Network topologies:

A Network Topology is the arrangement with which computer systems or network devices are connected to each other.

1. Bus topology:

All devices shares single communication line or cable

Data is sent in only one direction.

1. Ring topology:

Each host machine is connected to two devices, creating a circular network

Even in this data is transmitted in single direction

Failure of any host results in the failure of data transmission (whole ring)

1. Star topology:

All hosts in this topology are connected to a central device i.e point to point connection between hubs and nodes.

Hub device can be a hub/repeater\_layer1, switch/bridge\_ layer2, router/gateway\_ layer3.

Robustness \_if one link is failed only that link is affected, all other links will remain active.

1. Mesh topology:

Each computer and network device is interconnected with each other for fault tolerance.

Used for redundancy purpose, more reliable, robust

1. Tree topology:

Also known as hierarchical topology acts as extended star topology and inherits the properties of bus topology.

Multiple star networks are connected to other star networks in the form of tree structure.

1. Hybrid topology:

It’s a combination of different topologies.

Internet is the best example of hybrid technology.

Networking devices:

* Hub
* Repeaters
* NIC
* Bridges
* Switch
* Routers

NIC:

Connect a computer with network, allows users to connect with each other by using cables or wireless.

Three types of NIC: void NIC, wireless NIC, fiber optic NIC

Hub:

Common connection point for devices in a network, connects devices physically.

It is broadcasting.

Hubs cannot filter data, so data packets are sent to all connected devices.

Data is sent in binary format.

Half duplex i.e data can be sent in only one direction at a time.

Repeater:

Receives a signal and retransmits it.

Used to extend the signal to cover long distances.

When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device

Bridges:

Builds the connection with same bridge networks which uses the same protocol.

Operates at the data link layer.

Filters the content by reading MAC addresses of source and destination

Switch:

It’s a device used in the data link layer.

It has the capacity to make decision i.e before forwarding the data packet it checks the packet if there is any error it won’t forward the packet.

It’s multicasting device.

Data is sent in the form of frames based on MAC address. (getmac, )

Full duplex i.e data can be sent in two ways at the same time.

Router:

Used to communicate between 2 different networks.

Network layer device

Routes data packets based on ip address

Data will be sent in the form of packets.

IPV4:

Each and every pc or host are identified by an address in a network without ip address it is impossible to communicate with other systems.

Also known as “Logical address”.

32 bit ip address having 4 octets, supports maximum of 2^32

Fourth version internet protocol, connectionless protocol used in switched layer networks such as Ethernet.

Logical connection between network devices by providing identification for each device.

IPv4 uses 32-bit addresses for Ethernet communication in five classes: A, B, C, D and E.

A, B, C have a different bit length for addressing the network host

A: 1-126 – Large network

B: 128-191 \_ Medium sized network

C: 192-233 \_ Small network

D: 224-239 \_ addresses are reserved for multicasting

E: 240-255\_ addresses are reserved for future uses (research and development)

1. CLASS A: 1-126

Have 4 octets

Default subnet mask: 255.0.0.0

Private address range: 10.0.0.0 \_ 10.255.255.255

1. CLASS B: 128-191

Have 4 octets two for network and two for host

Default subnet mask: 255.255.0.0

Private address range: 172.16.0.0 \_ 172.31.255.255

1. CLASS C: 192-223

Have four octets three are used for network and one is used for host

Default subnet mask: 255.255.255.0

Private address range: 192.168.0.0 \_ 192.168.255.255

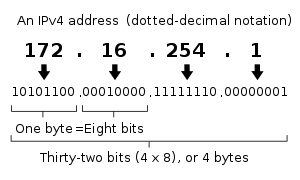
* 127.0.0.1\_ loopback address used to check self ip address (check NIC) so it is known as self testing ip address
* Run \_ Cmd\_ ping 127.0.0.1

SUBNET MASK:

It’s a 32 bit number used to differentiate the network component of ip address by dividing it into a network address and host address. Also known as address mask.

It determines both the number and size of subnets where the size of a subnet is the number of hosts that can be addressed, it reduces the cost of organization

In any given network 2 addresses are always reserved i.e 0 \_network address / network identification 255- broadcast address



APIPA: Automatic Private IP Address

Also called as link \_ local address

When DHCP is not working at that time client can automatically self configure an ip address

APIPA range: 169.254.0.1 \_169.254.255.254 (class B)

 Host search for a DHCP server on the network before assigning link-local addresses

In the automatic address configuration process, network hosts select a random candidate address within the reserved range and use [Address Resolution Protocol](https://en.wikipedia.org/wiki/Address_Resolution_Protocol) (ARP) probes to ascertain that the address is not in use on the network. If a reply is received to the ARP, it indicates the candidate IP address is already in use; a new random candidate IP address is then created and the process repeated. The process ends when there is no reply to the ARP, indicating the candidate IP address is available.

MULTICASTING:

It’s a method of sending ip datagrams to a group of interested people in a single transmission.

Point to multipoint communication

Multicast uses UDP (User Datagram Protocol)

Applied in the link layer and internet layer

BROADCAST ADDRESS:

It’s a special internet protocol address used to transmit messages and data packets to network systems.

Network administrator verifies successful data packet transmission via broadcast address.

DHCP and Bootstrap protocol clients uses broadcast addresses to locate and transmit respective server requests.

Many \_ many communication

Broadcasting address analogy:

*A teacher is preparing to announce the winner of a student competition and can use either of the following approaches: (1) The teacher could stop by each student’s desk and discreetly reveal the winner's name, or (2) The teacher could announce the winner's name to the class and then ask the winner to stand for recognition. The second option, which is more efficient, is broadcast addressing in the real world.*

*UNICAST ADDRESS:*

*An address that identifies a unique node on a network.*

*Point\_ Point communication*

A unicast address is used in the following instances:

* Unspecified Interface Address: A unicast address with a value of 0:0:0:0:0:0:0:0 is used in the absence of an unspecified interface address.
* Loopback Address: A unicast address with a value of 0:0:0:0:0:0:0:1 is used to specify a loopback address used to redirect the packets to their source.

ANYCAST:

It’s one of the features of IPv6

Single \_ nearest

OPEN SYSTEMS INTERCONNECTION MODEL (OSI MODEL)

It’s a conceptual and logical layout that defines communication used by systems open to interconnection and communication with other systems.

It defines a networking framework to implement protocols in layers, with control passed from one layer to another layer.

It is divided into seven subcomponents. They are:

1. Physical layer\_ bits
2. Data link layer\_ frame
3. Network layer\_ packets
4. Transport layer\_ segment
5. Session layer\_ data
6. Presentation layer\_ data
7. Application layer\_ data

OSI model is divided into two portions, 1. Hot layers 2. Media layers

Hot layers/ Software layers: application, presentation, session and transport (Heart of OSI)

Media layers/ Hardware layers: physical, data link, network

Trouble shooting can be done easily.

It provides standards for devices that are to be manufactured.

PHYSICAL LAYER:

This layer deals with bit level transmission between different devices

Responsible for electrical, mechanical and procedural checks.

Data will be converted into binary format.

Devices working at this layer are hubs, repeaters, cables, modems etc

Data will be in the form of electrical pulses in coaxial or twisted pair cables and in the form of light in optic fiber cables.

Functions of physical layer:

1. Hardware specification: contains details of physical cables, wireless cards etc.
2. Encoding and Signaling: how the bits are encoded in this medium.
3. Data transmission and reception: it is responsible for transferring each bit of data, transmission is not completely reliable as there is no error correction in this layer.
4. Topology and network design: network design is the integral part of this layer. It will decide where the devices and how many number of devices has to be placed

Application layer:

Provides networking services to the user. It is the only layer that directly interacts with the user.

Also known as “Desktop layer”, identification of services is done by using port numbers. It’s major network device in the gateway.

Total ports: 0-65535

Reserved ports: 0-1023

Open client ports: 1024-65535

Presentation layer:

Converts data into standard format.

Many tasks such as encoding- decoding, encryption- decryption, compression- decompression

Session layer:

Responsible for establishing, maintaining and terminating sessions

All VPN comes under the session layer

Ex: RPC: Remote Procedure Call

SQL: Structured Query Language

NFS: Network File System

Transport layer:

End- End connectivity, also known as “Heart of OSI”

This layer divides the web pages into segments and assigns a id which will be used for setting the arrangements in destination.

Source and destination port number are configured in this layer

Tasks performed by this layer are:

Identifying service

Multiplexing and de-multiplexing

Segmentation

Sequencing and reassembling

Error correction

Flow control

Network layer:

Responsible for providing path to data to reach the destination by using IP address.

Logical addressing works in this layer. Router is the network layer device.

It’s divided into two parts:

1. Routed protocols

IP, IPX, Apple Talk

1. Routing protocols

Data link layer:

This layer provides reliable transmission of packets by using the services of physical layer which transmits the bits over the medium in unreliable fashion.

Divided into two sublayers.

1. LLC: Logical Link Control

Talks about WAN protocols (PPP, HDLC, Frame-relay)

1. MAC: Media Access Control

Talks about physical address. It’s a 48 bit address, responsible for error detection

MAC Filtering:

Refers to security access control method whereby the 48 bit address assigned to every NIC is used to determine access to network. I.e. it may permit or deny the network access.

Devices working on this layer are switch, bridge etc

Framing: breaking input data into frames and caring about the frame boundaries and size of the each frame.

Services of data link layer:

1. Error detection and correction:  error detection refers to the techniques used to detect noise or other impairments introduced into data while it is transmitted from source to destination

Ex: HELLO 8 5 12 12 15 we will get a total of 52 i.e. 5+2=7 the data will be transmitted as “8 5 12 12 15 7” the receiver checks the last digit and decided whether it is the right data packet or not. Suppose it receives “7 5 12 12 15” then it calculates then we will get 51 i.e. 5+1=6 as this is wrong it will discard the packet.

Error correction is of two types: FEC and BEC

1. Addressing:
2. Flow control:

It is used in data communications to manage the flow of data among two different nodes that too in the cases where the sending device can send data much faster than the receiver can digest.

Xon - Xoff is an example of a flow control protocol that sync the sender with the receiver. It transmits transmit off signal when the receiver no longer has space in its buffer and a transmit on signal when the receiver can resume taking data. Xon-Xoff works on asynchronous serial connections.

Media Access Control:

Also known as physical address or hardware address.

It is a unique identifier provided to an Ethernet or network adapter over a network.

It is assigned by the vendor/ manufacturer of NIC

MAC addresses are permanent

It is a 12 digit hexadecimal address in which first 6 digits refer to the manufacturer’s id and the last 6 digits refers to any random/ unique identifier.

TCP/ IP layers:

1. Application
2. Transport
3. Internet
4. Network access (data link layer+ physical layer)

PROTOCOLS:

Set of rules that describes how data is transmitted over a network.

TCP/ IP PROTOCOL SUITE:

TCP: connection oriented

Reliable delivery of data

Ordering of delivery

USER DATAGRAM PROTOCOL:

Connectionless service

Unreliable

Protocol Port Number:

TCP:

FTP\_ 20, 21

POP3\_ 110 (receives the mails)

SSH (SECURED SHELL) \_ 22

NTP (network time protocol) \_123 (maintain the standard time within the organization)

Telnet\_ 23 (Accessing system remotely)

IMAP4 (Internet Message Access Protocol) \_ 143 (to make the messages centralized)

SMTP\_ 25

HTTPS\_ 443

HTTP\_ 80 (accessing websites)

UDP:

DNS\_ 53 (translating ip\_ name and vice versa)

DHCP\_ 67 (assigning ip address automatically/ dynamically)

TFTP (Trivial File Transfer protocol) \_ 69 (transferring of files in a secured way)

SNMP (Simple Network Management Protocol) \_ 161 (for monitoring the network)

TRANSMISSION MEDIA:

It determines the physical path between the transmitter and receiver in a data transmission system.

It is of two types. They are: 1. Guided 2. Unguided

Guided/ bounded:

Twisted pair cables\_ electrical pulses, decreases the cross talk interference

Co- axial cables\_ analog and digital signals

Optic fiber cables

Cross talk:

It is a phenomenon by which a signal transmitted on a circuit/ channel creates an undesired effect in another circuit/ channel.

Co\_ axial cables: less interference and cross talk when compared to twisted pair cable.

For long distance transmission of analog signals amplifiers are needed for every few km.

2 types of co\_ axial cables: thicknet and thinnet

Physical description:

Inner conductor is solid copper metal

Separated by insulating material

Outer conductor is braided shielded

Covered by sheath material

OPTICAL FIBER CABLES:

Transmits light signals, inner core is made up of glass/ plastic.

Outermost layer is jacket which is made up of plastic

50 microns in diameter.

2 types of optic fiber cables: 1. Single mode 2. Multimode

Unguided media:

1. Bluetooth:

Wireless protocol for exchanging data over a short distance by creating personal area network.

1. Infrared:

EM radiation with wave length longer than that of visible light.

TROUBLE SHOOTING COMMANDS:

PING\_ packet internet groper

TRACERT\_ displays the route and measures the transit delay in packet transfer

IPCONFIG

IPCONFIG/ALL

PING IPADDRESS\_ T

NETSTAT

NETSH WINSOCK RESET (for resetting NIC)

Wireless systems:

Cellular system

Wireless LAN’S

Satellite system

Paging system

PAN’s

Wi\_ fi network topologies:

Peer\_ Peer topology (adhoc)

AP based topology (infrastructive)

Peer\_ peer:

AP is not required.

Client devices can communicate with each other directly

Useful for setting up a wireless network quickly and easily.

Infrastructure network:

Client communicate through access point.

If a mobile station needs to communicate with other mobile station then it has to send information to AP first, then AP sends it to the destination MS.

Hotspot: it’s a geographical area that has a readily accessible wireless network.

Equipped with broadband connection and one or more AP that allow users to access the internet wirelessly.

Wi\_ Fi working:

Wi\_ fi hotspot can be created by installing an access point to an internet connection

AP acts as a base station.

Whenever Wi \_ fi enabled device encounters a hotspot the device can connect to that network wirelessly.

Single AP can support up to 30 users and can function with in a range of 100-150 feet

Elements of a wi\_ fi network:

AP: a wireless LAN transceiver of base station that can connect one or more wireless devices simultaneously to the internet.

Wi\_ fi cards:

They accept wireless signal and relay information. Can be internal and external.

TCP congestion control:

* **Flow and congestion control:** TCP takes care of flow control by ensuring that both ends have enough resources and both can handle the speed of data transfer of each other so that none of them gets overloaded with data. The term congestion control is used in almost the same context except that resources and speed of each router is also taken care of. The main concern is network resources in the latter case.

DHCP: (client\_ server model)

DHCP server dynamically assigns ip address and assigns other network configuration parameters to each device on a network so that they can communicate with other ip networks, manages TCP/ IP settings for devices on a network by automatically/ dynamically assigning the ip address

This conveys the address to the client. Router or a residential gateway can be enables as a DHCP server.

Basic working mechanism of DHCP:

COM\_ NETWORK DHCP client software sends a DHCP broadcast query requesting the information, any DHCP server may serve the request

