Networking Notes :
Almost 7-8 Questions In CCAT

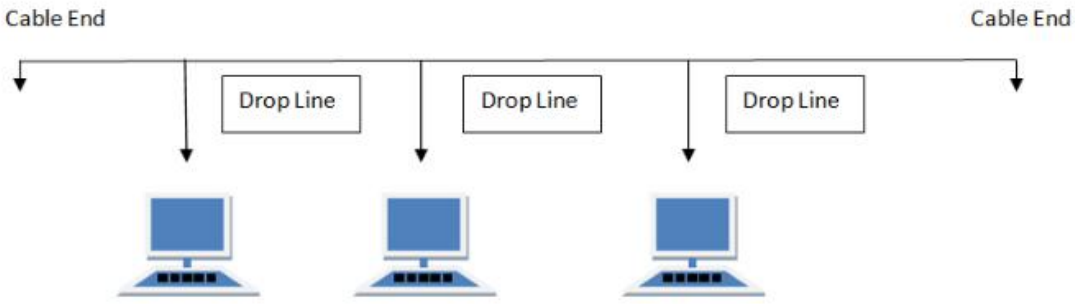
Topology :

Types of Network Topology :

Network Topology is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection.

1. BUS Topology :

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

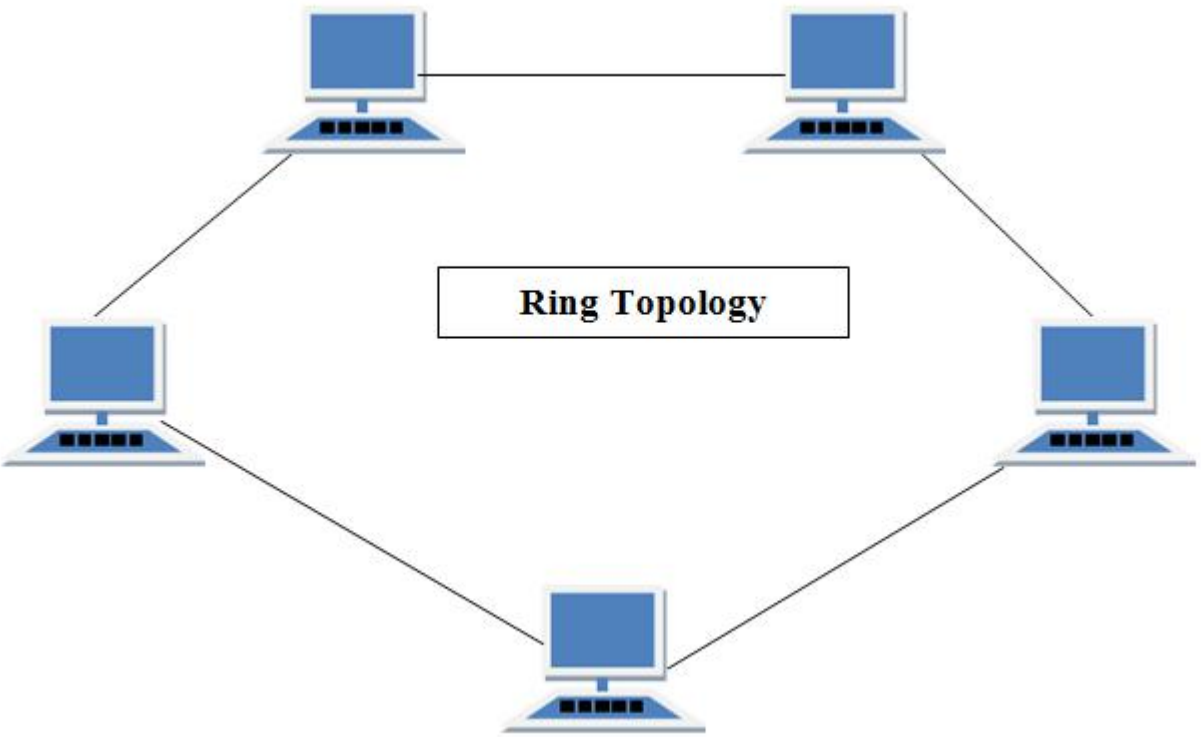
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

2.RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.

3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

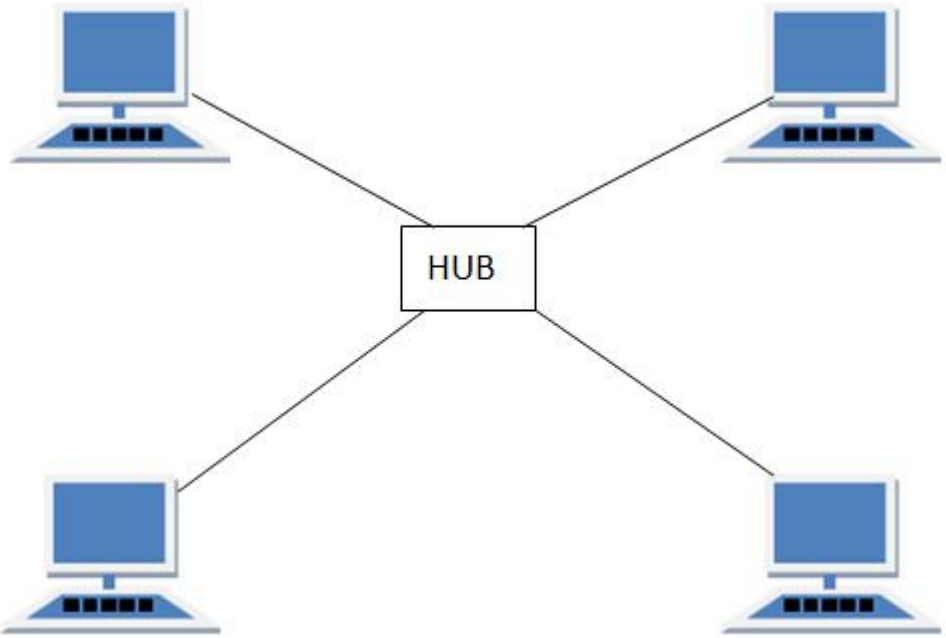
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

3.STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.

2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity.

4.MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has `n(n-1)/2` physical channels to link `n` devices.

There are two techniques to transmit data over the Mesh topology, they are :

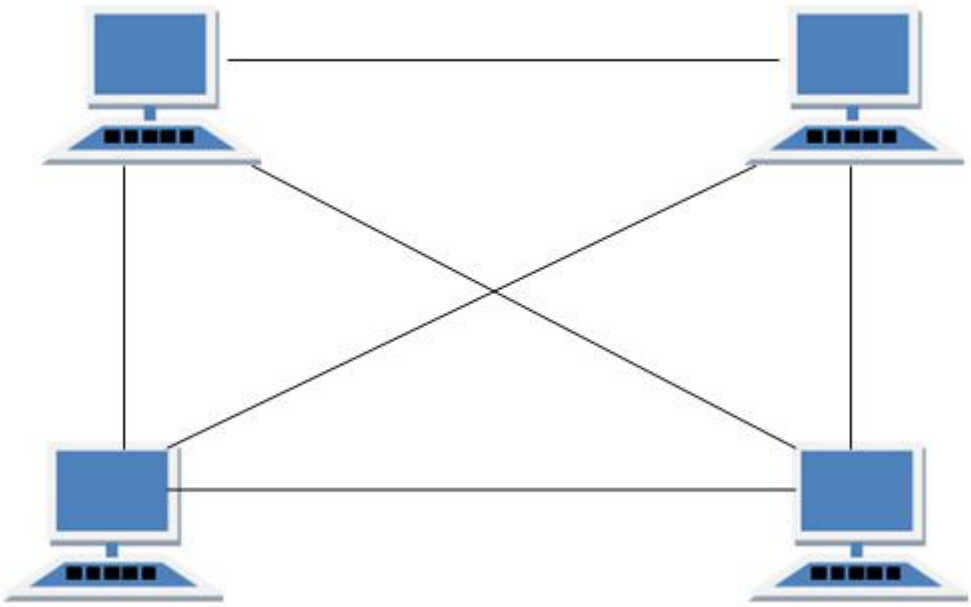
1. Routing
2. Flooding

MESH Topology: Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

MESH Topology: Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.



Types of Mesh Topology

1. **Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :** Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.

2. Robust.
3. Not flexible.

Advantages of Mesh Topology

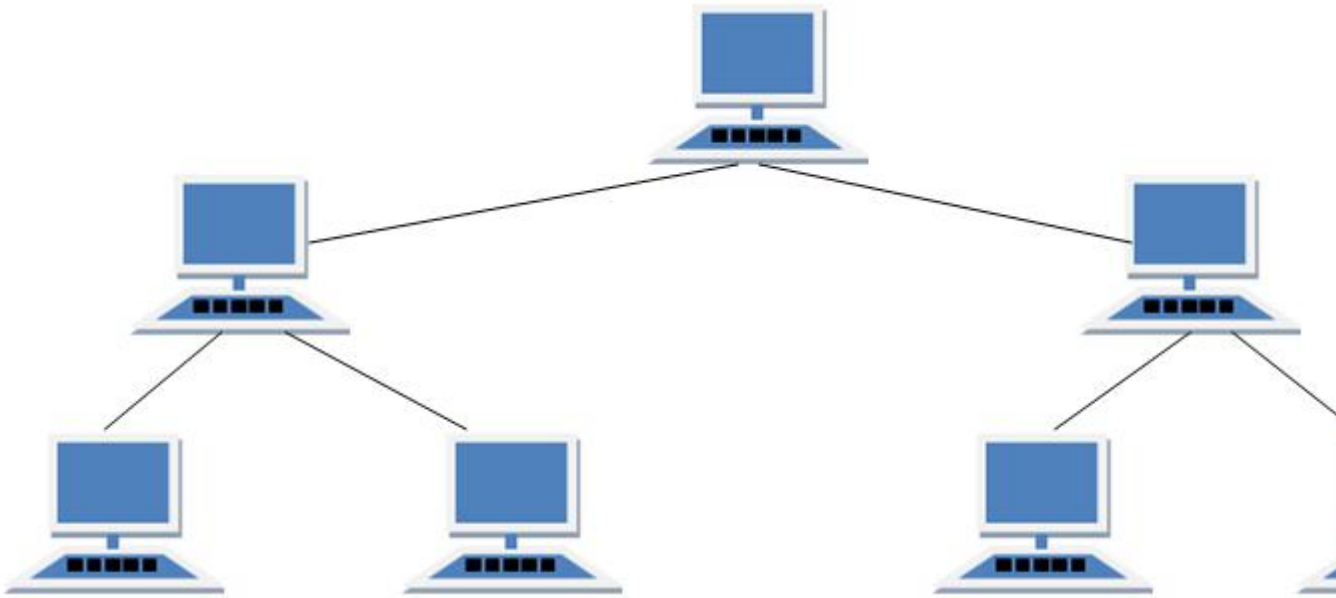
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

5.TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

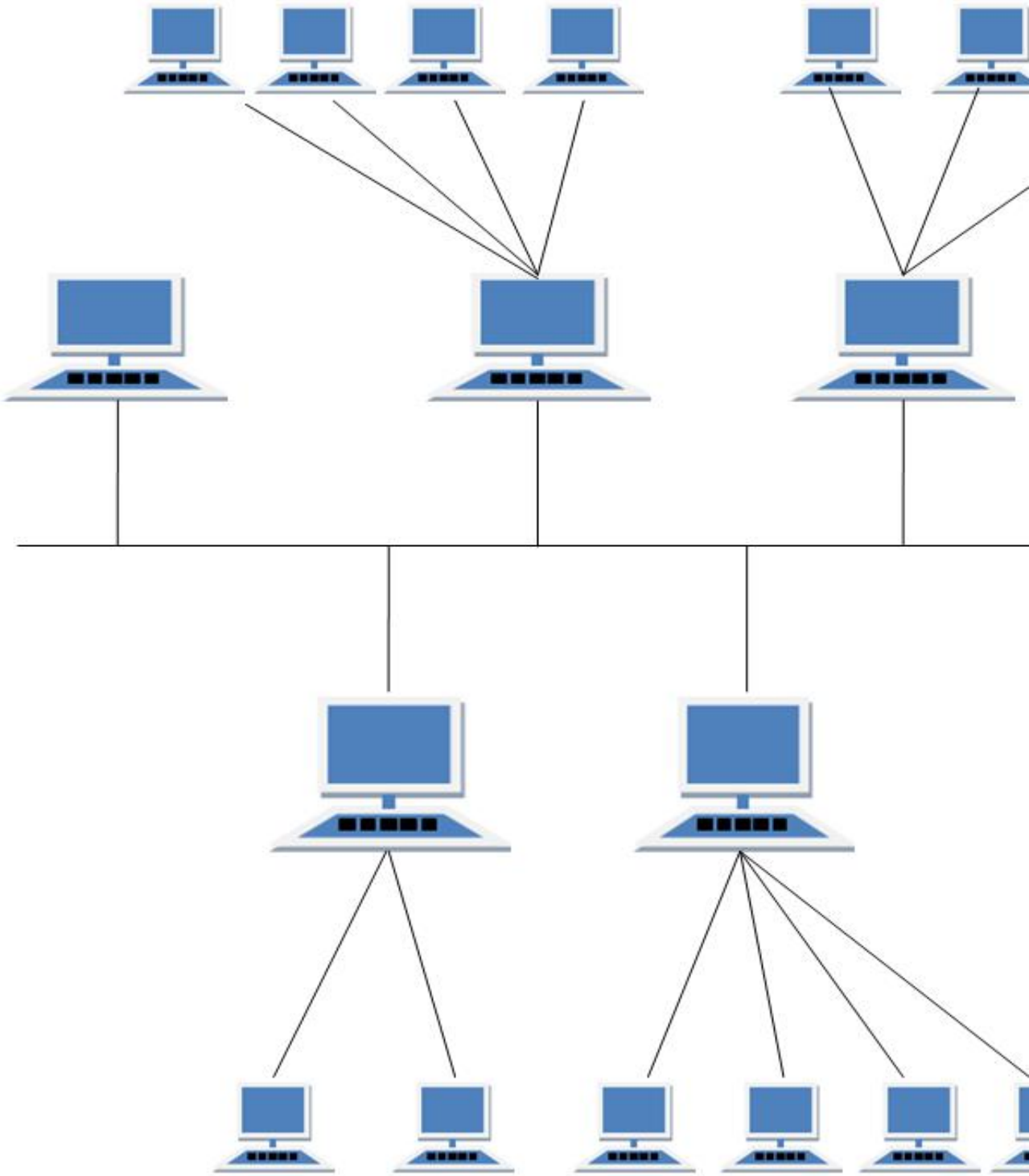
1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

6.HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Router)

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the

signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. 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.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub** :- These are the hubs which have their own power supply and can clean , boost and relay the signal along the network. It serves both

as a repeater as well as wiring center. These are used to extend maximum distance between nodes.

- **Passive Hub** :- These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend distance between nodes.

3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Types of Bridges

- **Transparent Bridges** :- These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network , reconfiguration of
the stations is unnecessary. These bridges makes

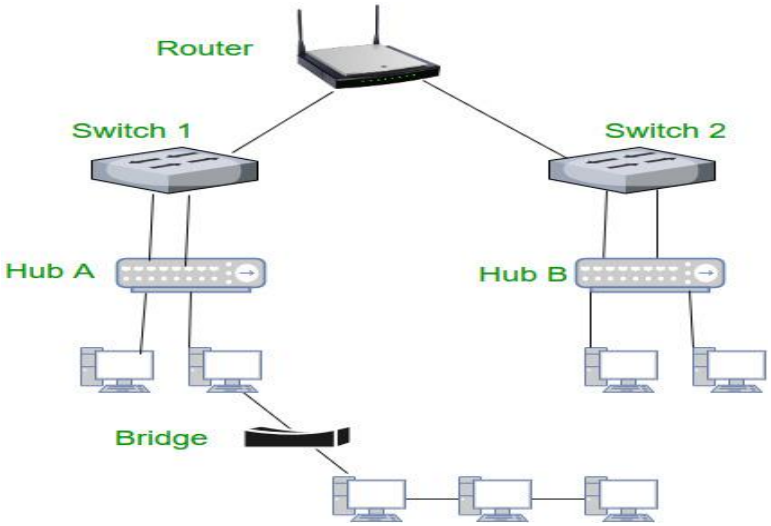
use of two processes i.e. bridge forwarding and bridge learning.

- **Source Routing Bridges** :- In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a specical frame called discovery frame, which spreads through the entire network using all possible paths to destination.

4. Switch – A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses.

Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

6. **Brouter** – It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic. ..

Note : Just explore above networking devices little bit more on internet so you can solve any question on networking devices .

Switching techniques:

Switched communication networks are those in which data transferred from source to destination is routed between various intermediate nodes. Switching is the technique by which nodes control or switch data to transmit it between specific points on a network. There are 3 common switching techniques:

1. Circuit Switching
2. Packet Switching
3. Message Switching

Message Switching –

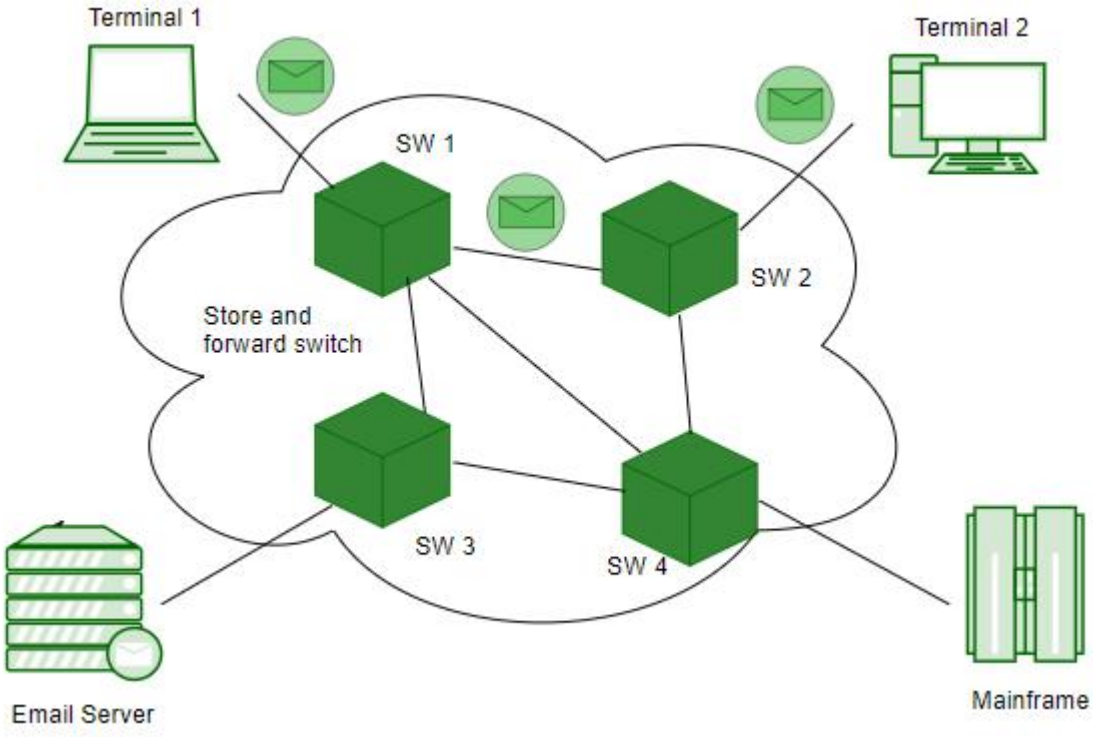
Message switching was a technique developed as an alternate to circuit switching, before packet switching was introduced. In message switching, end users communicate by sending and receiving messages that included the entire data to be shared. Messages are the smallest individual unit. Also, the sender and receiver are not directly connected. There are a number of intermediate nodes transfer data and ensure that the message

reaches its destination. Message switched data networks are hence called hop-by-hop systems.

They provide 2 distinct and important characteristics:

1. **Store and forward** – The intermediate nodes have the responsibility of transferring the entire message to the next node. Hence, each node must have storage capacity. A message will only be delivered if the next hop and the link connecting it are both available, otherwise it'll be stored indefinitely. A store-and-forward switch forwards a message only if sufficient resources are available and the next hop is accepting data. This is called the store-and-forward property.
2. **Message delivery** – This implies wrapping the entire information in a single message and transferring it from the source to the destination node. Each message must have a header that contains the message routing information, including the source and destination.

Message switching network consists of transmission links (channels), store-and-forward switch nodes and end stations as shown in the following picture:



Characteristics of message switching –

Message switching is advantageous as it enables efficient usage of network resources. Also, because of the store-and-forward capability of intermediary nodes, traffic can be efficiently regulated and controlled. Message delivery as one unit, rather than in pieces, is another benefit.

However, message switching has certain disadvantages as well. Since messages are stored indefinitely at each intermediate node, switches require large storage capacity. Also, these are pretty slow. This is because at each node, first there us wait

till the entire message is received, then it must be stored and transmitted after processing the next node and links to it depending on availability and channel traffic. Hence, message switching cannot be used for real time or interactive applications like video conference.

Applications –

The store-and-forward method was implemented in telegraph message switching centres. Today, although many major networks and systems are packet-switched or circuit switched networks, their delivery processes can be based on message switching. For example, in most electronic mail systems the delivery process is based on message switching, while the network is in fact either circuit-switched or packet-switched.

Circuit Switching VS Packet Switching:

CIRCUIT SWITCHING	PACKET SWITCHING
In circuit switching	In Packet switching

there are 3 phases i) Connection Establishment. ii) Data Transfer. iii) Connection Released.	directly data transfer takes place .
In circuit switching, each data unit know the entire path address which is provided by the source	In Packet switching, each data unit just know the final destination address intermediate path is decided by the routers.
In Circuit switching, data is processed at source system only	In Packet switching, data is processed at all intermediate node including source system.
Delay between data units in circuit switching is uniform.	Delay between data units in packet switching is not uniform.
Resource reservation is the feature of circuit switching because path is fixed for data	There is no resource reservation because bandwidth is shared among users.

transmission.	
Circuit switching is more reliable.	Packet switching is less reliable.
Wastage of resources are more in Circuit Switching	Less wastage of resources as compared to Circuit Switching
It is not a store and forward technique.	It is a store and forward technique.
Transmission of the data is done by the source	Transmission of the data is done not only by the source, but also by the intermediate routers
Congestion can occur during connection establishment time	Congestion can occur during data transfer phase

* Note : Just explore above 3 switching on google little bit more .

Types of area networks – LAN, MAN and WAN

The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN, MAN and WAN are the three major types of the network designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e. **LAN** covers the smallest area; **MAN** covers an area larger than LAN and **WAN** comprises the largest of all.

There are other types of Computer Networks also, like :

- PAN (Personal Area Network)
- SAN (Storage Area Network)
- EPN (Enterprise Private Network)
- VPN (Virtual Private Network)

Local Area Network (LAN) –

LAN or Local Area Network connects network devices in such a way that personal computer and workstations can share data, tools and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP

protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.

Data transmits at a very fast rate as the number of computers linked are limited. By definition, the connections must be high speed and relatively inexpensive hardware (Such as hubs, network adapters and Ethernet cables). LANs cover smaller geographical area (Size is limited to a few kilometers) and are privately owned. One can use it for an office building, home, hospital, schools, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

Early LAN's had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. Propagation delay is very short in a LAN. The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. The

fault tolerance of a LAN is more and there is less congestion in this network. For example : A bunch of students playing Counter Strike in the same room (without internet).

Metropolitan Area Network (MAN) –

MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but resides in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need a high-speed connectivity. Speeds of MAN ranges in terms of Mbps. It's hard to design and maintain a Metropolitan Area Network.

The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN is moderate. Devices used for transmission of data through MAN are: Modem and Wire/Cable. Examples of a MAN are the part of the telephone company network that can provide a high-speed

DSL line to the customer or the cable TV network in a city.

Wide Area Network (WAN) –

WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. A WAN could be a connection of LAN connecting to other LAN's via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive.

There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN or Satellite Link. Due to long distance transmission, the noise and error tend to be more in WAN.

WAN's data rate is slow about a 10th LAN's speed, since it involves increased distance and increased number of servers and terminals etc. Speeds of WAN

ranges from few kilobits per second (Kbps) to megabits per second (Mbps). Propagation delay is one of the biggest problems faced here. Devices used for transmission of data through WAN are: Optic wires, Microwaves and Satellites. Example of a Switched WAN is the asynchronous transfer mode (ATM) network and Point-to-Point WAN is dial-up line that connects a home computer to the Internet.

Difference Between LAN, MAN and WAN

March 29, 2016 12 Comments

The Network allows computers to connect and communicate with different computers via any medium. LAN, MAN, and WAN are the three types of the network designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the significant differences is in the geographical area they cover, i.e. LAN covers the smallest area; MAN covers an area larger than LAN and WAN comprises the largest of all.

Furthermore, LAN networks rely on the hardware and communication devices owned by them for the transmission. As against, this could not be possible in case of MAN and WAN which are obliged to use public, private, leased communication hardware as

these networks are spanned across a magnificent area.

Content: LAN Vs MAN Vs WAN

Comparison Chart

BASIS OF COMPARISON	LAN	MAN	WAN
Expands to	Local Area Network	Metropolitan Area Network	Wide Area Network
Meaning	A network that connects a group of computers in a small geographical area.	It covers relatively large region such as cities, towns.	It spans large locality and connects countries together. Example Internet.
Ownership of Network	Private	Private or Public	Private or Public
Design and maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long

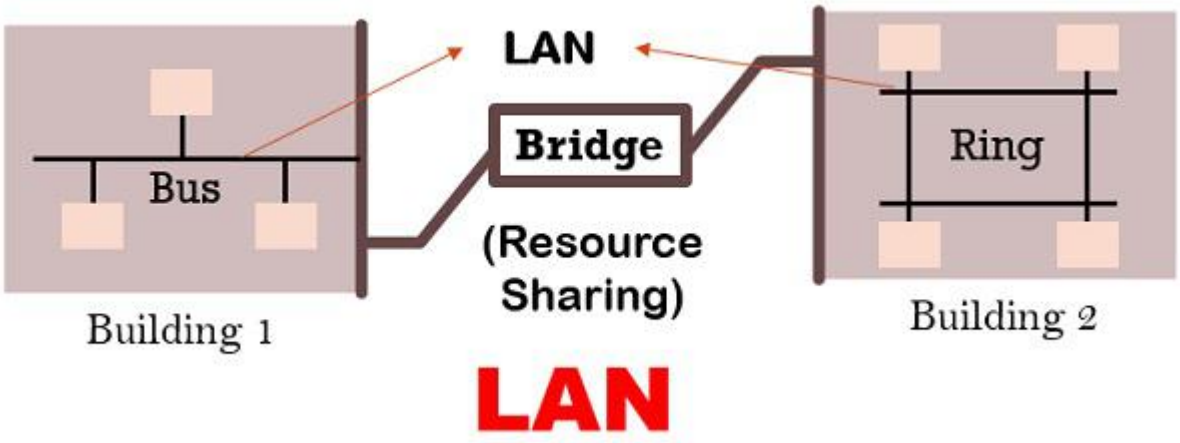
BASIS OF COMPARISON	LAN	MAN	WAN
Speed	High	Moderate	Low
Fault Tolerance	More Tolerant	Less Tolerant	Less Tolerant
Congestion	Less	More	More
Used for	College, School, Hospital.	Small towns, City.	Country/Continent.
Allows	Single pair of devices to communicate.	Multiple computers can simultaneously interact.	A huge group of computers communicate at the same time.

Definition of Local Area Network

LAN or Local Area Network links network devices in such a way that personal computer and workstations can share data, tools and programs. Data transmits at a very fast rate as the number of computers linked are limited. LAN's cover a smaller geographical area and are privately owned. One can use it for an office building, home, hospital, schools, etc. LAN is easy to design and maintain.

A Communication medium used for LAN has twisted pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized. LAN can be configured in the ring, bus and star topology. The ring topology is prevalent in the Token

Ring LANs of IBM and bus is widespread in Token Bus and Ethernet
LANs.

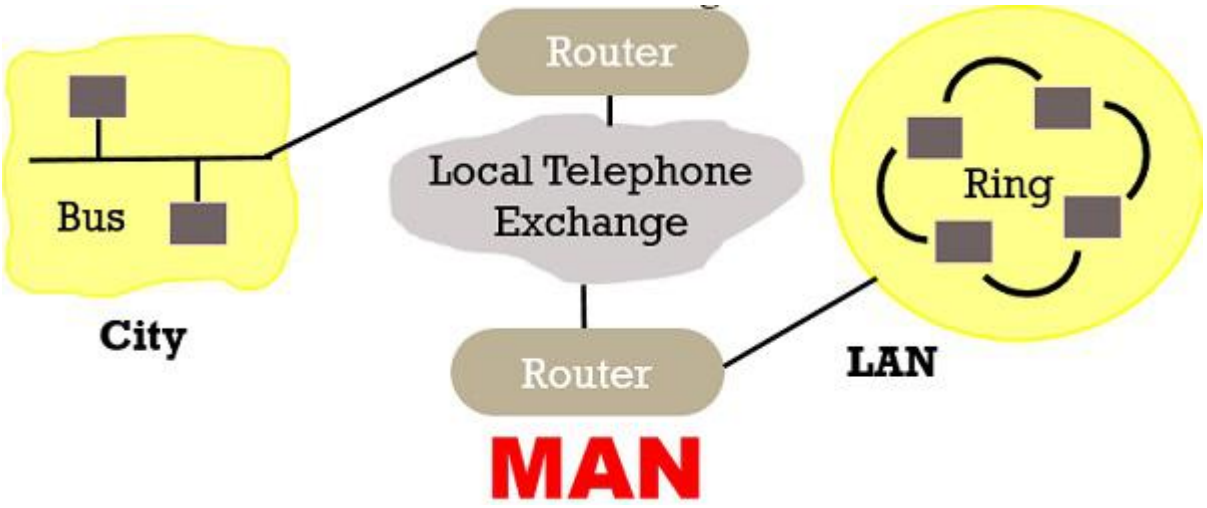


It is a **broadcast network** where the message is sent to all the connected hosts as all the host share the same transmission medium (wire). Broadcasting can be done in two ways statically and dynamically. In the **static technique**, the hosts are provided with a definite time slice for transmitting the information. While in the **dynamic method** the hosts can flexibly send the frame at any particular time.

Definition of Metropolitan Area Network

MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but resides in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). It's hard to design and maintain a Metropolitan Area

Network.



It is costly and may or may not be owned by a single organization. The data transfer rate of MAN is moderate.

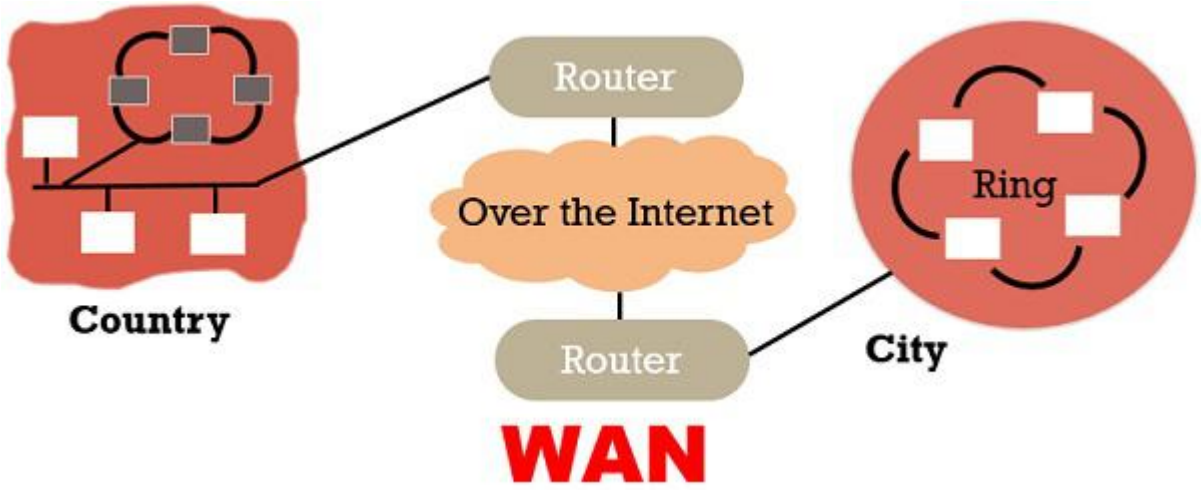
Types of MAN

MAN can be categorised into two types: DQDB and SMDS.

- **DQDB (Distributed Queue Dual Bus)**: It is considered as a dual bus configuration refers that each host in the network would be linked to the two backbone network lines.
- **SMDS (Switched Multimegabit Data Services)**: SMDS connects different LANs and permits packets to transfer to any other LAN on the SMDS. It is a high-speed MAN which uses packet switching as a datagram service.

WAN or Wide Area Network is a computer network that spans over a large geographical area. A WAN could be a connection of LAN connecting to other LAN's via telephone lines and radio waves.

Wide Area Network may or may not be privately owned. A Communication medium used for wide area network is PSTN or Satellite Link. Due to long distance transmission, the noise and error tend to be more in WAN. Propagation delay is one of the biggest problems faced
here.



Unlike LAN, WAN uses **switching** that allows multiple computers to connect with several switches instead of connecting with each other. It also uses the **store-and-forward** concept to transmit packets, where packets are stored in a buffer on a temporary basis then forwarded to the destination by following the predefined path.

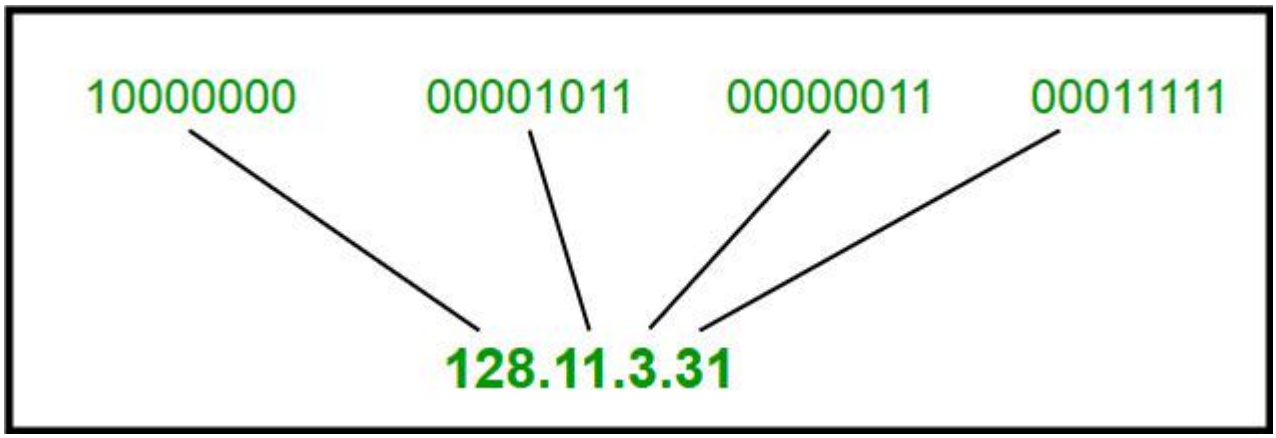
Key Differences Between LAN, MAN and WAN

1. The geographical area covered by LAN is small, whereas, MAN covers relatively large and WAN covers the greatest of all.
2. LAN is confined to schools, hospitals or buildings, whereas, MAN connects small towns or Cities and on the other hand, WAN covers Country or a group of Countries.
3. Devices used for transmission of data are-
   LAN: WiFi, Ethernet Cables.
   MAN: Modem and Wire/Cable
   WAN: Optic wires, Microwaves, Satellites.
4. LAN's transmit data at a faster rate than MAN and WAN.
5. Maintenance of LAN is easier than that of MAN and WAN.
6. The bandwidth available for transmission is higher in LAN than MAN and WAN.
7. Data transmission errors and noise are least in LAN, moderate in MAN and high in WAN.

IP Addressing

IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32 bit unique address having an address space of 232.
Generally, there are two notations in which IP address is written, dotted decimal notation and hexadecimal notation.

Dotted Decimal Notation



Hexadecimal Notation

Some points to be noted about dotted decimal notation :

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

Classful Addressing

The 32 bit IP address is divided into five sub-classes. These are:

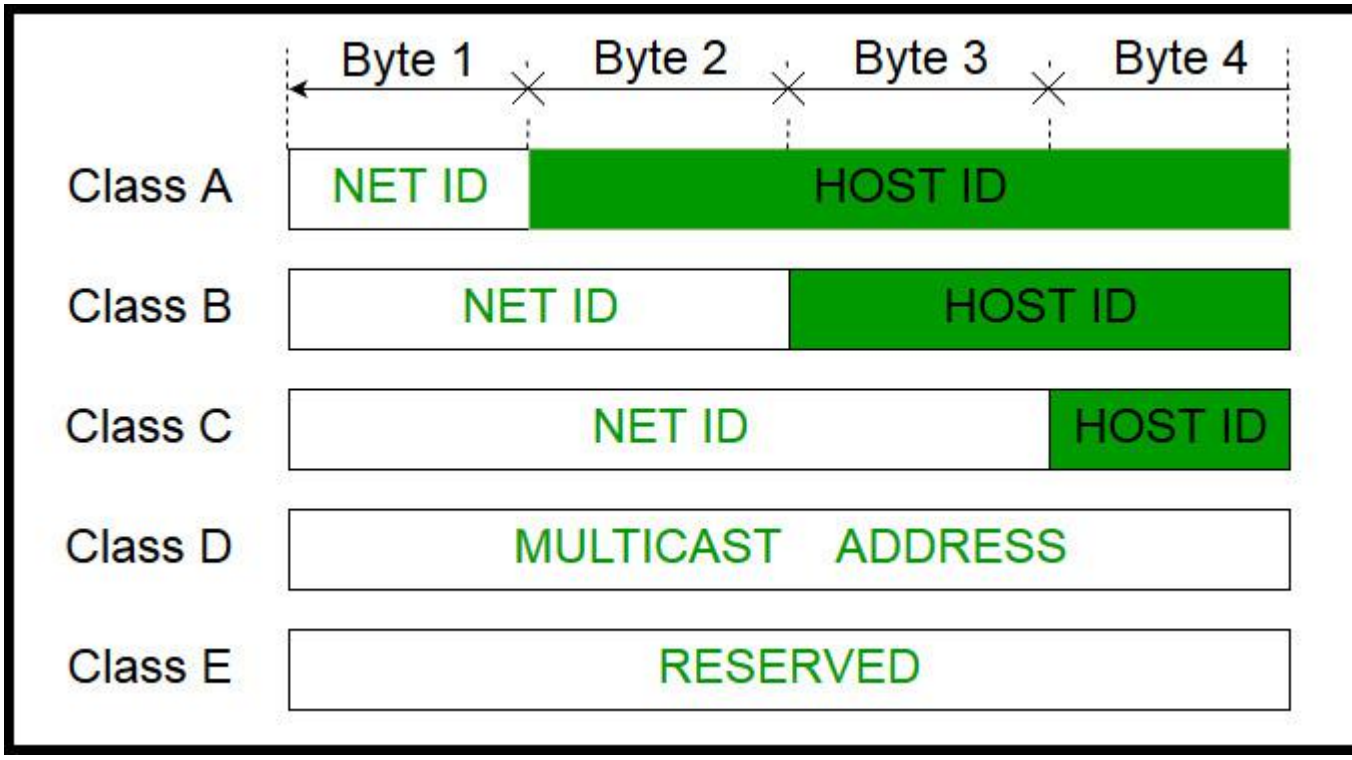
- Class A
- Class B
- Class C
- Class D

- Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address. IPv4 address is divided into two parts:

- **Network ID**
- **Host ID**

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns IP address to each device that is connected to its network.



Note: IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).

Note: While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

Class A:

IP address belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

The higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for class A is 255.x.x.x. Therefore, class A has a total of:

- 2^7-2= 126 network ID(Here 2 address is subracted because 0.0.0.0 and 127.x.y.z are special address.)
- 2^24 – 2 = 16,777,214 host ID

IP addresses belonging to class A ranges from 1.x.x.x – 126.x.x.x

Class B:

IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.

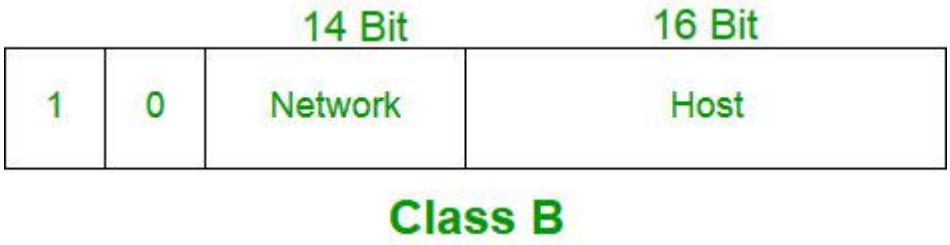
- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to

determine the host in any network. The default sub-net mask for class B is 255.255.x.x. Class B has a total of:

- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.



Class C :

IP address belonging to class C are assigned to small-sized networks.

- The network ID is 24 bits long.
- The host ID is 8 bits long.

The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:

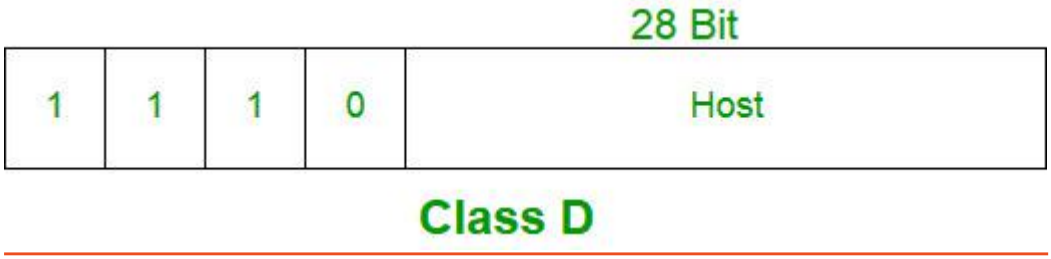
- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address

IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.

Class D :

IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.

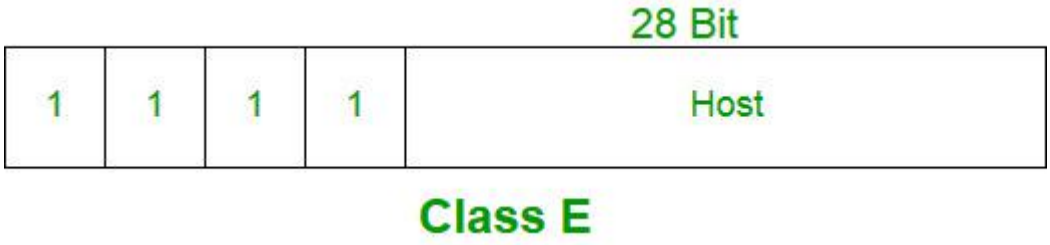
Class D does not posses any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.



Class E :

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254.

This class doesn't have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.



Rules for assigning Host ID:

Host ID's are used to identify a host within a network. The host ID are assigned based on the following rules:

- Within any network, the host ID must be unique to that network.
- Host ID in which all bits are set to O cannot be assigned because this host 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 reserved as a broadcast address to send packets to all the hosts present on that particular network.

Rules for assigning Network ID:

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network

ID. The network ID is assigned based on the following rules:

- The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loop-back functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Summary of Classful addressing :

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADD
CLASS A	0	8	24	2^7 (128)	2^{24}
CLASS B	10	16	16	2^{14} (16,384)	2^{16}
CLASS C	110	24	8	2^{21} (2,097,152)	2^8
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	

Problems with Classful Addressing:

The problem with this classful addressing method is that millions of class A address are wasted, many of the class B address are wasted, whereas, number of addresses available in class C is so small that it cannot cater the needs of organizations. Class D addresses are used for multicast routing and are

therefore available as a single block only. Class E addresses are reserved.

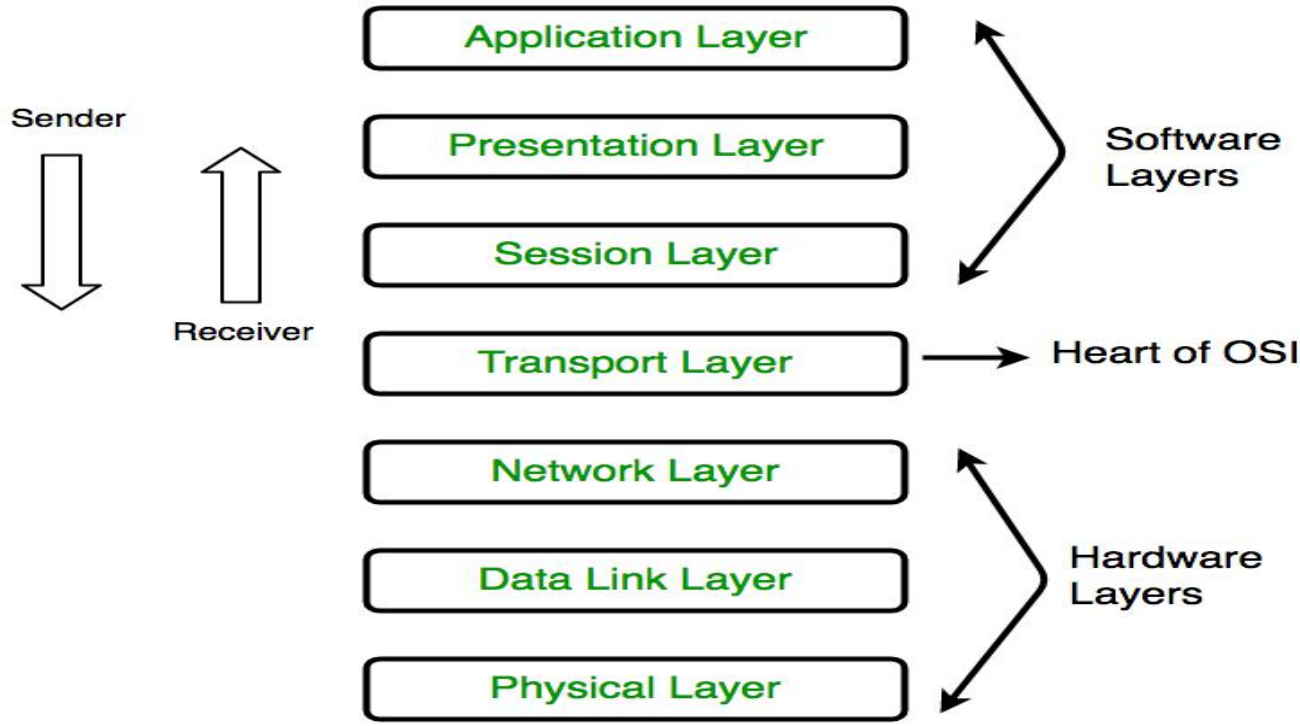
Since there are these problems, Classful networking was replaced by Classless Inter-Domain Routing (CIDR) in 1993. We will be discussing Classless addressing in next post.

* Note : Explore little bit more and specially classification of ips exam will give one ip and will ask this ip belongs to which class ? this type of questions will be there .

Layers of OSI Model :

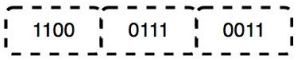
This is very Important topic for exam ccat read it carefully :

OSI stands for **Open Systems Interconnection**. It has been developed by ISO – '**International Organization of Standardization**', in the year 1974. 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.



1. Physical Layer (Layer 1) :

The lowest layer of the OSI reference model is the 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 the actual physical connection between the devices. When receiving data, this layer will get the signal received and convert it into Os and 1s and send them to the Data Link layer, which will put the frame back together.



The functions of the physical layer are :

1. **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

3. **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.
4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

* Hub, Repeater, Modem, Cables are Physical Layer devices.

** Network Layer, Data Link Layer and Physical Layer are also known as **Lower Layers** or **Hardware Layers**.

2. Data Link Layer (DLL) (Layer 2) :

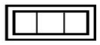
The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.

Data Link Layer is divided into two sub layers :

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

The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender 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.



The functions of the data Link layer are :

1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.

4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
5. **Access control:** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

* Packet in Data Link layer is referred as **Frame**.
** Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.
*** Switch & Bridge are Data Link Layer devices.

3. Network Layer (Layer 3) :

Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by network layer.
The functions of the Network layer are :

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
2. **Logical Addressing:** In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

* Segment in Network layer is referred as **Packet**.

✉

** Network layer is implemented by networking devices such as routers.

4. Transport Layer (Layer 4) :

Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End delivery of the complete message. Transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

• **At sender's side:**

Transport layer receives the formatted data from the upper layers, performs **Segmentation**and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.
Note: The sender need to know the port number associated with the receiver's application.
Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

- **At receiver's side:**

Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are :

1. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of

the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.

2. **Service Point Addressing:** In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by transport layer :

1. **Connection Oriented Service:** It is a three-phase process which include
   – Connection Establishment
   – Data Transfer
   – Termination / disconnection
   In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.
2. **Connection less service:** It is a one phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices.

Connection oriented Service is more reliable than connection less Service.

* Data in the Transport Layer is called as **Segments**.

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

5. Session Layer (Layer 5) :

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

The functions of the session layer are :

1. **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization** : This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.

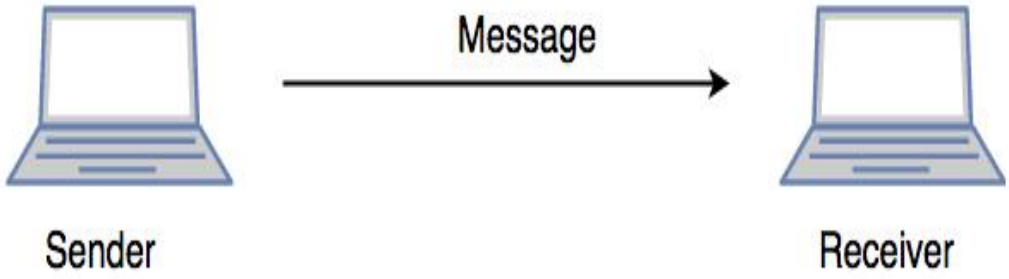
3. **Dialog Controller :** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

**All the below 3 layers(including Session Layer) are integrated as a single layer in TCP/IP model as "Application Layer".

Implementation of these 3 layers is done by the network application itself. These are also known as **Upper Layers or **Software Layers**.

SCENARIO:

Let's consider a scenario where a user wants to send a message through some Messenger application running in his browser. The "Messenger" here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data) and converted into bits (0's and 1's) so that it can be transmitted.



6. Presentation Layer (Layer 6) :

Presentation layer is also called the **Translation layer**.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
The functions of the presentation layer are :

1. **Translation** : For example, ASCII to EBCDIC.
2. **Encryption/ Decryption** : Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. **Compression:** Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7) :

At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information

to the user.

Ex: Application – Browsers, Skype Messenger etc.

**Application Layer is also called as Desktop Layer.

The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

OSI model acts as a reference model and is not implemented in Internet because of its late invention. Current model being used is the TCP/IP model.

TCP/IP Model :

Prerequisite – Layers of OSI Model

The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

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

The diagrammatic comparison of the TCP/IP and OSI model is as follows :

TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer

OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Difference between TCP/IP and OSI Model:

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both	OSI uses different

session and presentation layer in the application layer itself.	session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol

The first layer is the Process layer on the behalf of the sender and Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

1. Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.
We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

2. Internet 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 entire network. The main protocols residing at this layer are :

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:
   IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

3. Host-to-Host Layer -

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. Process Layer –

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. 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 carry out bank transactions.
2. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
3. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is	5. Transport Layer is both Connection

Connection Oriented.	Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are	10. In TCP/IP replacing protocol is

hidden in OSI model and are easily replaced as the technology changes.	not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers

Port Numbers (ftp,http,https,telnet,dns,pop) :

This is very large topic if you go so just do overview .

TCP and UDP

The Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are used to transmit network data to and from server and client applications. The main difference between the two protocols is that TCP uses a connection-oriented transport, while UDP uses a connectionless type of communication. When the TCP protocol is used, a special connection is opened up between two network devices, and the channel remains open to transmit data until it is closed.

On the other hand, a UDP transmission does not make a proper connection and merely broadcasts its data to the specified network address without any verification of receipt. For certain types of applications and services, a TCP connection makes more sense, while other types are more efficiently provided by UDP communication. The advantage of TCP is that the transmission is much more

reliable because it uses acknowledgement packets to ensure delivery. The advantage of UDP is that there is no connection, so it is much faster without all the checks and acknowledgements going on, but is also less reliable. In Table some common TCP/IP applications are shown with the type of protocol they use.

On this topic no more questions but just take a look on below notes :

http://dhost.com/list-of-commonly-used-port-numbers

Open above url and read that table 2,3 times u will get basic idea and thats enough for ccat.

Difference Between IPv4 and IPv6:

IPV4	IPV6
IPv4 has 32-bit address length	IPv6 has 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end	In IPv6 end to end

IPV4	IPV6
connection integrity is Unachievable	connection integrity is Achievable
It can generate 4.29×109 address space	Address space of IPv6 is quite large it can produce 3.4×1038 address space
Security feature is dependent on application	IPSEC is inbuilt security feature in the IPv6 protocol
Address representation of IPv4 in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation performed only by sender
In IPv4 Packet flow identification is not available	In IPv6 packetflow identification are Available and uses flow label field in the header
In IPv4 checksumfield	In IPv6 checksumfield is

IPV4	IPV6
is available	not available
It has broadcast Message Transmission Scheme	In IPv6 multicast and any cast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided

Differences between TCP and UDP

Prerequisite – Transport Layer responsibilities, TCP, UDP

TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a

TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
should close the connection after transmitting the data.	connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.
TCP is comparatively slower than UDP.	UDP is faster, simpler and more efficient

TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
	than TCP.
Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in User Datagram Protocol (UDP).
TCP header size is 20 bytes.	UDP Header size is 8 bytes.
TCP is heavy-weight.	UDP is lightweight.
TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.

Difference HTTP FTP SMTP :

PARAMETER	HTTP	FTP	SMTP
Port number	80	20 and 21	25
Type of band transfer	In-band	Out-of-band	In-band

PARAMETER	HTTP	FTP	SMTP
State	Stateless	Maintains state	-
Number of TCP connections	1	2 (Data Connection and Control Connection)	1
Type of TCP connection	Can use both Persistent and Non-persistent	Persistent for Control connection. Non-persistent for Data Connection	Persistent
Type of Protocol	Pull Protocol (Mainly)	-	Push Protocol (Primarily)
Type of Transfer	Transfer files between Web server and Web client	Transfer directly between computers	Transfers mails via Mail Servers

- *HTTP is stateless. A Stateless protocol implies that the HTTP Web Server does not maintains which request had originated from which user. Hence, to give a customized service to the user, HTTP uses Cookies.*

- FTP is Out-of-band, as it uses a separate channel to send data (Data connection), as to send control information (Control connection).
- As SMTP is much older that HTTP, it restricts all its messages to be in 7-bit ASCII format. Whereas HTTP has no such restriction.
- HTTP encapsulates each file in a different HTTP message. Whereas, SMTP places all the contents of a mail in a single message.

This is enough for ccat no need to go in very details because this subject has no further use in CDAC so study only for exam if you didn’ t understand any point go to google and clear your concept ..

!!!!All The Best Guys !!!!

** Some Important Notes For Operating Sys **

Guys Paging And segmentation is very important topic for ccat .

BASIS FOR COMPARISON	PAGING	SEGMENTATION
Basic	A page is of fixed	A segment is of

BASIS FOR COMPARISON	PAGING	SEGMENTATION
	block size.	variable size.
Fragmentation	Paging may lead to internal fragmentation.	Segmentation may lead to external fragmentation.
Address	The user specified address is divided by CPU into a page number and offset.	The user specifies each address by two quantities a segment number and the offset (Segment limit).
Size	The hardware decides the page size.	The segment size is specified by the user.
Table	Paging involves a page table that contains base address of each page.	Segmentation involves the segment table that contains segment number and offset (segment length).

Key Differences Between Paging and Segmentation

1. The basic difference between paging and segmentation is that a page is always of **fixed block size** whereas, a segment is of **variable size**.

2. Paging may lead to **internal fragmentation** as the page is of fixed block size, but it may happen that the process does not acquire the entire block size which will generate the internal fragment in memory. The segmentation may lead to **external fragmentation** as the memory is filled with the variable sized blocks.
3. In paging the user only provides a **single integer** as the address which is divided by the hardware into a **page number and Offset**. On the other hands, in segmentation the user specifies the address in two quantities i.e. **segment number and offset**.
4. The size of the page is decided or specified by the **hardware**. On the other hands, the size of the segment is specified by the **user**.
5. In paging, the **page table** maps the **logical address to the physical address**, and it contains base address of each page stored in the frames of physical memory space. However, in segmentation, the **segment table** maps the **logical address to the physical address**, and it contains segment number and offset (segment limit).

BASIS FOR COMPARISON	INTERNAL FRAGMENTATION	EXTERNAL FRAGMENTATION
Basic	It occurs when fixed sized memory blocks are allocated	It occurs when variable size memory space are

BASIS FOR COMPARISON	INTERNAL FRAGMENTATION	EXTERNAL FRAGMENTATION
	to the processes.	allocated to the processes dynamically.
Occurrence	When the memory assigned to the process is slightly larger than the memory requested by the process this creates free space in the allocated block causing internal fragmentation.	When the process is removed from the memory, it creates the free space in the memory causing external fragmentation.
Solution	The memory must be partitioned into variable sized blocks and assign the best fit block to the process.	Compaction, paging and segmentation.

Definition of Internal Fragmentation

Internal fragmentation occurs when the memory is divided into **fixed sized blocks**. Whenever a process request for the memory, the fixed sized block is allocated to the process. In case the memory assigned to the process is somewhat larger than the memory requested, then the difference

between assigned and requested memory is the **Internal fragmentation**.

This leftover space inside the fixed sized block can not be allocated to any process as it would not be sufficient to satisfy the request of memory by the process. Let us understand Internal fragmentation with the help of an example. The memory space is partitioned into the fixed-sized blocks of 18,464 bytes. Let us say a process request for 18,460 bytes and partitioned fixed-sized block of 18,464 bytes is allocated to the process. The result is 4 bytes of 18,464 bytes remained empty which is the internal fragmentation.

The overhead of keeping track of the internals hole created due to internal fragmentation is substantially more than the number of internal holes. The problem of internal fragmentation can be solved by **partitioning the memory into the variable sized block** and assign the best-sized block to a process requesting for the memory. Still, it will not totally eliminate the problem of internal fragmentation but will reduce it to some extent.

Definition of External Fragmentation

External fragmentation occurs when there is a sufficient amount of space in the memory to satisfy the memory request of a process. But the process's memory request can not be satisfied as the memory available is in a non-contiguous manner. Either you apply first-fit or best-fit memory allocation strategy it will cause external fragmentation.

When a process is loaded and removed from the memory the free space creates the hole in the memory space, and there are many such holes in the memory space, this is called External fragmentation. Although the first fit and best fit can affect the amount of external fragmentation, it can not be totally eliminated. **Compaction** may be the solution for external fragmentation.

Compaction algorithm shuffles all memory contents to one side and frees one large block of memory. But compaction algorithm is expensive. There is an alternative solution to solve external fragmentation issue which will allow a process to acquire physical memory in a non-contiguous manner. The techniques to achieve this solution are paging and segmentation.

Key Differences Between Internal and External fragmentation

1. The basic reason behind the occurrences of internal and external fragmentation is that internal fragmentation occurs when memory is partitioned into **fixed-sized blocks** whereas external fragmentation occurs when memory is partitioned into **variable size blocks**.
2. When the memory block allotted to the process comes out to be slightly larger than requested memory, then the free space left in the allotted memory block causes internal fragmentation. On the other hands, when the process is removed from the memory it creates free space

causing a hole in the memory which is called external fragmentation.

3. The problem of internal fragmentation can be solved by partitioning the memory into variable sized blocks and assign the best fit block to the requesting process. However, the solution for external fragmentation is compaction, but it is expensive to implement, so the processes must be allowed to acquire physical memory in a non-contiguous manner, to achieve this the technique of paging and segmentation is introduced.

BASIS FOR COMPARISON	PREEMPTIVE SCHEDULING	NON PREEMPTIVE SCHEDULING
Basic	The resources are allocated to a process for a limited time.	Once resources are allocated to a process, the process holds it till it completes its burst time or switches to waiting state.
Interrupt	Process can be interrupted in between.	Process can not be interrupted till it terminates or switches to waiting state.
Starvation	If a high priority process frequently arrives in the ready queue,	If a process with long burst time is running CPU, then another process with less CPU burst time may starve.

BASIS FOR COMPARISON	PREEMPTIVE SCHEDULING	NON PREEMPTIVE SCHEDULING
	low priority process may starve.	
Overhead	Preemptive scheduling has overheads of scheduling the processes.	Non-preemptive scheduling does not have overheads.
Flexibility	Preemptive scheduling is flexible.	Non-preemptive scheduling is rigid.
Cost	Preemptive scheduling is cost associated.	Non-preemptive scheduling is not cost associative.

Definition of Preemptive Scheduling

Preemptive scheduling is one which can be done in the circumstances when a process switches from **running state** to **ready state** or from **waiting state**to **ready state**. Here, the resources (CPU cycles) are allocated to the process for the **limited** amount of time and then is taken away, and the process is placed back in the ready queue again if it still has CPU burst time remaining. The process stays in ready queue till it gets next chance to execute.

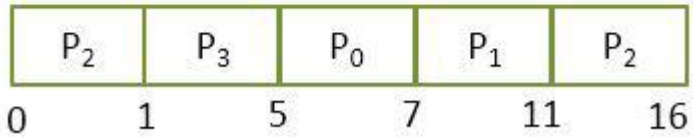
If a process with high priority arrives in the ready queue, it does not have to wait for the current process to complete its burst time. Instead, the

current process is interrupted in the middle of execution and is placed in the ready queue till the process with high priority is utilizing the CPU cycles. In this way, each process in the ready queue gets some time to run CPU. It makes the preemptive scheduling flexible but, increases the overhead of switching the process from running state to ready state and vise-verse.

Algorithms that work on preemptive scheduling are Round Robin. Shortest Job First (SJF) and Priority scheduling may or may not come under preemptive scheduling.

Let us take an example of Preemptive Scheduling, look in the picture below. We have four processes P0, P1, P2, P3. Out of which, P2 arrives at time 0. So the CPU is allocated to the process P2 as there is no other process in the queue. Meanwhile, P2 was executing, P3 arrives at time 1, now the remaining time for process P2 (5 milliseconds) which is larger than the time required by P3 (4 milli-sec). So CPU is allocated to processor

Process	Arrival Time	CPU Burst Time in millisec.
P_0	3	2
P_1	2	4
P_2	0	6
P_3	1	4



Preemptive Scheduling

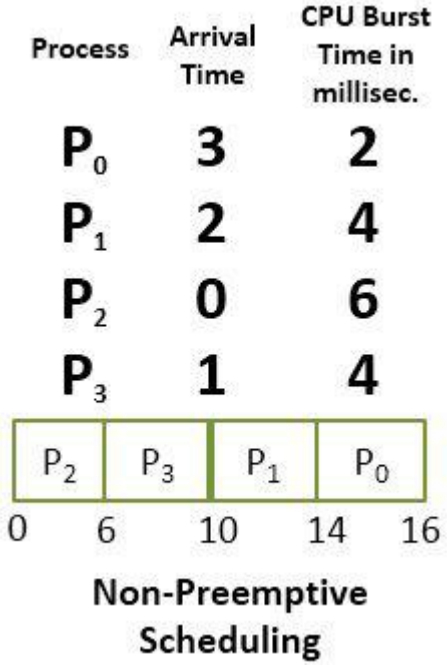
P3. Meanwhile, P3 was executing, process P1 arrives at time 2. Now the remaining time for P3 (3 milliseconds) is less than the time required by processes P1 (4 milliseconds) and P2 (5 milliseconds). So P3 is allowed to continue. While P3 is continuing process P0 arrives at time 3, now the remaining time for P3 (2 milliseconds) is equal to the time required by P0 (2 milliseconds). So P3 continues and after P3 terminates the CPU is allocated to P0 as it has less burst time than other. After P0 terminates, the CPU is allocated to P1 and then to P2.

Definition of Non-Preemptive Scheduling

Non-preemptive Scheduling is one which can be applied in the circumstances when a process **terminates**, or a process switches from **running** to **waiting state**. In Non-Preemptive Scheduling, once the resources (CPU) is allocated to a process, the process holds the CPU till it gets terminated or it reaches a waiting state.

Unlike preemptive scheduling, non-preemptive scheduling does not interrupt a process running CPU in middle of the execution. Instead, it waits for the process to complete its CPU burst time and then it can allocate the CPU to another process.

In Non-preemptive scheduling, if a process with long CPU burst time is executing then the other process will have to wait for a long time which increases the average waiting time of the processes in the ready queue. However, the non-preemptive scheduling does not have any overhead of switching the processes from ready queue to CPU but it makes the scheduling rigid as the process in execution is not even preempted for a process with higher



Non-Preemptive Scheduling

priority. Let us solve the above scheduling example in non-preemptive fashion. As initially the process P2 arrives at time 0, so CPU is allocated to the process P2 it takes 6 milliseconds to execute. In between all the processes i.e. P0, P1, P3 arrives into ready queue. But all waits till process P2 completes its CPU burst time. Then process that arrives after P2 i.e. P3 is then allocated the CPU till it

finishes it's burst time. Similarly, then P1 executes, and CPU is later given to process P0.

Key Differences Between Preemptive and Non-Preemptive Scheduling

1. The basic difference between preemptive and non-preemptive scheduling is that in preemptive scheduling the CPU is allocated to the processes for the **limited** time. While in Non-preemptive scheduling, the CPU is allocated to the process till it **terminates** or switches to **waiting state**.
2. The executing process in preemptive scheduling is **interrupted** in the middle of execution whereas, the executing process in non-preemptive scheduling is **not interrupted** in the middle of execution.
3. Preemptive Scheduling has the **overhead** of switching the process from ready state to running state, vise-verse, and maintaining the ready queue. On the other hands, non-preemptive scheduling has **no overhead** of switching the process from running state to ready state.
4. In preemptive scheduling, if a process with high priority frequently arrives in the ready queue then the process with low priority have to wait for a long, and it may have to starve. On the other hands, in the non-preemptive scheduling, if CPU is allocated to the process with larger burst time then the processes with small burst time may have to starve.

5. Preemptive scheduling is quite **flexible** because the critical processes are allowed to access CPU as they arrive into the ready queue, no matter what process is executing currently. Non-preemptive scheduling is **rigid** as even if a critical process enters the ready queue the process running CPU is not disturbed.
6. The Preemptive Scheduling is cost associative as it has to maintain the integrity of shared data which is not the case with Non-preemptive Scheduling.

* Note :Read Carefully all differences that will clear your confusions ..

BASIS FOR COMPARISON	FORK()	VFORK()
Basic	Child process and parent process has separate address spaces.	Child process and parent process shares the same address space.
Execution	Parent and child process execute simultaneously.	Parent process remains suspended till child process completes its execution.
Modification	If the child process alters any page in the address space, it is invisible to the	If child process alters any page in the address space, it is visible to the

BASIS FOR COMPARISON	FORK()	VFORK()
	parent process as the address space are separate.	parent process as they share the same address space.
Copy-on-write	fork() uses copy-on-write as an alternative where the parent and child shares same pages until any one of them modifies the shared page.	vfork() does not use copy-on-write.

Key Differences Between fork() and vfork()

1. The primary difference between fork and vfork is that the child process created by the **fork** has a **separate memory space** from the parent process. However, the child process created by the **vfork** system call shares the **same address space** of its parent process.
2. The child process created using fork **execute simultaneously**with the parent process. On the other hand, child process created using vfork **suspend** the execution of parent process till its execution is completed.
3. As the memory space of parent and child process is separate modification done by any of the processes does not affect other's pages. However, as the parent and child process shares the same memory address modification done by any process reflects in the address space.

4. The system call fork() uses **copy-on-write** as an alternative, which let child and parent process share the same address space until any one of them modifies the pages. On the other hand, the vfork does not use copy-on-write.

BASIS FOR COMPARSION	DEADLOCK	STARVATION
Basic	Deadlock is where no process proceeds, and get blocked.	Starvation is where low priority processes get blocked, and high priority process proceeds.
Arising condition	The occurrence of Mutual exclusion, Hold and wait, No preemption and Circular wait simultaneously.	Enforcement of priorities, uncontrolled resource management.
Other name	Circular wait.	Lifelock.
Resources	In deadlocked, requested resources are blocked by the other processes.	In starvation, the requested resources are continuously used by high priority processes.
Prevention	Avoiding mutual exclusion, hold and wait, and circular	Aging.

BASIS FOR COMPARSION	DEADLOCK	STARVATION
	wait and allowing preemption.	

Key Differences Between Deadlock and Starvation in OS

1. In a deadlock, none of the processes proceeds for execution, each process get blocked waiting for the resources acquired by the another process. On the other hand, starvation is a condition where the processes that possess higher priority is allowed to acquire the resources continuously by preventing the low priority processes to acquire resources resulting in indefinite blocking of low priority processes.
2. Deadlock arises when four conditions **Mutual exclusion, Hold and wait, No preemption, and Circular wait** occurs simultaneously. However, starvation occurs when process **priorities have been enforced** while allocating resources, or there is uncontrolled resource management in the system.
3. Deadlock is often called by the name **circular wait** whereas, the starvation is called **Lived lock**.
4. In Deadlock the resources are blocked by the process whereas, in starvation, the processes are continuously being used by the processes with high priorities.

5. Deadlock can be prevented by the avoiding the conditions like mutual exclusion, Hold and wait, and circular wait and by allowing the preemption of the processes that are holding resources for a long time. On the other hand, Starvation can be prevented by**aging**.

BASIS FOR COMPARISON	SEMAPHORE	MUTEX
Basic	Semaphore is a signalling mechanism.	Mutex is a locking mechanism.
Existence	Semaphore is an integer variable.	Mutex is an object.
Function	Semaphore allow multiple program threads to access a finite instance of resources.	Mutex allow multiple program thread to access a single resource but not simultaneously.
Ownership	Semaphore value can be changed by any process acquiring or releasing the resource.	Mutex object lock is released only by the process that has acquired the lock on it.
Categorize	Semaphore can be categorized into counting semaphore and binary semaphore.	Mutex is not categorized further.

BASIS FOR COMPARISON	SEMAPHORE	MUTEX
Operation	Semaphore value is modified using wait() and signal() operation.	Mutex object is locked or unlocked by the process requesting or releasing the resource.
Resources Occupied	If all resources are being used, the process requesting for resource performs wait() operation and block itself till semaphore count become greater than one.	If a mutex object is already locked, the process requesting for resources waits and queued by the system till lock is released.

Thats it guys I gave very detail notes and trust me this is more than enough to get good rank in cdac ccat .

Any Confusion I am always available email me call me text me whatever you want ..

!!!!! All The Best Again !!!