Government Polytechnic Kotabagh(Nainital)

(Branch- computer science and engg)

Subject –Computer network Sem - 4th Year -2nd year

NETWORK BASIS

Defination-A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network

Type of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time.

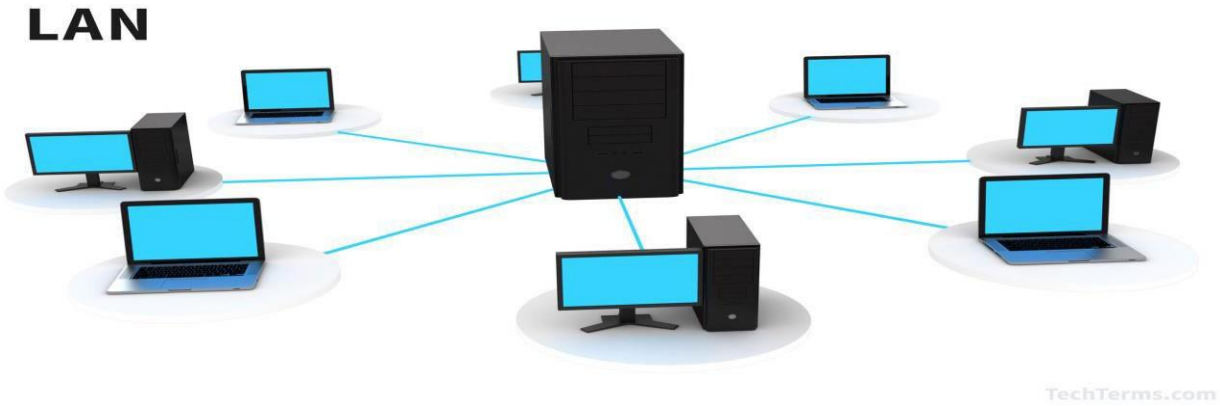
There are two possible types of connections: point-to-point and multipoint. 1

Point-to-Point -A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint- A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatiallyor temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

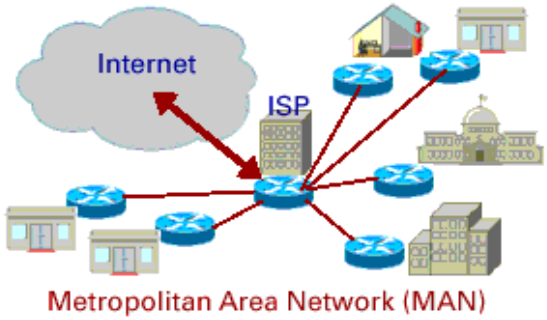
LAN (local area network)

Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometres in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information. LANs are distinguished from other kinds of networks by three characteristics: (1) Their size, (2) Their transmission technology, and (3) Their topology. LANs are restricted in size,



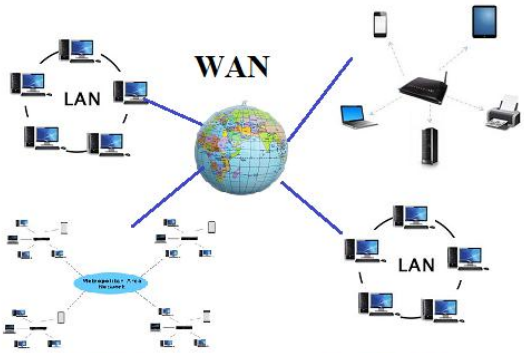
MAN (METROPOLITAN AREA NETWORK)

A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities



WAN(Wide Area Network)

- Wide area network provides long distance transmission of data. The size of the WAN is larger than LAN and MAN. A WAN can cover country, continent or even a whole world. Internet connection is an example of WAN. Other examples of WAN are mobile broadband connections such as 3G, 4G etc
- It is cheaper and more efficient to use the phone network for the link.
- Most WAN networks are used to transfer large blocks of data between its users.



Wide area network (WAN)

Advantages of WAN:

Centralized infrastructure: One of the main advantage of WAN is the that we do not need to maintain the backup and store data on local system as everything is stored online on a data centre, from where we can access the data through WAN.

Privacy: We can setup the WAN in such a way that it encrypts the data that we share online that way the data is secure and minimises the risk of unauthorized access.

Increased Bandwidth: With the WAN we get to choose the bandwidth based on the need, a large organization can have larger bandwidth that can carry large amount of data faster and efficiently.

Area: A WAN can cover a large area or even a whole world though internet connection thus we can connect with the person in another country through WAN which is not possible is other type of computer networks.

Disadvantages of WAN:

Antivirus: Since our systems are connected with the large amount of systems, there is possibility that we may unknowingly download the virus that can affect our system and become threat to our privacy and may lead to data loss.
Expensive: Cost of installation is very high.
Issue resolution: Issue resolution takes time as the WAN covers large area, it is really difficult to pin point the exact location where the issues raised and causing the proble

Peer to Peer network

a peer-to-peer (P2P) network is created when two or more PCs are connected and share resources without going through a separate server computer. A P2P network can be an ad hoc connection—a couple of

computers connected via a Universal Serial Bus to transfer files. A P2P network also can be a permanent infrastructure that links a half-dozen computers in a small office over copper wires. Or a P2P network can be a network on a much grander scale in which special protocols and applications set up direct relationships among users over the Inter

.

Advantages of Peer to Peer network

Some advantages of peer to peer computing are as follows:

- the network is quite easy to set up and maintain.
- It is easy to scale the peer to peer network and add more nodes. This only increases the data sharing capacity of the system.
- None of the nodes in the peer to peer network are dependent on the others for their functioning.

Disadvantages of Peer to Peer network:

- It is difficult to backup the data as it is stored in different computer systems and there is no central server.
- It is difficult to provide overall security in the peer to peer network as each system is independent and contains its own data.

Client server netework

- A client and server networking model is a model in which computers such as servers provide the network services to the other computers such as clients to perform a user based tasks. This model is known as client-server networking model.

- The application programs using the client-server model should follow the given below strategies: An application program is known as a client program, running on the local machine that requests for a service from an application program known as a server program, running on the remote machine.
- A client program runs only when it requests for a service from the server while the server program runs all time as it does not know when its service is required.
- A server provides a service for many clients not just for a single client. Therefore, we can say that client-server follows the many-to-one relationship. Many clients can use the service of one server.
- Services are required frequently, and many users have a specific client-server application program. For example, the client-server application program allows the user to access the files, send e-mail, and so on. If the services are more customized, then we should have one generic application program that allows the user to access the services available on the remote computer.

Advantages of Client-server networks:

- **Centralized:** Centralized back-up is possible in client-server networks, i.e., all the data is stored in a server.
- **Security:** These networks are more secure as all the shared resources are centrally administered.
- **Performance:** The use of the dedicated server increases the speed of sharing resources. This increases the performance of the overall system.

- **Scalability:** We can increase the number of clients and servers separately, i.e., the new element can be added, or we can add a new node in a network at any time.

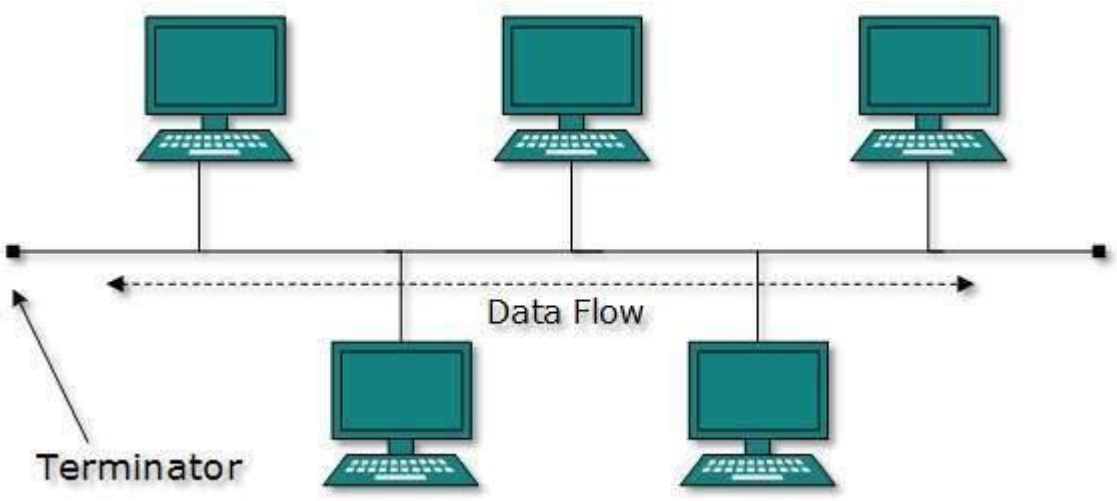
Disadvantages of Client-Server network:

- **Traffic Congestion** is a big problem in Client/Server networks. When a large number of clients send requests to the same server may cause the problem of Traffic congestion.
- It does not have a robustness of a networkA client/server network is very decisive. Sometimes, regular computer hardware does not serve a certain number of clients. In such situations, specific hardware is required at the server side to complete the work.

- Sometimes the resources exist in the server but may not exist in the client. For example, If the application is web, then we cannot take the print out directly on printers without taking out the print view window on the web.

Topologoies

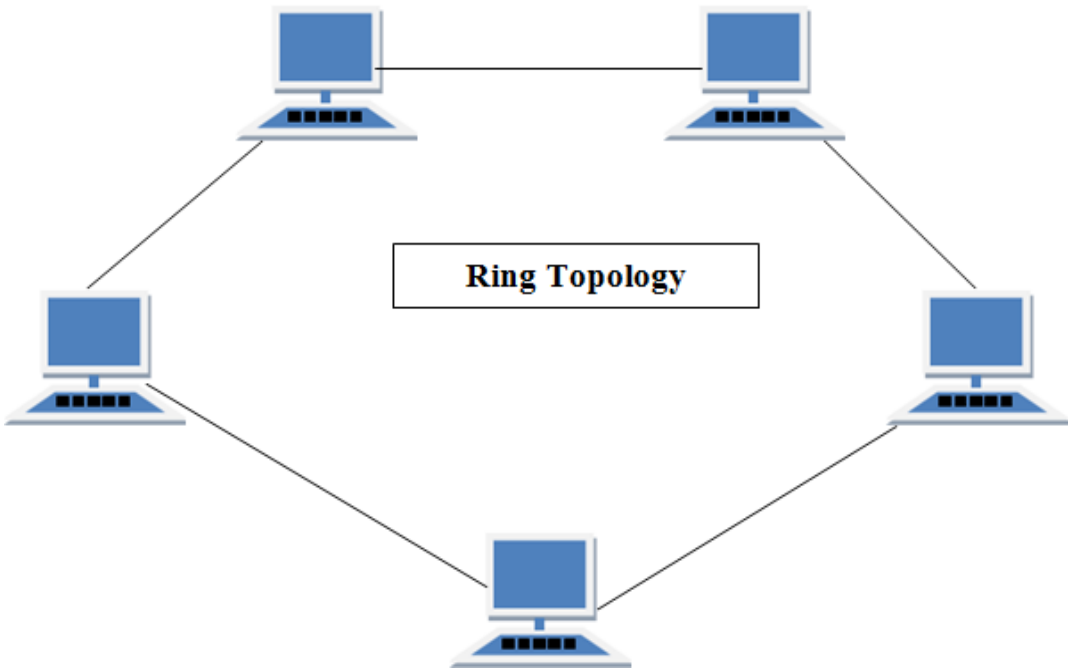
In case of Bus topology, all devices share single communication line or cable.Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.



Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.

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

- 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.
- The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.

Advantages of Ring Topology

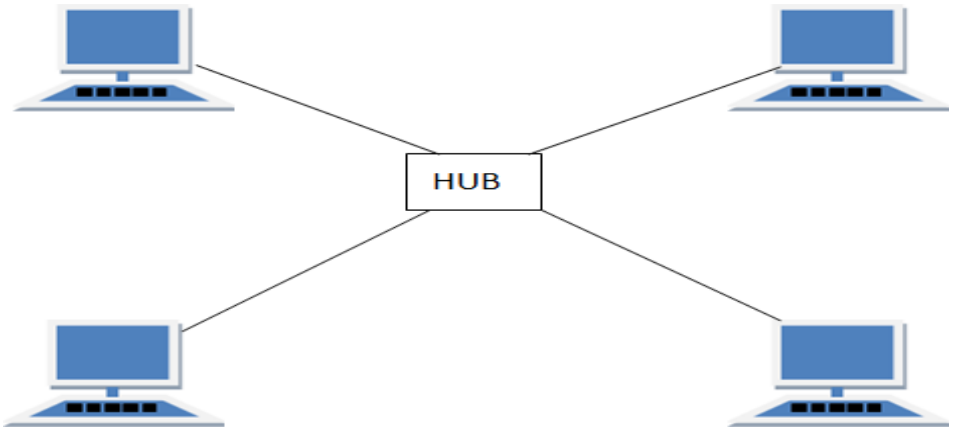
- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- Cheap to install and expand

Disadvantages of Ring Topology

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

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

- Every node has its own dedicated connection to the hub.
- Hub acts as a repeater for data flow.

- Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

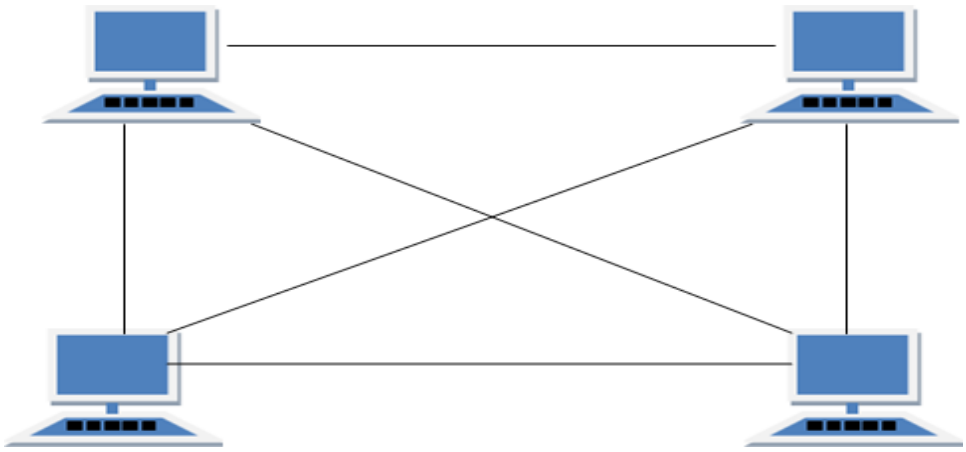
- Fast performance with few nodes and low network traffic.
- Hub can be upgraded easily.
- Easy to troubleshoot.
- Easy to setup and modify.

Disadvantages of Star Topology

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

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.



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

- Fully connected.
- Robust.
- Not flexible.

Advantages of Mesh Topology

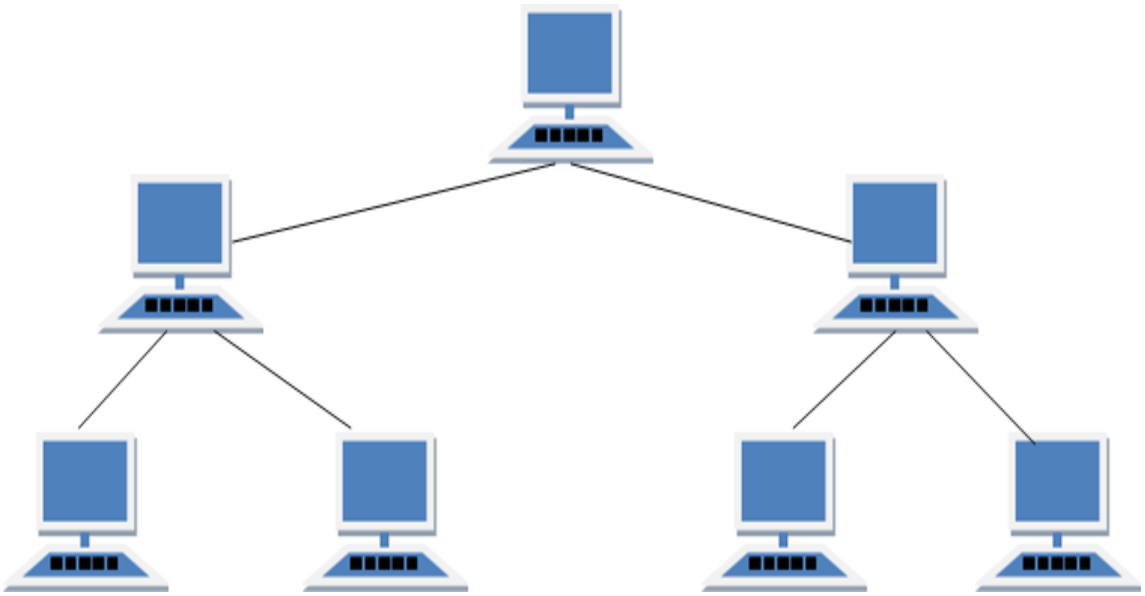
- Each connection can carry its own data load.
- It is robust.
- Fault is diagnosed easily

Disadvantages of Mesh Topology

- Installation and configuration is difficult.
- Cabling cost is more.
- Bulk wiring is required.

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

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

Advantages of Tree Topology

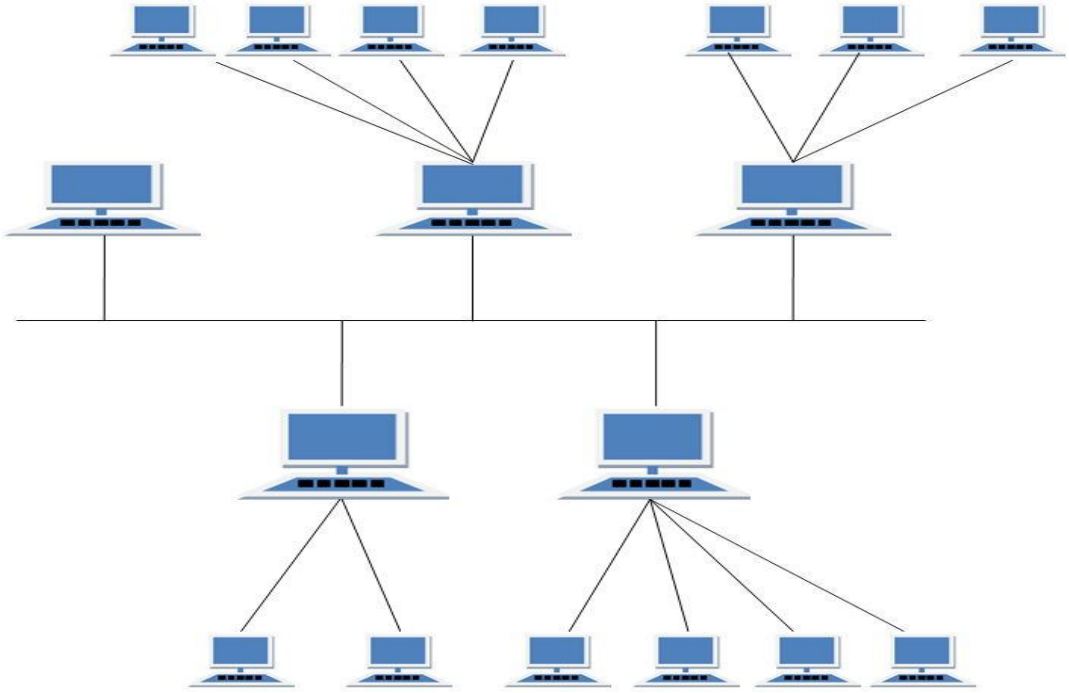
- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.

Disadvantages of Tree Topology

- Heavily cabled.
- Costly.
- If more nodes are added maintenance is difficult.
- Central hub fails, network fails.

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

- It is a combination of two or topologies
- Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

- Reliable as Error detecting and trouble shooting is easy.
- Effective.
- Scalable as size can be increased easily.
- Flexible.

Disadvantages of Hybrid Topology

- Complex in design.
- Costly.

Switching technologies

Circuit switching: it is a technique that directly connects the sender and the receiver in an unbroken path.

- Telephone switching equipment, for example, establishes a path that connects the caller's telephone to the receiver's telephone by making a physical connection.

- With this type of switching technique, once a connection is established, a dedicated path exists between both ends until the connection is terminated.

- Routing decisions must be made when the circuit is first established, but there are no decisions made after that time

- Circuit switching in a network operates almost the same way as the telephone system works.

- A complete end-to-end path must exist before communication can take place.

Advantages:

- The communication channel (once established) is dedicated.

Disadvantages:

- Possible long wait to establish a connection, (10 seconds, more on long- distance or international calls.) during which no data can be transmitted.

- More expensive than any other switching techniques, because a dedicated path is required for each connection.

- Inefficient use of the communication channel, because the channel is not used when the connected systems are not using it.

Packet Switching:

Packet Switching

• Packet switching can be seen as a solution that tries to combine the advantages of message and circuit switching and to minimize the disadvantages of both.

• There are two methods of packet switching: Datagram and virtual circuit.

• In both packet switching methods, a message is broken into small parts, called packets.

• Each packet is tagged with appropriate source and destination addresses.

• With current technology, packets are generally accepted onto the network on a first-come, first-served basis. If the network becomes overloaded, packets are delayed or discarded (``dropped").

• In packet switching, the analog signal from your phone is converted into a digital data stream. That series of digital bits is then divided into relatively tiny clusters of bits, called packets.

• Datagram packet switching is similar to message switching in that each packet is a self-contained unit with complete addressing information attached.

• This fact allows packets to take a variety of possible paths through the network.

• So the packets, each with the same destination address, do not follow the same route, and they may arrive out of sequence at the exit point node (or the destination).

• Reordering is done at the destination point based on the sequence number of the packets.

• It is possible for a packet to be destroyed if one of the nodes on its way is crashed momentarily. Thus all its queued packets may be lost.

• In the virtual circuit approach, a preplanned route is established before any data packets are sent.

• A logical connection is established when a sender send a "call request packet" to the receiver and the receiver send back an acknowledge packet "call accepted packet" to the sender if the receiver agrees on conversational parameters.

Advantages:

• Packet switching is cost effective, because switching devices do not need massive amount of secondary storage.

• Packet switching offers improved delay characteristics, because there are no long messages in the queue (maximum packet size is fixed).

• Packet can be rerouted if there is any problem, such as, busy or disabled links.

•The advantage of packet switching is that many network users can share the same channel at the same time. Packet switching can maximize link efficiency by making optimal use of link bandwidth.

Disadvantages:

• Protocols for packet switching are typically more complex.

• It can add some initial costs in implementation.

• If packet is lost, sender needs to retransmit the data. Another disadvantage is that packet-switched systems still can't deliver the same quality as dedicated circuits in applications requiring very little delay - like voice conversations or moving images.

Message Switching

• With message switching there is no need to establish a dedicated path between two stations.

• When a station sends a message, the destination address is appended to the message.

• The message is then transmitted through the network, in its entirety, from node to node.

• Each node receives the entire message, stores it in its entirety on disk, and then transmits the message to the next node.

• This type of network is called a store-and-forward network.

A message-switching node is typically a general-purpose computer. The device needs sufficient secondary-storage capacity to store the incoming messages, which could be long. A time delay is introduced using this type of scheme due to store- and-forward time, plus the time required to find the next node in the transmission path.

Advantages:

• Channel efficiency can be greater compared to circuit-switched systems, because more devices are sharing the channel.

• Traffic congestion can be reduced, because messages may be temporarily stored in route.

• Message priorities can be established due to store-and-forward technique.

- Message broadcasting can be achieved with the use of broadcast address appended in the message

Disadvantages

- Message switching is not compatible with interactive applications.

- Store-and-forward devices are expensive, because they must have large disks to hold potentially long messages

GOVERNMENT POLYTECHNIC KOTABAGH
OSI MODELS

Established in 1947, the International Standards Organization(ISO) is a multinational body dedicated to world wide agreement on international standards .An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. It was first introduced in the late 1970s .An open system is a set of protocols that all owes any two different system to communicate regardless of the underlying architecture. The purpose of the OSI mode list show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software

Layer	Function	Example
Application (7)	Services that are used with end user applications	SMTP,
Presentation (6)	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
Session (5)	Establishes/ends connections between two hosts	NetBIOS, PPTP
Transport (4)	Responsible for the transport protocol and error handling	TCP, UDP
Network (3)	Reads the IP address form the packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the data packet	Switches
Physical (1)	Send data on to the physical wire.	Hubs, NICS, Cable

Layer 7: Physical Layer

The lowest layer of the OSI model is concerned with data communication in the form of electrical, optic, or electromagnetic signals physically transmitting information between networking devices and infrastructure. The Physical Layer is essentially responsible for the communication of unstructured raw data streams over a physical medium. It defines a range of aspects associated with the electrical, mechanical, and physical systems and networking devices

that include the specifications; e.g. cable size, signal frequency, voltages, etc.; topologies such as Bus, Star, Ring, and Mesh; communication modes such as Simplex, Half Duplex, and Full Duplex; data Transmission Performance e.g. Bit Rate and Bit Synchronization; as well as modulation, switching, and interfacing with the physical transmission medium as described here. Common protocols include Wi-Fi, Ethernet, and others as listed here. The hardware includes networking devices, antennas, cables, modem, intermediate devices such as repeaters and hubs.

Layer 6: Data Link Layer

The second layer of the OSI model concerns data transmission between the nodes within a network and manages the connections between physically connected devices such as switches. The raw data received from the physical layer is synchronized and packaged into data frames that contain the necessary protocols to route information between appropriate nodes. The Data Link Layeris further divided into two sublayers: Logical Link Control (LLC) sublayer responsible for flow controls and error controls that ensure error-free and accurate data transmission between the network nodes; and the Media Access Control (MAC) sublayer responsible for managing access and permissions to transmit data between the network nodes. The data is transmitted sequentially and the layer expects acknowledgement for the encapsulated raw data sent between the nodes.

Layer 5: Network Layer

The third layer of the OSI model organizes and transmits data between multiple networks. This layer is responsible for routing the data via the best physical path based on a range of factors including network characteristics, best available path, traffic controls, congestion of data packets, and priority of service, among others. The network layer implements logical addressing for data packets to distinguish between the source and destination networks. Other functions at the Network Layer include encapsulation and fragmentation, as well as congestion controls and error handling. The outgoing data is divided into packets and incoming data is reassembled into information that is consumable at a higher application level. Network Layer hardware includes routes, bridge routers, 3-layer switches, and protocols such as Internet (IPv4) Protocol version 4 and Internet Protocol version 6 (IPv6).

Layer 4: Transport Layer

The fourth layer of the OSI model ensures complete and reliable delivery of data packets. The Transport Layer provides mechanisms such as error control, flow control, and congestion control to keep track of the data packets, check for errors and duplication, and resend the information that fails delivery. It involves the service-point addressing function to ensure that the packet is sent in response to a specific process (via a port address). Packet Segmentation and reassembly ensure that the data is divided and sequentially sent to the destination where it is rechecked for integrity and accuracy based on the receiving sequence. Common protocols include the Transmission Control Protocol (TCP) for connection-oriented data transmission and User Datagram Protocol (UDP) for connectionless data transmission.

Layer 3: Session Layer

The Session Layer manages sessions between servers to coordinate the communication – as the first of the top three OSI model layers that deal with the software level. Session refers to any interactive data exchange between two entities within a network. Common examples include HTTPS sessions that allow Internet users to visit and browse websites for a specific time period. The Session Layer is responsible for a range of functions including opening, closing, and re-establishing session activities, authentication and authorization of communication between specific apps and servers, identifying full-duplex or half-duplex operations, and synchronizing data streams. Common Session Layer protocols include Remote procedure call protocol (RPC), Point-to-Point Tunneling Protocol (PPTP), Session Control Protocol (SCP), and Session Description Protocol (SDP) as described here.

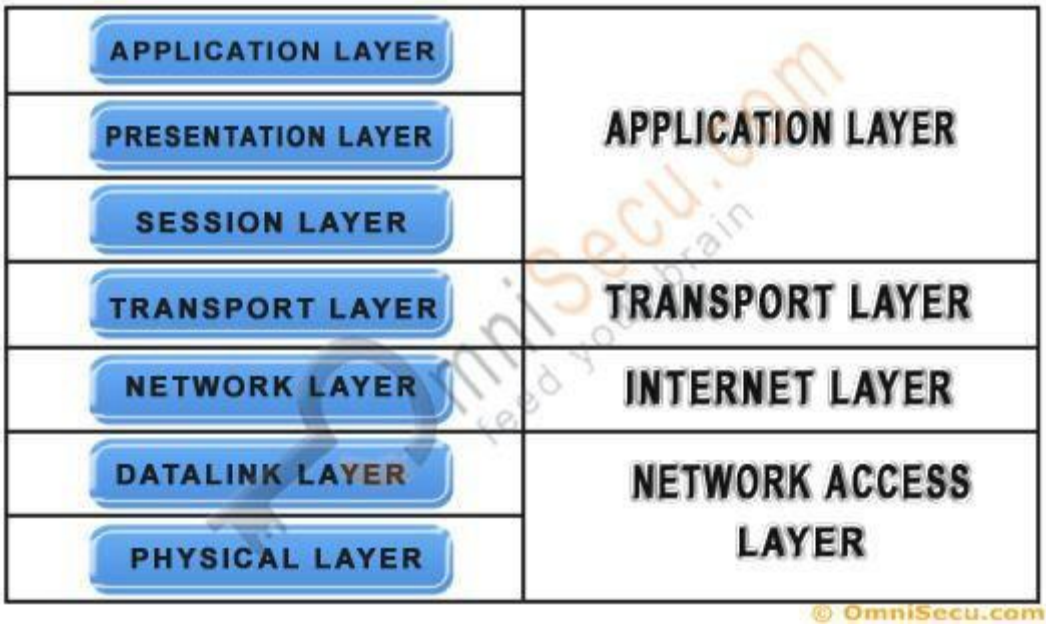
Layer 2: Presentation Layer

The sixth layer of the OSI model converts data formats between applications and the networks. Responsibilities of the Presentation Layer include data conversion, character code translation, data compression, encryption and decryption. The Presentation Layer, also called the Syntax Layer, maps the semantics and syntax of the data such that the received information is consumable for every distinct network entity. For example, the data we transfer from our encryption-based communication app is formatted and encrypted at this layer before it is sent across the network. At the receiving end, the data is decrypted and formatted into text or media information as originally intended.

Layer 1: Application Layer

The Application Layer concerns the networking processes at the application level. This layer interacts directly with end-users to provide support for email, network data sharing, file transfers, and directory services, among other distributed information services. The upper most layer of the OSI model identifies networking entities to facilitate networking requests by end-user requests, determines resource availability, synchronizes communication, and manages application-specific networking requirements. The Application Layer also identifies constraints at the application level such as those associated with authentication, privacy, quality of service, networking devices, and data syntax. The most common Application Layer protocols include File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and Domain Name System (DNS).

TCP/IP



Layer 4: Application layer

is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3: Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2: Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagrams, which contain source and destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks. The Internet layer is also responsible for routing of IP datagrams.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1: Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

4. NETWORK ARCHITECTURE

Ethernet

Definition: **Ethernet** is a computer network technology which is used in different area networks like LAN, MAN, WAN. *Ethernet* connecting computers together with cable so the computers can share information. Within each main branch of the network, "Ethernet" can connect up to 1,024 personal computers and workstations. *Ethernet provides services on the Physical (Layers 1) and Data Link Layer (Layers 2) of OSI reference model.*The Data Link Layer is further divided into two sublayers that are Logical Link Control (LLC) and Media Access Control (MAC),these sublayers can be used to establish the transmission paths and format data before transmiting on the same network segment.

Systems that use ethernet communication divide their data into packets, which are also known as frames. These frames further contain source and destination address, a mechanism which was used to detect errors in the data and retransmission requests.

Ethernet Specification and Standardisation

Fast Ethernet

The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds. This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure. Fast Ethernet provides faster throughput for video, multimedia, graphics, Internet surfing and stronger error detection and correction.

There are three types of Fast Ethernet:
100BASE-TX for use with level 5 UTP cable; 100BASE- FX for use with fiber-optic cable; and 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable. The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard.

Network managers who want to incorporate Fast Ethernet into an existing configuration are required to make many decisions. The number of users in each site on the network that need the higher throughput must be determined; which segments of the backbone need to be reconfigured specifically for 100BASE-T; plus what hardware is necessary in order to connect the 100BASE-T segments with existing 10BASE-T segments. Gigabit Ethernet is a future technology that promises a migration path beyond Fast Ethernet so the next generation of networks will support even higher data transfer speeds.

Gigabit Ethernet was developed to meet the need for faster communication networks with applications such as multimedia and Voice over IP (VoIP). Also known as "gigabit-Ethernet-over-copper" or 1000Base-T, GigE is a version of Ethernet that runs at speeds 10 times faster than 100Base-T. It is defined in the IEEE 802.3 standard and is currently used as an enterprise backbone. Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone to interconnect high performance switches, routers and servers.

From the data link layer of the OSI model upward, the look and implementation of Gigabit Ethernet is identical to that of Ethernet. The most important differences between Gigabit Ethernet and Fast Ethernet include the additional support of full duplex operation in the MAC layer and the data rates.

5. Network Connectivity

Hub A network hub is a node that broadcasts data to every computer or Ethernet-based device connected to it. A hub is less sophisticated than a switch, the latter of which can isolate data transmissions to specific devices.

Network hubs are best suited for small, simple local area network (LAN) environments. Hubs cannot provide routing capabilities or other advanced network services. Because they operate by forwarding packets across all ports indiscriminately, network hubs are sometimes referred to as "dumb switches."

With limited capabilities and poor scalability, network hubs had primarily one competitive advantage over switches: lower prices. As switch prices fell in the early to mid-2000s, hubs began getting phased out of use. Today, hubs are far less commonly deployed. But network hubs have some niche uses and continue to offer a simple means of networking.Hub falls in two categories:

Active Hub: They are smarter than the passive hubs. They not only provide the path for the data signals infact they regenerate, concentrate and strengthen the signals before sending them to their destinations. Active hubs are also termed as ‘repeaters’.

Passive Hub: They are more like point contact for the wires to built in the physical network. They have nothing to do with modifying the signals.

switch

A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The 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.

GATEWAY

Gateway is a node (router) in a computer network, a key *stopping point* for data on its way to or from other networks. Thanks to gateways, we are able to communicate and send data back and forth. The Internet wouldn't be any use to us without gateways (as well as a lot of other hardware and software).

In a workplace, the gateway is the computer that routes traffic from a workstation to the outside network that is serving up the Web pages. For basic Internet connections at home, the gateway is the Internet Service Provider that gives you access to the entire Internet.

A node is simply a physical place where the data stops for either transporting or reading/using. (A computer or modem is a node; a computer cable isn't.) Here are a few node notes:

- On the Internet, the node that's a stopping point can be a gateway or a host node.
- A computer that controls the traffic your Internet Service Provider (ISP) receives is a node.

When a computer-server acts as a gateway, it also operates as a firewall and a proxy server. A firewall keeps out unwanted traffic and outsiders off a private network. A proxy server is software that "sits" between programs on your computer that you use (such as a Web browser) and a computer server—the computer that serves your network. The proxy server's task is to make sure the real server can handle your online data requests.

Bridges

A bridge in a computer network connects with other bridge networks that utilize a similar protocol. These network devices work at the data link layer in an OSI model to connect two different networks and provide communication between them. Similar to hubs and repeaters, bridges broadcast data to each node. But, maintains the MAC (media access control) address table to find out new segments. So following transmissions are transmitted to the preferred receiver

The main functions of bridges in a computer network include the following.

- This networking device is used for dividing local area networks into several segments.
- In the OSI model, it works under the data link layer.
- It is used to store the address of MAC in PC used in a network and also used for diminishing the network traffic.

Advantages/Disadvantages of Bridge in Computer Network

The advantages are

- It acts as a repeater to extend a network
- Network traffic on a segment can be reduced by subdividing it into network communications
- Collisions can be reduced.
- Some types of bridges connect the networks with the help of architectures & types of media.
- Bridges increase the available bandwidth to individual nodes because fewer network nodes share a collision domain
- It avoids waste BW (bandwidth)
- The length of the network can be increased.
- Connects different segments of network transmission

The disadvantages are

- It is unable to read specific IP addresses because they are more troubled with the MAC addresses.
- They cannot help while building the network between the different architectures of networks.
- It transfers all kinds of broadcast messages, so they are incapable to stop the scope of messages.
- These are expensive as we compare with repeaters
- It doesn't handle more variable & complex data load which occurs from WAN.