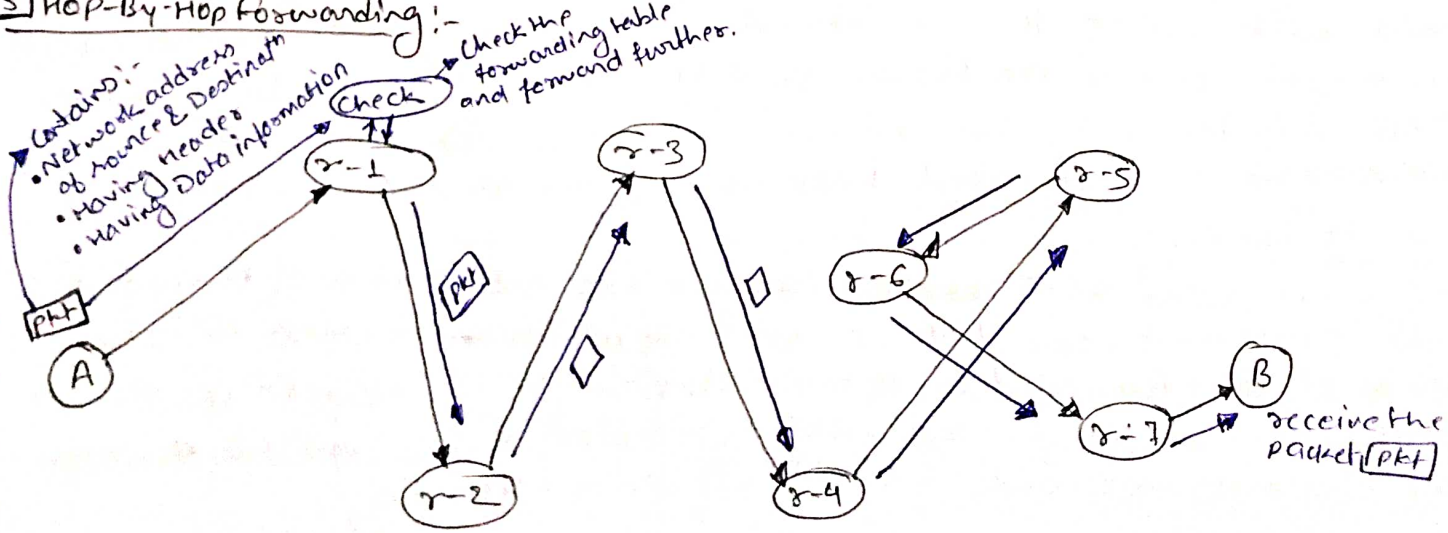
3 How does forwarding works?

→ Routers basically look at the destination address's IP prefix, searches the forwarding table for a match, and forward the packets to the corresponding next hop in the forwarding table.

4 What Happens if the Prefix Overlaps?

→ Since prefix might overlap (this is possible as classless Addressing is used everywhere) an incoming IP's prefix may match multiple IP entries in a table.

5 HOP-By-Hop Forwarding :-



Now what if someone adds a new routes in between this router network would that new router also be included in this or what really happends. Answer of this is that that new router also included in this routers networks. Now another question came up that is about forwarding table, How this new router will know about other Routers and destination.

Answer → Control Plane.

→ This Routes network can be visualize as a graph.

where,

Routers ⟶ Nodes

Links ⟶ Edges.

Types of Routing :-

→ Routing is a process that is performed by Network layer devices in order to deliver the packet by choosing an optimal path from one network to another.

There are 3 types of Routing :-

1. Static Routing
2. Default Routing
3. Dynamic Routing.

1 Static Routing :-

→ Static Routing is a process in which we have to manually add routes to the routing table.

Advantages :-

- No routing overhead for router CPU which means a cheaper router can be used to do routing.
- It adds security because only the administrator can allow routing to particular networks only.
- No bandwidth usage between routers.

Disadvantages :-

- For Large Network it is a hectic task for the administrator to manually add each route for the network in the routing table on each router.
- The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have a very good knowledge of the routes of the topology.

2 Default Routing :-

→ This is a method where router is configured to send all packets towards a single router (next hop). It doesn't matter to which network the packets belongs to, it is forwarded out to the router which is configured for default routing. It is generally used with Stub router. A Stub router is a router that has only one route to reach all other networks.

3 Dynamic Routing :-

→ Dynamic Routing makes adjustments of the routes according to the current state of the route in the routing table. Dynamic Routing uses protocols to discover network destinations and the routes to reach them. R.I.P (Routing Information Protocol) and OSPF (Open Shortest Path First) are the protocols used in Dynamic Routing

Features :-

- The routers should have the same dynamic protocol running in order to exchange routes.
- When a router finds a change in the topology then the router advertises it all to all other routers.

Advantages :-

- Easy to configure.
- More effective at selecting the best route to the destination remote network and also for ~~discovering~~ discovering remote network.

Disadvantages

- Consumes more bandwidth for communicating with other neighbours.
- Less secure than static Routing.

Middle Box

1 NAT (Network Address Translation)

→ Network Address Translation is a process in which one or more local IP address is translated to one or more global IP address and vice versa in order to provide Internet access to local host. Also it does the translation of port numbers. i.e. masks the port number of host with another port number, in the packet ~~that~~ that will be routed to the destination. It then makes the ~~corresponding~~ corresponding entries of IP address and port number in the NAT table. NAT generally ~~work~~ operates on a router or firewall.

To access the internet, one public IP address is needed, we can only use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the internet through a single public address. To achieve this, the translation of a private IP address to a Public IP address is requir. which can be done by NAT.

Working :-

→ Generally, the border router is configured for NAT i.e. the router which has one interface in local (inside) network and one interface in the global (outside) network when a packet traverse outside the local (inside) Network, then NAT converts the the ~~local (inside)~~ local (Private) IP address to a global (public) IP address. when a packet enters the local network, the global (Public) IP address is converted to a local (private) IP address.

If NAT runs out of addresses. i.e. no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

Types of NAT

1. Static NAT: In this, single private IP address is mapped with a single public IP address. It used in web hosting.
2. Dynamic NAT: In this, multiple private IP addresses are mapped to a pool of public IP address. It is used when we know the number of fixed users who want to access the internet at a given point of time.
3. Port Address Translation (PAT): In this, many local (Private) IP address are mapped or translated to a single public IP address. Port numbers are used to distinguish the traffic. This is the most frequently used one.

How NAT protects us

- It hides the IP address of any device on your network from the outside world giving them all a single address.
- It requires every incoming packet of information to have been asked by a device. If a malicious data packet isn't on the list of expected communications it gets rejected.
- Some firewalls can be whitelisting to block unauthorized outgoing traffic so that if you do contract a piece of malware your firewall may prevent it from communicating with your device.

2) Firewall

- The firewall is a network security system that is used to monitor the incoming and outgoing traffic and blocks the same based on the firewall securities policies.

It acts as a wall between the internet (public network) and the networking devices (a private network). It is either a hardware device, software programs or a combination of both, It adds a layer of security to the network.

#Internet Control Message Protocol (ICMP)

- Since IP does not have an built-in mechanism for sending errors and control message. It depends on ICMP to provide an error control.

It is used for reporting errors and management queries. It is a supporting protocol and is used by network devices like routers for sending errors messages and operations information, e.g. the requested service is not available or that a host or router could not be reached.

Hot Standby Router Protocol (HSRP)

- It is a CISCO proprietary protocol, which provides redundancy for a local subnet. In HSRP, two or more routers gives an illusion of a virtual Router. HSRP allows you to configure two or more routers as standby routers and only a single act as an active router at a time. All the routers in single HSRP group shares a single MAC address and IP address, which acts as a default gateway to the local network. The active router is responsible for forwarding the traffic. If it fails, the Standby router takes up all the responsibilities of the active router and forwards the traffic.

Distance Vector Routing (DVR) Protocol :

→ A Distance vector Routing (DVR) protocol requires that a routes inform its neighbours of topology changes periodically. Historically known as old ARPANET routing ~~protocol~~ algorithm (or known as Bellman-ford algorithm)

■ Bellman-ford Basics : Each router maintains a Distance vector table containing the distance between itself and all possible destination nodes. Distances based on chosen matrix. are computed using information from the neighbours distance vector.

Open Shortest Path First (OSPF) Protocol

→ OSPF Protocol is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First (SPF) algorithm.

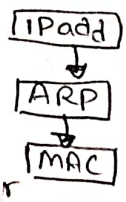
A link-State-Routing protocol is a protocol that uses the concept of triggered updates i.e. If there is a changes observed in the learned routing table then the updates are triggered only. not like the distance-vector routing protocol where the routing table is exchanged at a period of time.

ARP and how it works

■ Address Resolution Protocol : ARP is a communication protocol used for discovering physical address associated with given network address. Typically, ARP is a network layer to data link layer mapped process, which is used to discover MAC address for given Internet Protocol Address

■ Working :

most of the computer application/programs uses IPaddress to send/receive messages, however, the actual communication happens over the physical add. (MAC Address). So our mission is to get the destination MAC address which helps in communicating with other devices. This is where ARP comes in to picture, its functionality is to translate IP address to MAC address.



Now,

Imagine ~~that~~ a device wants to communicate ~~over~~ with other device over the internet what ARP does?

The devices of the network peel the header of the data link layer from the PDU alsocalled as frame and trasfer the packet to network layer. where the network ID of packet is validated with destination IP's network ID of the packet and if it is equals then it responds to the source with the MAC address of the destination, else, the packet reaches the gateway of the network and broadcasts the packet to the devices it is connected with and validates their network ID.

The above process continues till the second last network device in the path reaches the destination where it gets validated and ARP, in turn, responds with the MAC address of destination.

Packet flow in the Same Network :-

→ To transfer a packet from source to destination, both the IP address and MAC address of destination should be known. If the destination MAC address is not present then ARP will resolve this issue first then the packet will be delivered to the destination host.

There are simple rules for packet flow in a Network :

① If the destination host is present in the same network as the source host then the packet will be delivered directly to the destination host using MAC address.

② Within a network the packet will be delivered on the basis of MAC address

③ MAC address never crosses its broadcast domain.

Packet Flows in Different Network :-

→ To deliver the packet to destination host the source IP, destination IP, source MAC address, destination MAC address should be known,

Some basic rules for packet to flow :-

① If the destination host is present in same network, packet will be directly delivered.

② If the destination host is present in different network then the packet is delivered to the default gateway first which in turn delivers the packet to the destination host.

③ If ARP is not resolve then ARP will Resolve first.

④ MAC address never crosses its broadcast domain.

Layer-2 Switches v/s Layer-3 Switches

Switch :- A switch is a device which sends a data packet in a local Network

Now, what its advantage over Hub?

→ A Hub floods the network with the packets and only destination system receives that packet while others just drop, due to which the traffic increases a lot. To solve this problem switches come into picture.

A Switches first learns, by flooding network just like hub to fill MAC-address table, on which port a particular device is connected. After learning it sends packet to that particular host only.

Layer-2 switches works on Layer-2 (Data Link layer) and sends 'frames' to destination ports using MAC address table which stores the MAC address of a device associated with that port.

Layer-3 Switches works on Layer-3 (Network layer) where it route packet by using IP address, used widely on VLANs

Difference between Ping and Traceroute.

Need ?

→ In computer networks, data is sent as packets (PDU). Each packet is transmitted individually and may also follow a different route to reach the destination. Once all packets of original ~~packets were~~ message reaches the destination they are re-assembled to form the original message But sometimes, it may happen that the web server is down, network congestion, or some other technical glich is there, that may prevent the message from reaching the destination. To diagnose such congestions and network failure, we use two programs that are Ping & Traceroute.

1 Ping :-

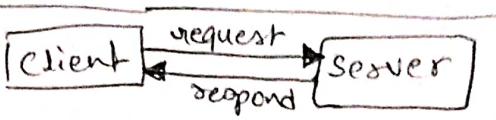
→ Ping is a utility that helps one to check if a particular IP address is accessable or not. Ping works by sending a packet to the specified address and waits for the reply.
It also measures round trip time and reports errors.
Ping is also used in checking if the computers on a local network are active For this, In cmd, type : ping 127.0.0.1.
The IP address 127.0.0.1 is the address of the local host and would receive a ping reply even if the sender is not connected to the internet.

2 Traceroute :-

→ It is a utility that traces a packet from your computer to the host, and will also show the number of steps (hops) required to reach there, along with the time by each step.
Traceroute works by sending the packets of data with low survival time (Time to Live - TTL) which specifies how many steps (hops) can a packet survive before it is returned. when a packet can't reach the final destination and expire at intermediate step, that node returns a packet id and identifies itself. So by increasing the TTL gradually, Traceroute is able to identify the intermediate hops. If any of the hops come back with request "Request Timed Out", it denotes network congestion and a reason for slow loading web pages. and dropped connections.

The main difference between Ping and Traceroute is that, Ping is a quick and easy utility to tell if a specified server is reachable and how long will it take to send and receive data from the server whereas Traceroute finds the exact route taken to reach the server and time taken by each step (hop)

Servers in Computer Network :



- A server is a computer program or a device that provides functionality for clients which are other programs or devices. This architecture is called the client-server model.
- A single overall computation is distributed across multiple process or devices.
- Servers can provide various functionalities called services like, sharing data or resources among multiple devices/clients or performing computation for clients.
- Multiple clients can served by a single server, and a single client can use multiple servers.
- A client process may run on the same device, It can also connect over a network to a server to run on a different device.

Ex: Web servers, Mail servers, game servers, database servers, file servers, Application servers etc.

Types of Servers and their Applications :-

1 Application Server :

- These servers hosts web apps (computer programs that run inside a web browser) allowing the users in the network to run and use them preventing the installing a copy of on their own computers.
- These servers need not be part of the World Wide Web
- Their clients are computers with web browser

2 Catalog Server :

- These servers maintains an index or table of contents of information that can be found across a large distributed network. Distributed Network may include computers, users, files shared on file servers and web apps. Example of Catelog Servers are Directory servers and name servers.
- Their clients are any computer program that needs to find something on the network. Example can be domain member attempting to log in, an email client looking for an email address, or a user looking for a file.

3 Communication Servers :

- These servers maintains an environment needed for one communication endpoint to find other endpoints and then communicates with them. These servers may or maynot include a directory of communication endpoints and a presence of detection service, depending on the openness and security parameters of the network. Their clients are communication endpoints.

4 Computing Servers :

- These servers share vast amounts of computing resources which included CPU and RAM over a network. Any computer program that needs more CPU power and RAM than a personal computer can probably afford and can use these type of servers.
- The Client must now be a networked computer to implement the client-server model which is necessity.

5. Database Server :
→ These servers maintains and shares any form of database over a network. A database is a organized collection of data with predefined properties that may be displayed in a table. • Clients of these servers are Spreadsheets; accounting software, asset management software or virtually any computer program that consumes well-organized data, especially in large volumes.

6. Fax server :
→ These servers share one or more fax machines over a network which eliminates the hassle of physical access. ~~Any~~
• Any fax sender or recipient are the clients of these servers.

7. File Server :
→ Shares files and folders, storage space to hold files and folders, or both over a network
• Networked computers are the intended clients, even though local programs can be clients.

8. Game Servers :
→ These servers enables several computers or gaming devices to play multiplayer games.
• Personal computer or gaming consoles are their clients.

9. Mail Servers :
→ These servers makes email communication possible in the same way as a post office makes snail mail communication possible.
• Clients of these servers are sender & receiver of mails (e-mails)

10. Print Servers :
→ These servers shares one or more printers over a network which eliminates the hassle of physical access.
• Clients are computers in need of printing something.

11. Proxy Servers :
→ This acts as an intermediary between clients and a server accepting incoming traffic from the client and send it to the server
Reason to use proxy server includes content control and filtering, improving traffic performance, preventing unauthorized network access or simply routing the traffic over a large and complex network.
• These clients are any networked computer

12. Web-Servers :
→ These servers hosts web pages. A web servers is responsible for making the world wide web possible. Each website has one or more web servers.
• These clients are computers with web browser.

Port No.: 16 bit
MAC Add: 48 bit
IP add: 32 bit

4. Transport Layer

Transport Layer :

- Transport Layer is the ~~second~~ fourth layer of TCP/IP model.
- It is an end-to-end layer used to delives messages to a host. It termed as an end-to-end layer because it ~~provides a point-poi~~ provides a point-to-point conection rather than a hop-to-hop between the source host to destination.
- Unit of ~~dat~~ PDU in the Transport Layer is a segment.
- Standard protocols used in Transport layer is TCP, UDP, DCCP, etc.

■ Responsibilities of Transport Layer :

- **Process to process delivery**: Data link layer requires MAC address of source-destination hosts to deliver a frame, Network layer requires IP address for appropriate routing of packets, Transport Layer requires a Port number to correctly deliver the segments of data to a correct process amongst the multiple processes running on a particular hosts.

  Port Number :- It is a 16 bit address used to identify client-Server program uniquely
- **End-To-End Connection**: The Transport Layer is also responsible for end-to-end communication between hosts, mainly uses TCP and UDP.

  TCP: It is a secure, connection-oriented protocol that uses a handshake protocol to establish a robust connection between two end hosts. It ensures reliable delivery of messages

  UDP: It is a stateless and unreliable protocol that ensures best delivery It is suitable for the application that have no much concern with flow or error control and requires sending the bulk of data like video conferencing. It is often used in multicasting protocol.
- **Multiplexing and Demultiplexing**:

  Multiplexing : multiplexing allows simultaneous use of different applications over a network that is running on a host. The transport layer provide us this mechanism to send packet streams from various application simultaneously over network Transport layer accept these packets from different processes differentiated by their port number and passes them to network layer after adding proper header.

  Demultiplexing : It is required at receiver side to obtain the data coming from various processes. Transport receives the segments of data from the network layer and delivers it to the appropriate process running on the received machine.

- **Congestion Control**

Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occure. As a result retransmission of packets from sources increases the congestion further
In this situation, the transport layer provides Congestion Control in different ways: It uses Open LOOP Congestion control to prevent congestion and closed loop congestion to remove the congestion.
TCP provides Leaky bucket technique for congestion control.

- **Data Integrity and Errors correction:**

Transport layer checks for the Errors in the messages coming from the application layer by using Error detection codes, computing checksums. It checks whether the received data is not corrupted and uses the ACK and NACK services to inform the sender if the data has arrived or not checks for the integrity of data.

- **Flow Control:**

Transport layer provides the flow control mechanism between different layers of TCP/IP model.

Congestion Control in Computer Networks:

Congestion:

→ A state occurs in the network layer when the ~~too~~ message traffic is so heavy that it slows down network response time.

Congestion causes choking of the communication medium. when too many packets are displayed in a method of subnet, subnet's performance degraded. Hence., a network's communication channel is called congested if packets are traversing the path and experience delays mainly over the path's propagation delay.

One of the main cause of congestion is that traffic is often bursty.

Traffic Shaping: It is a mechanism to control the amount and the rate of the traffic sent to the network. Approach of congestion control management is called Traffic Shapping.

Two types of Congestion Control or Traffic Shaping:

1. Leaky Bucket
2. Tooken Bucket.

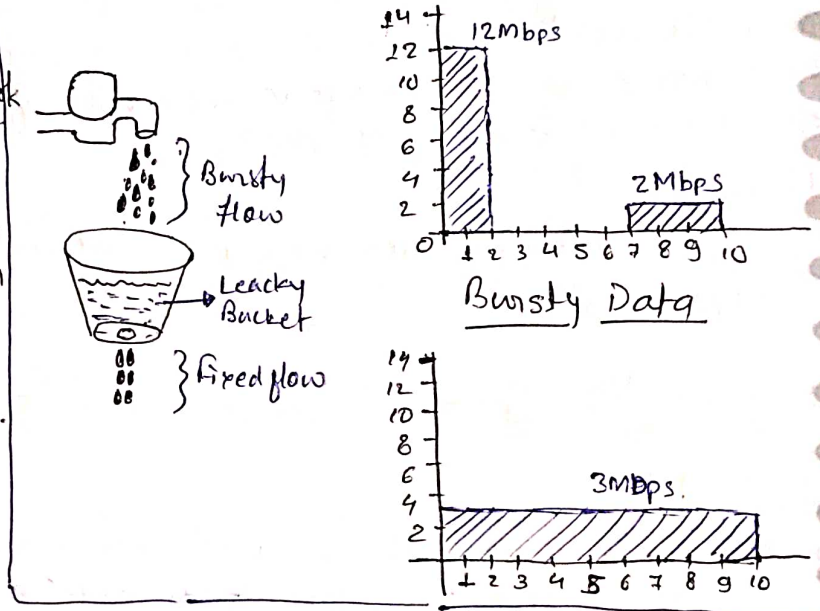
1] Leaky Bucket:

→ This algorithm allows controlling the rate at which a record is injected into a network and manages boustiness in the data rate.

Explanation:-

Suppose we have a bucket in which we are pouring water in a random order but we have to get water in fixed rate, for this we will make a hole at the bottom of the bucket, It will ensure that the water coming out is in fixed rate also if bucket will fill we will stop paring in it.

The input rate can vary but the output rate remains constant, similarly in networking, Leacky Bucket technique smooth the ~~bs~~ bursty traffic. Bursty traffic chunks are stored in Bucket and ~~set~~ sent out with an average rate.



In the fig. we assume that the network has committed a bandwith of 3 Mbps for a host.

The use of the Leaky Bucket shapes the input traffic to make it conform to this commitment.

In fig. the host sends a burst of data at a rate of 12Mbps for 2sec. (total of 24Mbits). Then the host is silent for 5 sec. and then sends data at the rate of 2Mbps for 3 sec. (6 Mbits of data). In all, the hosts sends total of 30 Mbits of data for 10sec. The leacky Bucket smooths the traffic by sending out data at a rate of 3Mbits for 10sec.

- Without the Leacky Bucket, the beginning burst may hurt the network by consuming more bandwidth than is set aside for this host. So in this way congestion is prevented.

2] Token Bucket Algorithm:

→ It is a control algorithm that indicates when traffic should be sent, This order comes based on the display of tokens in the bucket. The Bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the Bucket are deleted for the ability to share a packet.

When tokens are shown, a flow to transmit traffic appears in the display of tokens. No tokens means no flow sends its packets. Hence a flow transfers traffic upto its peak burst rate in good tokens in the bucket.

- Thus, the token bucket algorithm adds a token to the bucket each 1/r seconds, The volumn of bucket is b-tokens. when a token is appears, and the bucket is complete, token is discarded. If a packet of n bytes appears and n tokens are deleted from the bucket. the packet is forwarded to the network.

When a packet of n bytes appears but fewer than n tokens are available, No tokens are removed from the bucket in such a case, and the packet is considered non-conformant. The non-conformant packets can be either dropped or queued for next transmission when sufficient tokens have accumulated in the bucket.

■ Need of Token Bucket Algorithm:

• The leaky bucket Algorithm enforces output patterns at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic, we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Some Advantages of Token Bucket over Leaky Bucket:

• If bucket is full in Token Bucket, the tokens are discarded not packets, while in leaky Bucket, packets are discarded.

• Token Bucket can send large bursts at a faster rate while leaky Bucket always send a packet at constant rate.

Transmission Control Protocol (TCP)

→ The Transmission Control Protocol is the most common transport layer protocol. It works together with IP and provides a reliable transport service between processes using the network layer service.

1 Services and Segment Structure in TCP

(1) Process-to-Process Communication:

- The TCP provides Process-To-Process communication i.e. transfer of data that takes place between individual processes executing on end systems. This is done using port numbers.

(2) Stream Oriented:

- This means that the data is sent and received as a stream of bytes (unlike UDP or IP that divides the bits into datagram or packets)

(3) Full duplex service:

- This means that the communication can take place in both direction at a same time

(4) Connection-Oriented Service:

- Unlike UDP, TCP provides a connection oriented service, which has 3 phases:
  - Connection Establishment
  - Data transfer
  - connection terminated.

(5) Reliability:

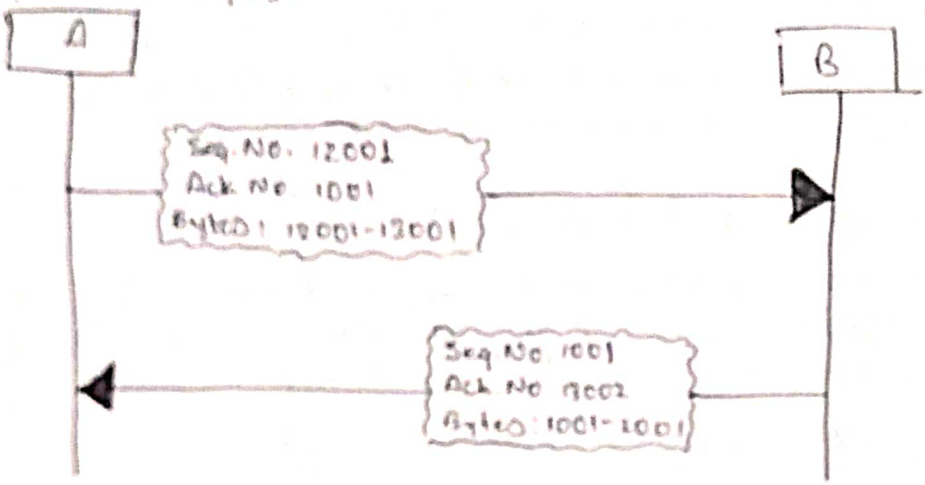
- TCP is reliable as it uses checksum for error detection, attempts to recover lost or also corrupted packets by re-transmission, acknowledgement policy and timers. Uses features like byte number, sequence number and acknowledgment number to ensure reliability. Also it uses congestion control mechanism.

(6) Multiplexing

- TCP does multiplexing and demultiplexing at the sender and receiver ends also as a number of logical connections can be established between port numbers over a physical connection.

Byte Numbers, Sequence Numbers and Acknowledgement Numbers:

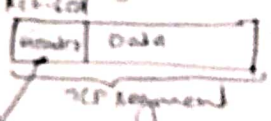
- Sequence numbers are given to segments so at receiver end they can be reassembled if they arrive in different orders. The sequence number of a segment is the byte number of first byte that is being sent.
- The Acknowledgement number is required since TCP provides full-duplex service. The acknowledgment number is the next byte number that the receiver expects to receive which also provides acknowledgement for receiving the previous bytes.



TCP segment Structure

- A TCP segment consist of a data and a header that is added by TCP to data segment.

The header of TCP segment can range from 20-60 bytes



Header fields:

- Source Port Address: 16-bit field that holds the port add of application that is sending the data segment.
- Destination Port Address: 16-bit field that holds the port add of destination that is receiving receiving segments.
- Sequence number: 32 bit field that holds Seq number
- Acknowledgement number: 32 bit field that hold Ack No.
- Header Length (HLEN): 4-bit field, that indicates the length of Header.
- Control flag: These are 6 bit control bits that controls connection establish connection termination, flow control, mode of transfer etc.
- Window Size: This bit field tells the window size of sending TCP in bytes.
- Checksum: This field hold checksums for error control
- Urgent Pointer: This field is used to point to data that is urgently required that needs to reach the receiving process at the earliest.

containing:
- Source & Destination port No
- Seq & Ack number
- Reserve bits
- Window Size, HLEN
- etc

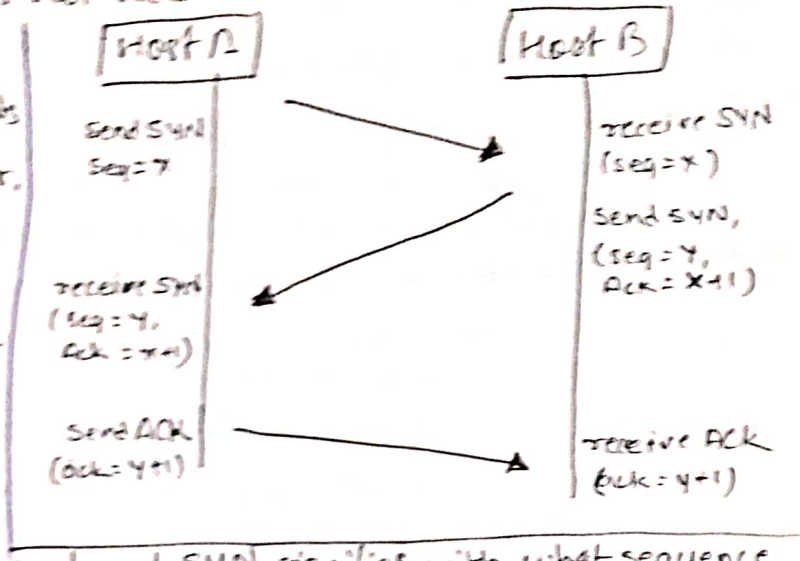
TCP connection:

- TCP is a connection oriented. A TCP connection is established by 3 way-hand shake.

2 TCP - 3 Way Handshake Process:

- From application layer, info is transferred to the Transport layer where TCP comes into picture. Two imp protocol of Transport layer are TCP & UDP out of which TCP is prevalent (as it provides reliability for connection establishment)
- TCP provides reliable communication with PAR (Positive Acknowledgement Retransmission) PDU of transport layer is segment
- How a device using PAR, resend the data unit until it receives an acknowledgement. If the data unit is received at the receiver's end is damaged (it checks the data with checksum functionality of transport layer that is used for error detection), then the receiver discards the segment & the sender has to resend the data unit for which positive acknowledgement is not received.

How it works:



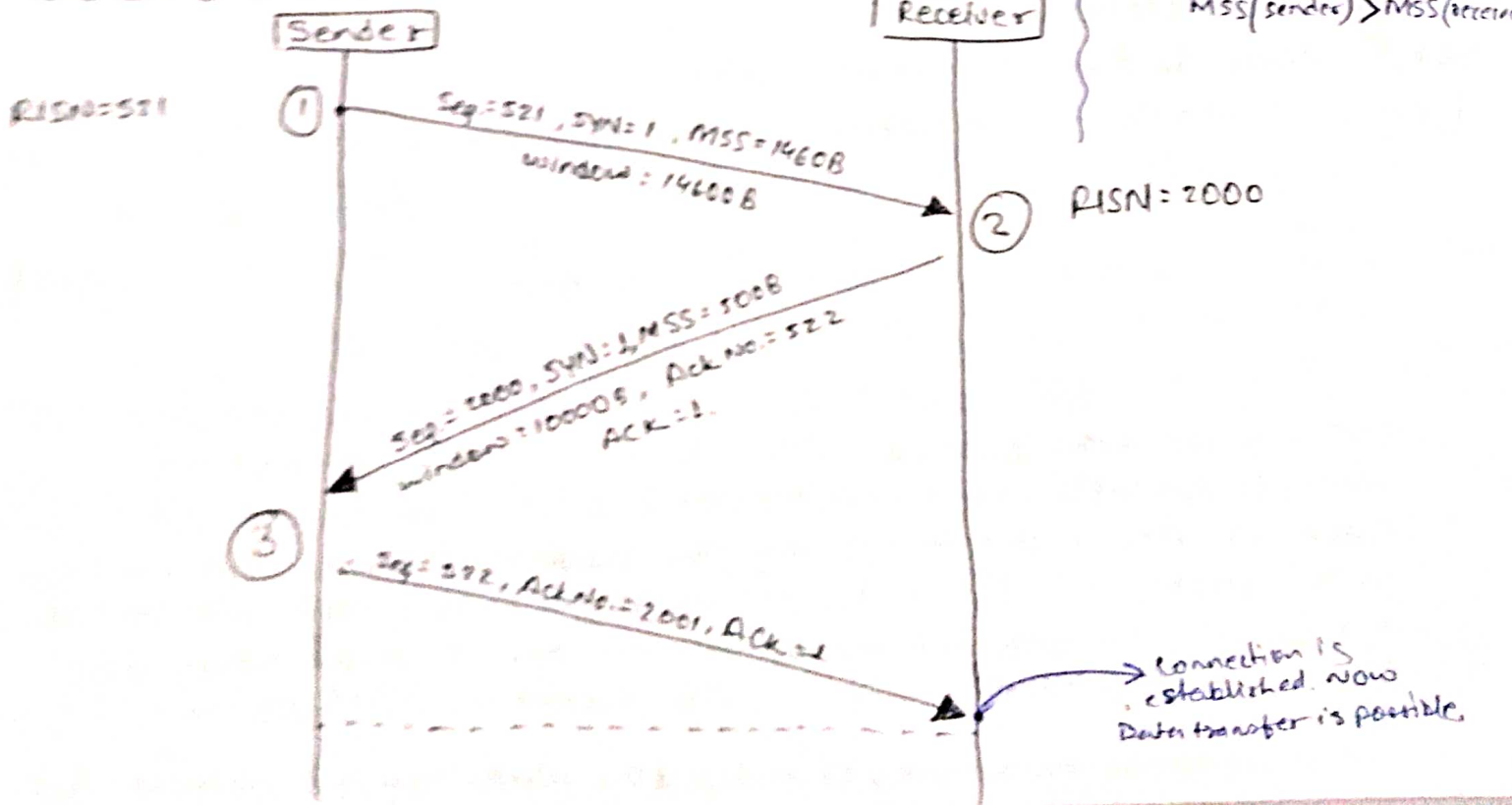
Step 1 : SYN : In first step, client wants to establish a connection with a server, so it sends a segment with SYN (Synchronize Sequence No.) which informs the server that the client is likely to start communication and with what sequence number it starts segments with.

Step 2 : (SYN + ACK) : Server responds to the client request with SYN + ACK. Acknowledgement number (Ack) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segment with.

Step 3 : ACK : In the final part client Acknowledges the response of the Server and they both establish a reliable connection with which they will start the actual data transfer.

Connection Establishment:

RISN : Random Initial Sequence Number
MSS : Maximum Segment Size
MSS(sender) > MSS(receiver)



TCP Connection Termination :

→ TCP supports two types of connection release :

① Graceful Connection Release : In this, the connection is open until both parties have closed their sides of connection.

② Abrupt connection Release : In this, either one entity is forced to close the connection or one user closes both directions of data Transfer.

3 Error Control in TCP :

- TCP protocol has methods for finding out ~~cour~~ corrupted segments, missing segments, out-of-order segments and duplicate segments.

Error Control in TCP is mainly done by the use of three simple techniques :-

① Checksum : Every segment contains a checksum field which is used to find corrupted segments. If the segment is corrupted, then that segment is discarded by the destination TCP and is considered as Lost.

② Acknowledgement : It is used to affirm that the data segments have been delivered. Control segments that contain no data but have seq. number will be acknowledged as well but ACK segments are not acknowledged.

③ Retransmission : When a segment is missing, delayed to deliver to a receiver, or is corrupted when it is checked by receiver then that segment is retransmitted again.

segments are retransmitted only during two events :

- when the sender receives three duplicate acknowledgements (ACK)
- when a retransmission timer expires.

4 TCP - Timer :

- TCP uses several Timers to ensure that excessive delays are not encountered during communications.

TCP implementation uses four Timers :

① Retransmission Timer : To retransmit lost segments, TCP uses Retransmission Timeout (RTO). When TCP sends a segment, the timer starts and stops when the acknowledgement is received. If the timer expires timeout occurs and the segment is retransmitted.

Retransmission Time Out is for 1 Round Trip Time (RTT).

② Persistent Timer : To deal with a zero-window-size deadlock situation, TCP uses a persistence timer. When the sending TCP receives an acknowledgment with a window size of zero, it starts a persistance Timer. When persistence timer goes off, the sending TCP sends a special segment called probe. This segment contains only 1 byte of new data. It has a sequence number, but its sequence number is never acknowledged. It is even ignored in calculating the sequence number for the rest of the data.

The probe causes the receiving TCP to resent the acknowledgment which was lost.

③ Keep Alive Timer: A keep Alive Timer is used to prevent a long idle connection between two TCP's. If a client opens a TCP connection to a server, transfers some data and become silent, the client will crash. In this case the connection remains open forever. So a keep Alive Timer is used. Each time the server hears from a client, it resets this Timer. The Timeout is usually 2 hours. If the server does not does not hear from the client after 2 hours, it sends a probe segment. If there is no response after 10 probes, each of which is 75 sec apart, it assumes that the client is down and terminates the connection.

④ Time Wait Timer: This timer is used during TCP connection Termination. The timer starts after sending the last Ack for 2nd FIN and closing the connection.

5 TCP Flags:

- Flags are used to indicates a particular state of connection or to provide some addition information like troubleshooting or to handle control etc most commonly used flags are SYN, ACK, FIN.
Each flag corresponds to 1 bit information.

Types of Flag:

① Synchronization (SYN): It is used in first step of connection establishment or 3-way handshake process between two hosts.
Only first packet from sender as well as receiver should have this flag
This is used for synchronizing sequence numbers i.e. to tell the other end which sequence number they should accept.

② Acknowledgement (ACK): It is used to acknowledge packets which are successful received by the host. The flag is set if the acknowledgement number filld contains a valid acknowledgement number.

③ Finish (FIN): It is used to request for connection termination i.e. when there is no more data from the sender, it requests for connection termination. This is the last packet sent by sender. It frees the reserved resources and gracefully terminate the connection.

④ Reset (RST): It is used to terminate the connection if the sender feels something is wrong with the TCP connection or that the conversation should not exist. It can get send from receiver side when packet is send to particular host that was not expecting it.

⑤ Urgent (URG): Data inside a segment with URG=1 flag is forwarded to applicat^{n} layer immediately even if there are more data to be given to app. layer. It is used to notify the receiver to process the urgent packets before processing all other packets.

⑥ Push (PSH): In general, it tells the receiver to process these packets as they are received instead of buffering them.

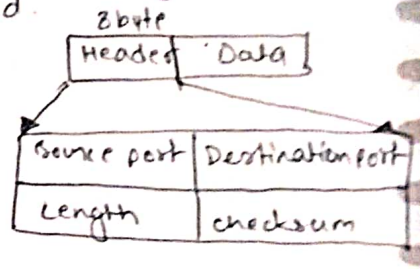
UDP (User Datagram Protocol):

→ User Datagram Protocol (UDP) is a Transport layer protocol
→ Unlike TCP, it is an unreliable and connection less protocol. So there is no need to establish a connection prior to data transfer.

Though TCP is a dominant transport layer protocol used with most of Internet services, provides assured delivery, reliability etc but all these services cost us additional overhead and latency. Therefore it is slower in some cases where UDP comes into pit picture. For real time services like gaming, voice or video communication, live conferences, we need UDP.
Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets.
There is no error checking in UDP, so it also saves bandwidth.
UDP is more efficient in terms of both latency and bandwidth.

UDP header:

→ UDP header is an 8-bytes fixed & simple header, Unlike TCP, which vary from 20 to 60 bytes.
→ The first 8 bytes contains all the necessary information (in header) and remaining part contains data.
→ UDP port number fields are each 16 bits long, therefore the range for port number is defined from 0 to 65535, port number 0 is reserved.



Important fields in UDP Header:

① Source Port: It is a 2 Byte long field, used to identify the port number of source.
② Destination Port: It is a 2 byte long field, used to identify the port number of Destination.
③ Length: Length is a length of UDP including header and the data. It is a 16 bits field.
④ Checksum: It is a 2 Bytes long field, used for error detection.

NOTE: Unlike TCP, the checksum calculation is not mandatory in UDP. No error control or flow control is provided by UDP. Hence UDP depends on IP and ICMP for error reporting.

Applications of UDP:-

→ Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control
→ It is a suitable for multicasting as UDP supports packet switching.
→ UDP takes a datagram from network layer, attaches its header and sends it to the user, so it works fast.
→ Normally used for real-time applications which can not tolerate uneven delays between sections of a received message.
→ UDP is used in transport layer, Application layer can do some task through UDP, UDP is also used for some routing update protocols like RIP (Routing Information protocol).

5. Application Layer

→ The application layer is present at the top of OSI model. It is the layer through which users interact. It provides services to the user. Uses web applications or internet application or network application.

Protocols in Application Layer

[1] HTTP

→ The HyperText Transfer Protocol (HTTP) is an application layer protocol that uses TCP as an underlying transport and typically runs on port 80.
HTTP is a stateless protocol i.e. server maintains no information about past client requests.

[2] TELNET :

→ TELNET stands for the TELetype NETwork. It help in terminal emulation
It allows Telnet clients to access the resources of the Telnet Server.
It is used for managing files on the internet. It is used for the initial setup of devices like switches.
The telnet command is a command that uses the Telnet protocol to communicate with a remote device.
Port number of Telnet is 23.

command :

telnet [\\RemoteServer],

\\RemoteServer : Specifies the name of the server to which you want to connect

[3] FTP

→ It stands for File Transfer Protocol. It is the protocol that actually lets us transfer files,
FTP is not just a protocol but is also a program.
Port number of FTP is 20 for data and 21 for control.

command :

ftp machinename,

[4] TFTP

→ Stands for Trivial File Transfer Protocol. It is the stripped-down, stock version of FTP, but its the protocol of choice if you know exactly what you want and where to find it.
Its a technology for transferring files between network devices and is a simplified version of FTP
Port number of TFTP is 69.

command

tftp [options...] [host [port]] [-c command]

5 NFS :

→ Stands for Network File System. It allows remote hosts to mount files over a network and interact with those file systems as though they are mounted locally.
This enables system administrators to consolidate resources onto centralized servers on the network
Port number for the NFS is 2049.

Command

service nfs start

6 SMTP

→ Stands for Simple Mail Transfer Protocol. It is the part of the TCP/IP protocal. Using a process called "Store and forward", SMTP moves your email on and across networks.
It works closely with MTA (Mail Transfer Agent) to send your communication to the right computer and email inbox.
The port Number of SMTP is 25.

Command

MAIL FROM: <mail@abc.com?

7 LPD

→ Stands for Line Printer Daemon. It is designed for printer sharing. It is the part that receives and processes the request. A 'daemon' is a server or agent
Port number of LPD is 515.

8 X window :

→ It defines a protocol for the writing of graphical user Interface-based client/server applications.
The idea is to allow a program called a client, to run on one computer.
It is primarily used in interconnected mainframes.
Port No. for x window starts from 6000 and inc. by 1 for each server.

command

Run xdm in runlevel 5

9 SNMP :

→ Stands for Simple Network Management Protocol. It gathers the data by polling the devices on the network from a management stations at fixed or random intervals, requiring them to disclose certain information.
It is a way that servers can share information about their current state, and also a channel through which an administrate can modify pre-defines values.
Port no. of SNMP is 161 (for TCP) and 162 (for UDP)

commands

snmpget -mALL -v1 -cpublic snmp_agent_ip.Address sysName.0

10 DNS

→ Stands for Domain Name System. DNS service translate the domain name into corresponding IP address.
For example domain name www.abc.com might translate to 198.105.232.4
Port No. of DNS is 53.

command

ipconfig /flushdns

11 DHCP :

→ It stands for Dynamic Host Configuration Protocol (DHCP). It gives IP addresses to hosts. There is a lot of information a DHCP server can provide to a host when the host is registering for an IP address with the DHCP server.
Port number of DHCP is 67, 68.

command

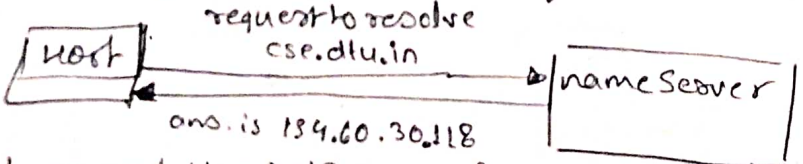
clear ip dhcp binding { address | * }

Domain Name System (DNS)

→ DNS is a host name to IP address translation service. It is an application layer protocol for message exchange between clients & servers.
There is not only one DNS server, There are series of DNS servers used to resolve the domain name. DNS uses cache to work efficently so that it can quickly refer to DNS lookups its already performed rather than performing a DNS lookup over and over again.
Although DNS caching increase the speed of domain name resolution process But the major change in the domain then takes a day to reflect world wide.

Imp Terms

- DNS record : Domain name, ip address, what is the validity? what is time to live ? and all the info related to domain name, These records are used to store them.
- Namespace : set of possible names, flat or hierarchical. Naming System maintains a collection of bindings of names to values. - given a name, a resolution mechanism returns the corresponding value.
- Name Server : It is an implementation of the resolution mechanism.



The Host request the DNS name Server to resolve the domain name. And the name server returns the ip address corresponding to that domain name to the host so that the host can further connect to ip address.

Hierarchy of Name Servers:

- **Root Name Server:** It is contacted by name servers that cannot resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and return the IP address to the host.
- **Top Level Servers:** It is responsible for .com, .org, .edu etc and all top level country domains like .uk, .fr, .ca, .in etc.
  They have info about authoritative domain servers and known names and IP addresses of each authoritative name servers for the second level domai
- **Authoritative name Server:** This is organizations DNS server, providing authoritative hostName to IP mapping for organization servers. It can maintained by organizations or service provider.

For example, In order to reach cse.dtu.in we have to ask the root DNS server. then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritati domain server will return the associative ip address.

Address Resolution in DNS

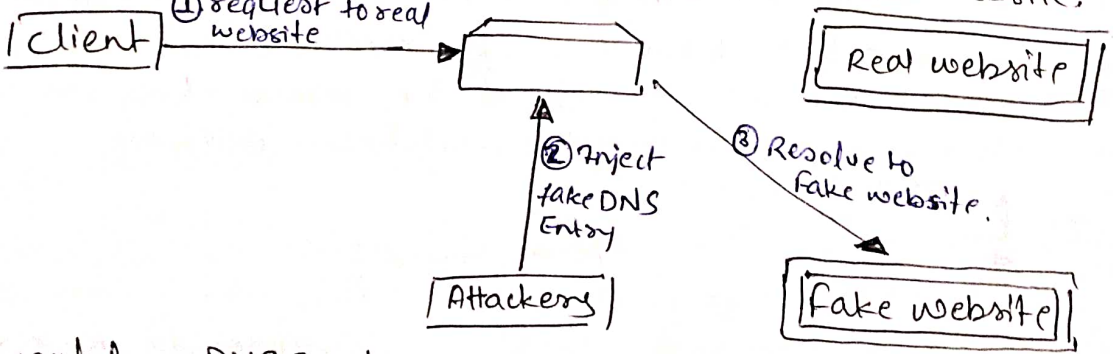
- Mapping a domain name to an IP address is known as Name-Address Resolution The DNS resolver performs this operation by consulting name servers.

A resolution can be of two types:-

1. Recursive Resolution
2. Iterative Resolution.

DNS Spoofing or DNS cache poisoning:

DNS Spoofing: It means getting a wrong entry or IP address of the request site from the DNS server. Attackers find out the flaws in the DNS system and take control and will redirect to a malicious website.



To Prevent from DNS Spoofing:-

→ DNS Security Extensions (DNSSEC) is used to add an additional layer of ~~secu~~ security in the DNS resolution process to prevent security ~~threats~~ threats such as DNS spoofing or DNS cache poisoning.

DNSSEC protects against such attackers by digitally 'signing' data so you can be assured it is valid.

Why does DNS use UDP and not TCP :

→ DNS is an application layer protocol. All application layer protocol use one of the two transport layer protocol, UDP and TCP. TCP is reliable and UDP is not reliable. DNS is supposed to be reliable, but it uses UDP why?

There are the following interesting facts about TCP & UDP on transport layer

① UDP is much faster, TCP is slower as it requires 3-way handshake. The load on DNS server is also important factor. DNS servers (since they use UDP) don't have to keep connections.

② DNS requests are generally very small and fit well within UDP segments.

③ UDP is not reliable, but reliability can be added to the application layer. An application can use UDP and can be reliable by using a timeout and resend at the application layer.

DNS primarily uses UDP on port no. 53 to serve request. DNS queries consist of a single UDP request from the client followed by a single UDP reply from server. When length of answer exceeds 512 bytes and both clients & server supports EDNS, larger UDP packets are used otherwise TCP the queries is sent again using TCP.

Dynamic Host Configuration Protocol (DHCP)

→ DHCP is an application layer protocol which is used to provide!

- Subnet mask
- Router Address.
- DNS Address
- Vendor Class Identifier.

DHCP servers dynamically distributes network configuration parameters such as IP address, subnet mask, and gateway addresses.

DHCP is based on client-Server model and based on discovery, offer, request and ACK.

DHCP port number for server is 67 and for client is 68. It is a client-Server protocol, uses UDP services.

In DHCP, the client and the server exchange mainly 4 DHCP messages. In order to make connection also called as DORA process. but there are 8 DHCP messages in the process.

These messages are :-

① DHCP Discover message : This message is generated by client host in order to discover if there is any DHCP server/servers are present in the network or not.
This message is 342 or 576 byte long.

② DHCP offer message : The server will respond to host in this message specifying the unleased IP address and other TCP configuration information
This message is broadcast by the server.
Size of message is 342 bytes

3) DHCP Request message: when client receives a offer letter/message, it responds by broadcasting a DHCP request message. The client will produce a gratuitous ARP in order to find if there is any other host present in the network with same IP address. If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP add. A client ID is also added in this message.

NOTE: This msg. is broadcast after the ARP request broadcast by the PC to find out whether any other host is not using that offered IP. If there is no reply, then the client host broadcast the DHCP request msg for server showing the acceptance of IP add.

4) DHCP Acknowledgement message: In response to the request msg received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.

5) DHCP negative Acknowledgement message: whenever a DHCP server receives a request message that is invalid according to the scopes that is configured with, it send DHCP Nak message to client.

6) DHCP Decline: If DHCP client determines the offered configuration parameters are different or invalid it sends a DHCP decline message to the server.

7) DHCP release: A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.

8) DHCP inform: If a client has obtained IP address manually then the client uses a DHCP inform to obtain other local configuration parameters, such as Domain name.
In reply to DHCP inform msg, server generates a DHCP Ack msg. with configurations suitable for client without allocating new IP address.

- Advantages of using DHCP
  - centralized management of IP add.
  - ease of adding new clients to network.
  - reuse of IP addresses reducing, total number of IP add. that are required
  - Simple reconfiguration of IP add space on DHCP server without needing to reconfigure each client
- Disadvantages of using DHCP:
  - IP conflict can occur.

Simple Network Management Protocol (SNMP)

SNMP

→ It is an application layer protocol that uses UDP port number 161/162. SNMP is used to monitor the network, detect network faults, sometimes it is used to configure remote devices.

SNMP Components:

① **SNMP manager**: It is a centralized system used to monitor network. It is also known as Network management Station (NMS)

② **SNMP agent**: It is a software management module installed on a manged devices. like PC, routers, servers, switches etc.

③ **Management Information Base**: It consist of information on resources that are to be managed. This information is organized hierarchically It consists of objects instances which are essentially variables.

SNMP messages:

① **GetRequest**: SNMP manger sends this msg to request data from SNMP agent. In response to this SNMP agent responds with requested value through response msg.

② **GetNextRequest**: This msg can be sent to discover available data on an SNMP agent The SNMP manager can request data continuously until no more data is left In this way the SNMP manager know all the available data on SNMP agent.

③ **GetBulkRequest**: This msg is used to retrive large data at once by SNMP manger from the SNMP agent.

④ **SetRequest**: It is used by the SNMP ~~manger~~ manager to set value of an object instance on the SNMP agent.

⑤ **Response**: It is a msg. sent from the agent upon a request from the manger.

⑥ **Trap**: These are the message sent by agent without being requested by the manger. It is sent when a fault has occured.

⑦ **InformRequest**: Used to identify if the Trap msg has been received by the manger or not.

SNMP security level:

→ It defines the type of a security algorithm performed on SNMP packets. These are used only in SNMPv3. There are 3 security levels:

① **noAuthNoPriv**: This (No Authentication, NO Privacy) security level uses a community string for authentication and no encryption for privacy.

② **authNoPriv**: This security level (Authentication, No Privacy) uses HMAC with MD5 for authentication and no encryption is used for privacy.

③ **authPriv**: This security level (Authentication, Privacy) uses HMAC with MD5 or SHA for authentication and encryption uses the DES-56 algorithm!

SNMP versions

① SNMPv1 : uses comunity strings for authentication. and uses UDP only.

② SNMPv2 : uses community strings for authentication. It uses UDP but can be configured to use TCP.

③ SNMPv3 : It uses Hash-based MAC with MD5 or SHA for authentication and DES-56 encryption for privacy. This version uses TCP

Simple Mail Transfer Protocol (SMTP)

→ Internet systems uses SMTP to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (Post office Protocol) and IMAP (Internet Message Access Protocol) are used to retrive those emails at the receiver's side.

SMTP ~~SMTP~~ Fundamental

→ SMTP ~~SMTP~~ is an application layer protocol. The client who wants to send mail opens a TCP connection to SMTP server and sends the mail across the connection. The SMTP server is an always-on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection through port 25. After successfully establishing a TCP connection the client process sends the mail instantly.

SMTP model (two types)

① End-to-End method
② Store-and-forward method.

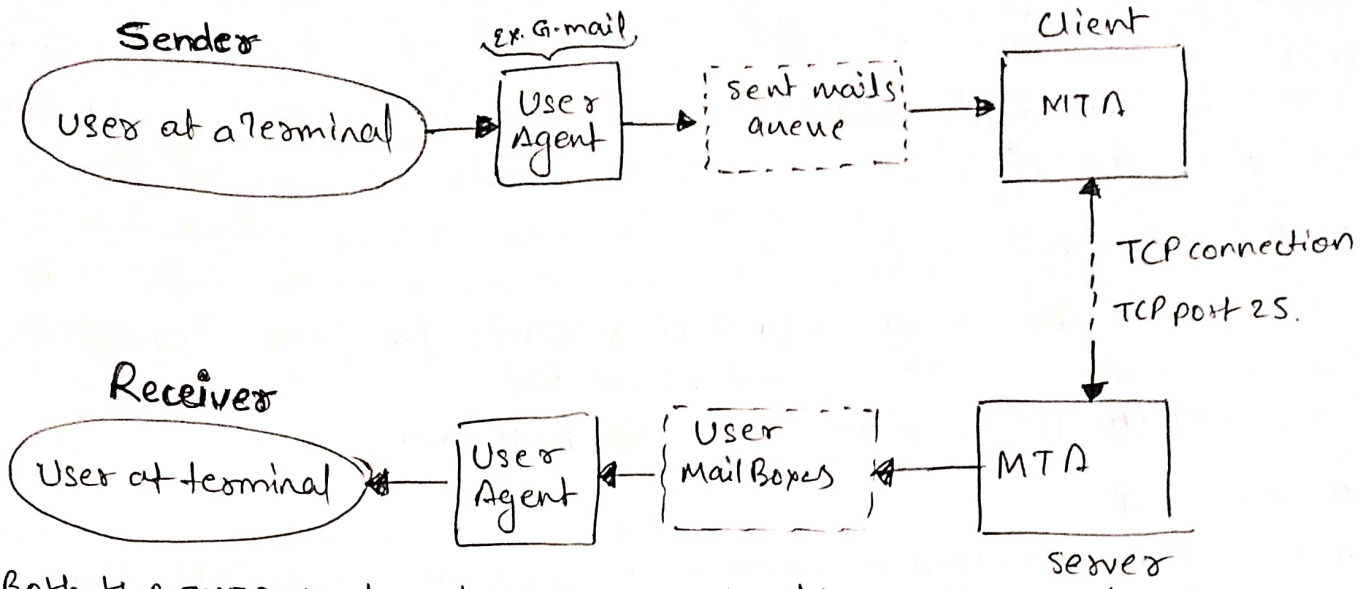
The End-to-End model is used to communicates between different organizations. And Store-and-Forward method is used to communicate within an organization. An SMTP client who wants to send mail, will directly contact to destination's host SMTP, in order to send mail to the destination. The SMTP server keep the mail to itself until it is successfully copied to the receiver's SMTP.

Model of SMTP system :

→ In SMTP model, user deals with User Agent (UA) Ex. Microsoft Outlook, Yahoo, Gmail.

→ In order to exchange the mail using TCP, MTA (Message Transfer Agent) is used. The user sending the mail doesn't have to deal with MTA as it is the responsibility of system admin to set up local MTA. The MTA maintains a small queue of mails so that it can schedule repeat delivery of mails in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agent.

This can be easily understand by the Diagram below (in ext page)



★ Both the SMTP client and SMTP server should have 2 components i-e. ① User-Agent (UA)
② Message Transfer Agent (MTA).

File Transfer Protocol (FTP)

→ FTP is an application layer protocol that moves files between local and remote file systems. It runs on the top of TCP like HTTP. To transfer a file, two TCP connections are used by FTP in parallel: ① control connection and ② Data Connection.

① Control Connection:
→ For sending control information like user identification, password, commands to change the remote directory, commands to retrive and store files. etc., FTP use of control connection.
The control connection is initiated on port No. 21.

② Data Connection:
→ For sending the actual file, FTP makes use of a Data connection.
A data connection is initiated on port number 20.

FTP sends the control info. out-of-Band as it uses a separate control connection. Some protocols send their request and response header lines and the data in same TCP connection. Therefore they are ~~known~~ as said to send their control information in-band. HTTP and SMTP are such examples.

■ FTP session:
→ When a FTP session is started between a client and a server, the client initiates a control TCP connection with the server. The client sends control info. over this. When server receives this, it initiates a data connection to the client. Only one file can be sent over one data connection. But the control connection remains active throughout the session. As HTTP is a stateless i.e. it doesn't keep track of any user state, But FTP ~~is~~ needs to maintain a state about its user throughout the session.

Advantages of FTP

- Speed
- File sharing, bet^n two machines file can be shared on the network.
- Efficiency is more in FTP.

Disadvantages of FTP

- File size limit is the drawback of FTP, only 2GB size files can be transferred.
- multiple receivers are not supported by the FTP.
- FTP does not encrypt the data, (biggest drawback of FTP)

Anonymous FTP:

- Anonymous FTP is enabled on some sites whose files are available for public access. A user can access these files without having any username or password. Instead, the username is set to anonymous and the password the guest by default. Here user access is very limited. For example, the user can be allowed to copy the files but not to navigate through directories.

HTTP Non-Persistent & Persistent Connection.

→ Hyper Text Transfer Protocol (HTTP) is an application layer protocol that ~~xxxxxx~~ uses TCP as an underlying transport and runs on port 80. HTTP is a stateless protocol i.e. server maintains no ~~if~~ information about past client requests.

→ HTTP is a protocol using which hypertext is transferred over the web.

HTTP connections:

① Persistent
② Non-Persistent.

what is RTT (Round-Trip-Time)

→ measure (in ms) of the latency of a network — that is, the time between initiating a network request and receiving a response.

→ It refers to the time taken by a network request to reach a destination and to revert back to the original source.

Difference between Persistent & non-Persistent connection

Nonpersistent HTTP	Persistent HTTP
• requires 2 RTT's per object	• server leaves connection open after sending response
• OS overhead for each TCP connection.	• Subsequent HTTP messages between some client/server sent over open connection
• Browsers often open parallel TCP connections to fetch referenced objects.	• Client sends requests as soon as it encounters a referenced object
	• as little as one RTT for all the referenced objects

Difference Between http:// and https://

→ HTTP is a protocol using which hypertext is transferred over the web. Due to its simplicity, http has been the most widely used protocol for data transfer (hypertext) over the web but the data (i.e. hypertext) exchanged using http isn't as secure as we would like it to be. Infact, hypertext exchanged using http goes as a plain text. i.e. anyone between the browser and server can read it easily

? But why do we need this security over the web?
⇒ for financial Transaction, passwords, imp informations etc.

→ Https was introduced so that a secure session is setup first between server and Browser. then hypertext was exchanged.
Cryptographic protocols such as SSL and/or TLS is present in Https.
i.e. https = http + cryptographic. → Secure Socket Layer → Transport Layer Security

→ Also another difference between http & https is that http uses default port 80 while https uses default port 443
Security in https is achieved ~~by~~ at the cost of processing time becaus web server and web Browser needs to exchange encryption keys using certificates before actual data can be transferred.
Bassically, setting up of a secure session is done before the actual hypertext exchange between server and browser.

■ Difference bet" http & https

- URL of http starts with "http://" and URL of https "https://"
- HTTP uses port 80 while https uses port 443.
- HTTP is unsecure and https is secure
- HTTP Works at Aplication layer while HTTPS works at transport layer.
- HTTP, encryption is absent while In HTTPS encryption is present.
- HTTP, does not require any certificates, HTTPS requires certificates like SSL.

Multipurpos Internet Mail Protocol (MIME)
Extension

→ It allows to the users to exchange different kinds of data files on the Internet like audio, video, application program etc.

■ Features of MIME

- Able to send multiple attachments with a single message.
- Unlimited message length
- Binary attachments (exe; audio, video, img. etc)

Difference Between Internet and Web

→ The Internet is a global Network while the web (World Wide Web) is a collection of information that can be accessed via internet.
→ web applications use HTTP protocol which is a layer over TCP protocol, whereas Internet applications can use either TCP or UDP protocol.

Wifi (Wireless Fidelity)

- wifi stands for wireless fidelity. It is a technology for wireless local area networking with devices based on IEEE 802.11 standards
  Wifi compatible devices can connect to the internet via WLAN network and a wireless Access Point (AP). Every WLAN has an access point which is responsible for receiving and transmitting data from/to users.

Wifi Protected Setup (WPS)

- The wifi Protected Setup (WPS) is a wireless network security standard that tries to make connections between a router and wireless devices.
- WPS works only for wireless networks that uses a password that is protected with wifi Protected Access (WPA) or wifi Protected Access II (WPA2) Personal security protocol.
- WPS does not work on wireless network that uses the Wired Equivalent Privacy (WEP) security, which can be easily cracked by hackers.
- In a standard setup, we cant connect a wireless device to a wireless network until we know the network name (ie. Service Set Identifier (SSID)) and its password (also called WPA-PSK key).

Wifi Protected Access (WPA)

- The two security protocols and security certification programs are WPA and WPA2
  WPA also reffered as the draft IEEE:802.11i standard, available in 2003.
  WPA2 reffered as draft IEEE:802.11i-2004 standard, available in 2004.

WPA

- The WPA protocol implements almost all of the IEEE 802.11i standard. The Temporal key Integrity Protocol (TKIP) was adopted for WPA. WEP uses a 64 bit or 128 bit encryption key that must be manually entered on wireless access points and devices which once entered can never be changed.
  TKIP employs a per-packet key, which means that it dynamically generates a new 128 bit key for each packet and thus prevents the types of attacks that compromised WEP.
- WPA included a message Integrity Check, which is designed to prevent attacker to alter or resent data packets. This replaced the Cyclic Redundancy Check (CRC) that was used by WEP. CRC's had a main flaw that it did not provide a sufficiently strong data integrity guarantee for the packets it handled.
  WPA uses a msg integrity check algorithm called (TKIP) to varify the integrity of the packets.
  TKIP is stronger than CRC but algo used in WPA2 is more stronger.
  Researchers discovered a flaw in WPA similar to older weaknesses in WEP and the limitations of the msg integrity code hash function, named Michael, that is used to retrieve the keystream from short packets to use for re-injection and spoofing.

[2] WPA 2

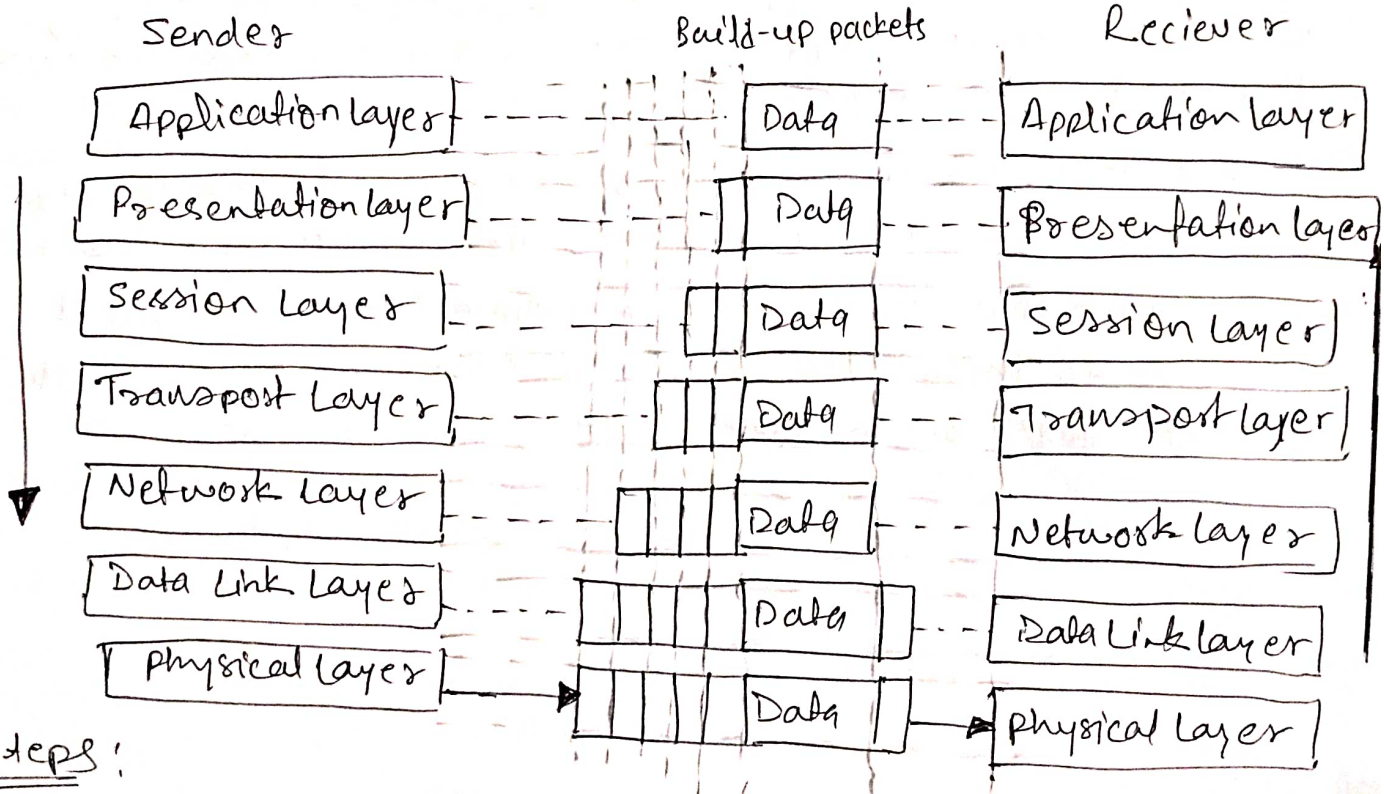
→ WPA2 replaced WPA. WPA2 which requires testing and certification by the wifi Alliance, implemented the mandatory elements of IEEE 802.11i. Particularly, it included mandatory support for CCMP (Counter mode CBC-MAC protocol), an AES (Advanced Encryption standard) based encryption mode. Certification began in September 2004, WPA2 certification is mandatory for all new devices to bear the wifi trademark from March 13, 2006.

How Communication happens using OSI model

→ The OSI model defines a seven layer set of functional elements, (from physical interrelations at physical layer (Layer 1) to application layer (Layer 7)

TCP and IP are two network standards that defines the internet.

■ The communication process in the OSI model :



→ Steps :

① Each layer of the sender adds info to the msg received from above layer and moves the entire package just below the layer

② Each layer added its info in the form of headers. Headers are added at the level of the messages (6, 5, 4, 3 and 2). A Header is added at the Data Link layer (Layer 2).

(3) At the physical layer, communication is direct. i.e. the sender sends a stream of bits to the receiver. At the physical layer the entire package is converted into a form that can be transferred to the receiver. On the receiver side, each process is accompained layer-by-layer to receive and delete msg data.

(4) Always the upper OSI layers are implemented in the software (Transport layer, session layer, Presentation layer, App. layer) and the lower layers are combination of hardware & software. (i.e. layer 2 & 3) except for physical layer which is mostly hardware.

Layer 1, 2, 3 (physical layer, Data Link layer, Network layer) are network support layers. They deal with physical aspect of moving data such as electrical specification, physical connections, physical address, and transport time and reliability from one device to another

Layer 4 (Transport layer) end to end ensures reliable data transmission

(5) Not all applications need to use 7-layers. The lower three layers are sufficient for most applications. Each layer is made up of electronic circuits and/or software and has a seperate existance from rest of the layers.

(6) Each layers is assumed to handle msgs or data from the layers that are above or below it. (This is done by following protocol rules)

(7) Thus, each layer takes data from adjacent layer, Handles it according to these rules, and then sends the processed data to next layer on the other side.

#Packet Traveling

#OSI Model :

OSI Layer1 - Physical :

→ The physical layer of OSI model is responsible for the transfer of bits i.e. the 0's and 1's which make up all computer code.

→ This layer represents the physical medium which is carrying the traffic between two nodes. An example would be Ethernet cable or Serial cable But what about wireless, such as WiFi, As such WiFi, despite it not having a physical, tangible presence, is also considered a layer1 protocol

• In simple words, Layer 1 is anything that carries 1's and 0's bet^n two nod

→ The actual formate of data on the wire can vary with each medium, like, in Ethernet, bits are transferred in form of electric pulse, and In case of WiFi; bits are transferred in the form of radio waves.

→ Repeaters & Hub are also operate at this layer.
Repeaters simply repeats a signal from one medium to other. and A Hub is simply a multi-port Repeater.

OSI Layer 2 - Data Link

→ The Data Link Layer of the OSI model is responsible for interfacing with the physical layer. Effectively, Layer 2 is responsible for putting 1's and 0's on the wire. and pulling 1's and 0's from the wire

→ The NIC that we plug our Ethernet wire into handles the Layer 2 functionality. It receives signals from the wire, and transmits signals on to the wire.
WiFi NIC works the same way, receiving and transmitting radio waves which are then interpreted as a series of 1's and 0's.

→ Layer 2 will then group together those 1's and 0's into chunks known as frames.

→ There is an addressing system exists at Layer 2 known as MAC address. The MAC add. uniquely identifies each individual NIC.

→ Aside from NIC, switch also operates at this layer. A switch's primary responsibility is to facilitate communication within Networks.

→ Function of Data Link Layer is to deliver packets from one NIC to another. OR, (Another way):
The role of Layer 2 is to deliver packets from hop to hop.

OSI Layer 3 - Network:

→ The Network layer of OSI model is responsible for packet delivery from end-to-end.
→ It does this by using another addressing scheme that can logically identify every node connected to the Internet. This addressing scheme is known as Internet Protocol (IP address)
→ It is considered logical because an IP address is not a permanent identification of a computer. Unlike the MAC add. which is considered a physical add, the IP add. is not burned into any computer hardware by the manufacture.
→ Routers are Network Devices that Operate at Layer 3 of the OSI model. A Router's primary responsibility is to facilitate communication between networks.

OSI → Layer 2 vs Layer 3

→ Layer 2 uses MAC add. and is responsible for packet to deliver from hop-by-hop
→ Layer 3 uses IP add. and is responsible for packet delivery from end-to-end.
→ When computer has data to send, it encapsulates it in a IP header which will include info. like the Source & Destination IP add. of the two "ends" of the communication.

The IP header and Data are further encapsulated in a MAC add. Header, which will include info. like the Source & Destination MAC add. of the current "hop" in the ~~path~~ path towards the final destination.

OSI Layer 4 - Transport

→ The Transport Layer of OSI model is responsible for distinguishing network streams.
→ At any given time on a user's computer there might be an Internet browser open, while music is being streamed, while a messenger is running. Each of these applications are sending and receiving data from the internet and all the data is arriving in form of 1's and 0's on to that computer's NIC.

Something has to exist in order to distinguish which 1's and 0's belong to the messenger or browser or streaming music. That "something" is Layer 4.

→ Layer 4 accomplishes this by using an addressing scheme known as port Numbers.

→ Specifically, two methods of distinguishing network streams exist. They are known as the TCP and the UDP.

→ If Layer 2 is responsible for hop-by-hop delivery, and Layer 3 is responsible for end-to-end delivery, it can be said that Layer 4 is responsible for service-to-service delivery.

OSI Layers 5, 6, 7

→ The Session, Presentation, and Application Layers of OSI model handles the final steps before the data transferred through the network (facilitated by Layers 1-4) is displayed to the end user.