Unit 2: Introduction to Computer Networks[5 Hrs.]

2.1 Definitions, Uses, Benefits

2.2 Network Topologies and its types (Bus, Star, Ring, Mesh, Hybrid,…)

2.3 Types of Computer Networks (PAN, LAN, MAN, WAN, CAN,…)

2.4 Networking Types (Client/Server, P2P)

2.5 Overview of Protocols and Standards

2.6 OSI Reference Model

2.7 TCP/IP Models and its Comparison with OSI

2.8 Networking Hardware: NIC, Hub, Repeater, Switch, Bridge, Router)

2.9 Basic Networking Command

2.1 Definitions, Uses, Benefits

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.
A computer network is a set of connected computers. Computers on a network are called nodes. The connection between computers can be done via cabling, most commonly the Ethernet cable, or wirelessly through radio waves. Connected computers can share resources, like access to the Internet, printers, file servers, and others.
Uses and benefits of a computer network:

1. File sharing: Networking of computers helps the network users to share data files.

2. Hardware sharing: Users can share devices such as printers, scanners, CD-ROM drives, hard drives etc. Without computer networks, device sharing is not possible.

3. Application sharing: Applications can be shared over the network, and this allows implementing client/server applications.

4. User communication: Networks allow users to communicate using e-mail, newsgroups, and video conferencing etc.

5. Network gaming: A lot of network games are available, which allow multi-users to play from different locations.

6. Voice over IP (VoIP): Voice over Internet Protocol (IP) is a revolutionary change in telecommunication which allows to send telephone calls (voice data) using standard Internet Protocol (IP) rather than by traditional PSTN.

2.2 Network Topologies and its types (Bus, Star, Ring, Mesh, Hybrid,…)

Network Topology

In communication networks, a topology is a usually schematic description of the arrangement of a network, including its nodes and connecting lines. There are two ways of defining network geometry: the physical topology and the logical (or signal) topology. It defines the shape of communication network. There are five common types of network Topologies:

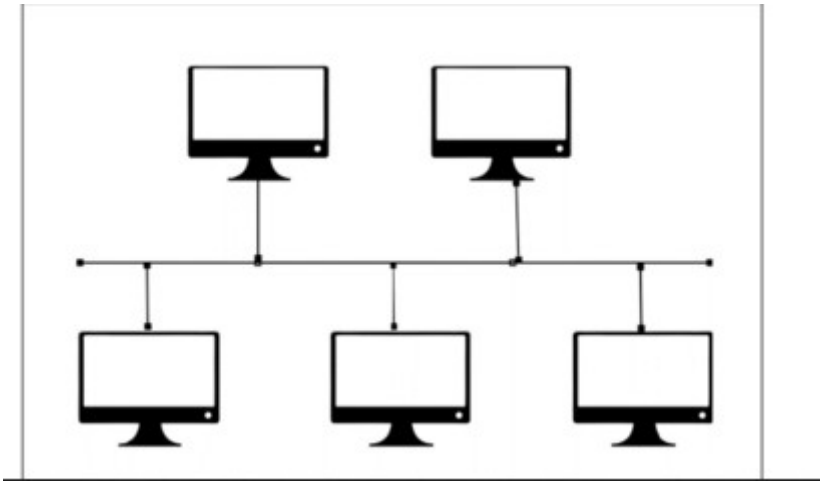
1. Bus Topology
2. Ring Topology
3. Star Topology
4. Tree Topology
5. Mesh Topology

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.

In linear bus topology, all computers are connected by a single length of cabling with a terminator at each end. The bus topology is the simplest and most widely used network design.

Bus networks are the most common LANs. They have no switches, and in their simplest form, no repeaters, but simply share a common linear communication medium.



Features of Bus Topology

It transmits data only in one direction.

Every device is connected to a single cable

Advantages of Bus Topology

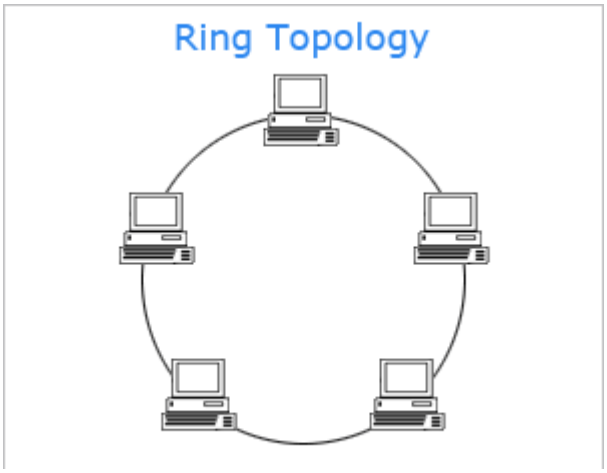
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

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 neighbor for each device. In ring topology the computers are arranged in a circle. Data travels around the ring in one direction, with each device on the ring acting as a repeater. Ring Networks typically use a Token Passing Protocol. The layout is similar to linear bus, except that the nodes are connected in a circle using cable segments. Each node passes information along to the next, until it reaches at its intended destination.The ring topology is usually found in peer-to-peer (PCs connected in pairs) networks, in which each machine manages both information processing and distribution of data files.



Features of Ring Topology

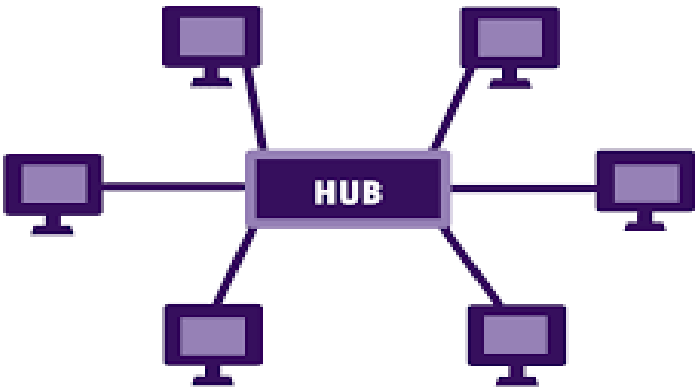
1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. 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.
3. 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 Star Topology, all the cables run from the computers to a central location, where they are connected by a hub. Hub is a device used to extend a network so that additional work stations can be attached.
In Star topology each node is connected to single centrally located server, using its own dedicated segment of cable. A star topology is a LAN architecture in which endpoints on the network are connected to a common central hub, or switch, by dedicated links. In this topology each node is connected to a centralized switch by a dedicated physical link. The switch provides a path between any two devices wishing to communicate, either physically in a circuit switch or logically in a packet switch.



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 Fiber or coaxial cable.

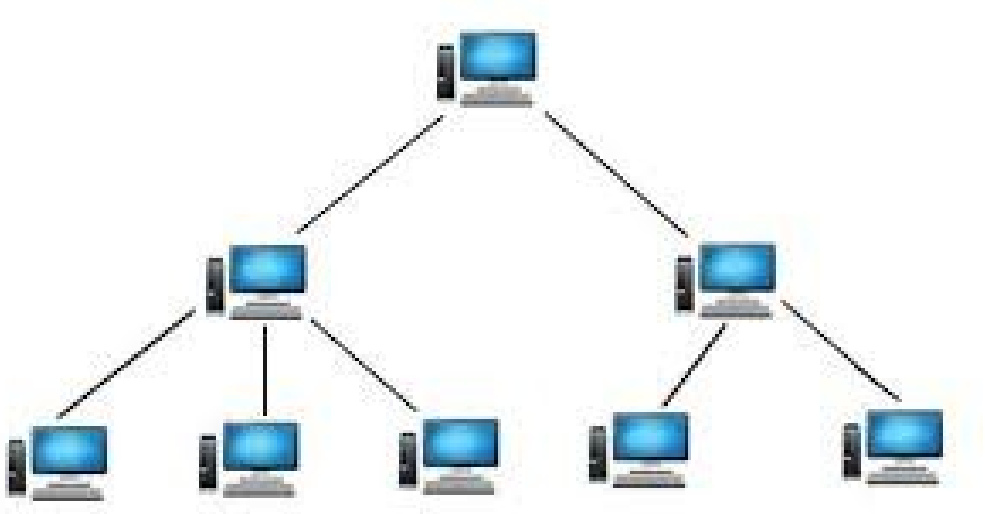
Advantages of Star Topology
1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.

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. 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.
This is a network topology containing zero or more nodes/computers linked together in a hierarchical fashion. The topmost node is called the root. The root may have zero or more child nodes, connected by edges (links); the root is the parent root to its children. Each node can have in turn zero or more nodes of its own. Nodes sharing the same parents are called siblings. Every node in the tree has exactly one parent node (except root which has no parents), and all nodes in the tree are descendants of the root node. These relationships ensure that there is one and only one path from one node to any other node in the tree. Tree topology LAN architecture is identical to BUS topology network, except that branches with multiple nodes are possible in this case.
The advantages and disadvantages of Tree topology
are same as that of Bus Topology.



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.

5. Mesh Topology

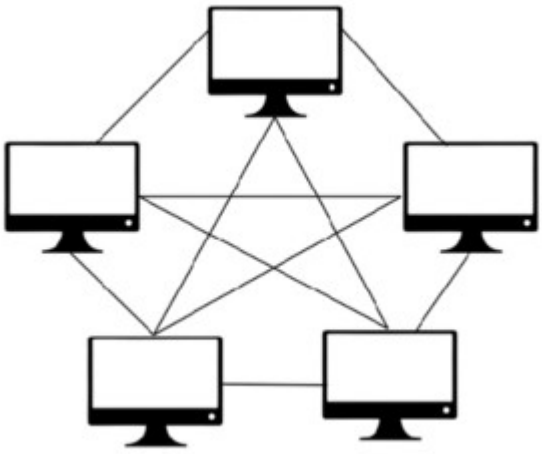
In this topology, two or more nodes are connected together in an arbitrary fashion. Any two nodes in a Mesh or Graph may or may not be connected by a link. Not all the nodes need to be connected

in a graph, but if the path can be traced between any two nodes, the graph is a connected one.
A Mesh Topology is a Mixture of BUS topology, STAR Topology, Ring and Tree Topology, with no restriction of connection among all the nodes in a network.
The mesh network topology employs either of two schemes, called full mesh and partial mesh.
In the full mesh topology, each workstation is connected directly to each of the others. In the partial mesh topology, some workstations are connected to all the others, and some are connected only to those other nodes with which they exchange the most data.

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.

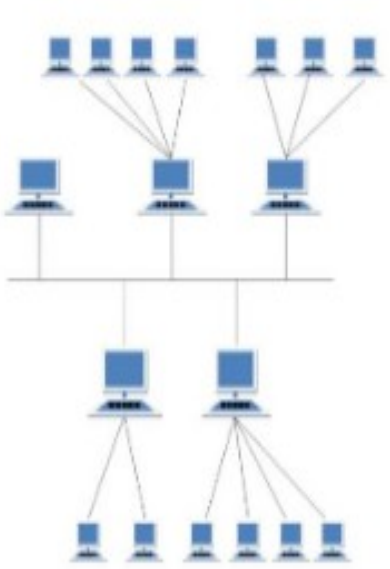


Features of Mesh Topology
1. Fully connected.
2. Robust.
3. Not flexible.

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.

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.

2.3 Types of Computer Networks (PAN, LAN, MAN, WAN, CAN,…)

There are many ways in which different networks can be classified, such as their size, capabilities and the geographical distance they cover. Generally, networks are distinguished based on their geographical span. A network can be as small as distance between your mobile phone and its Bluetooth headphone and as large as the internet itself, covering the whole geographical world.

1. Local Area Network (LAN)

A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN). Usually, LAN covers an organization' offices, schools, colleges or universities. Number of systems connected in LAN may vary from as least as two to as much as 16 million.
LAN provides a useful way of sharing the resources between end users. The resources such as printers, file servers, scanners, and

internet are easily sharable among computers. LANs are composed of inexpensive networking and routing equipment. It may contain local servers serving file storage and other locally shared applications. LAN can be wired, wireless, or in both forms at once.

2. Metropolitan Area Network (MAN)

The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network. It can be in the form of Ethernet, Token-ring, ATM, or Fiber Distributed Data Interface (FDDI). Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city. MAN works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or internet. This is a network which is larger than a LAN but smaller than a WAN, and incorporates elements of both. It typically spans a town or city and is owned by a single person or company, such as a local council or a large company.

3. Wide Area Network (WAN)

WAN networks connect computers together over large physical distances, remotely connecting them over one huge network and allowing them to communicate even when far apart. The Internet is a WAN, and connects computers all around the world together. LANs connect to WANs, such as the internet, using routers to transfer data and information quickly and securely. WANs are usually too large to be controlled by one administrator, and so usually have collective ownership, or in the case of the internet, are publicly owned. WAN may use advanced technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and Synchronous Optical Network (SONET).

4. Personal Area Network (PAN)

PAN is the most basic type of computer network. It is a type of network designed to connect devices within a short range, typically around one person. It allows your personal devices, like smartphones, tablets, laptops, and wearables, to communicate and share data with each other. PAN offers a network range of 1 to 10 meters from person to device providing communication. Its transmission speed is very high with very easy maintenance and very low cost.
Examples of PAN are Bluetooth connection between a phone and wireless earbuds , Infrared communication between TV and remote.

3. Campus Area Network (CAN)

CAN is bigger than a LAN but smaller than a MAN. This is a type of computer network that is usually used in places like a school or colleges. This network covers a limited geographical area that is, it spreads across several buildings within the campus. CAN mainly use Ethernet technology with a range of few kilometers. Its transmission speed is very high with a moderate maintenance cost and moderate cost.
Examples of CAN are networks that cover schools, colleges, buildings, etc.

2.4 Networking Types (Client/Server, P2P)

Client-Server Model
A client-server network is designed for end-users, called clients, to access resources such as files, songs, video collections, or some other service from a central computer called a server. A server's sole purpose is to do what its name implies - serve its clients!

The type of computing system, in which one powerful workstation serves the requests of other systems, is an example of client server technology. Once the server has fulfilled the client's request, the connection is terminated. Your Web browser is a client program that has requested a service from a server; in fact, the service and resource the server provided is the delivery of this Web page.

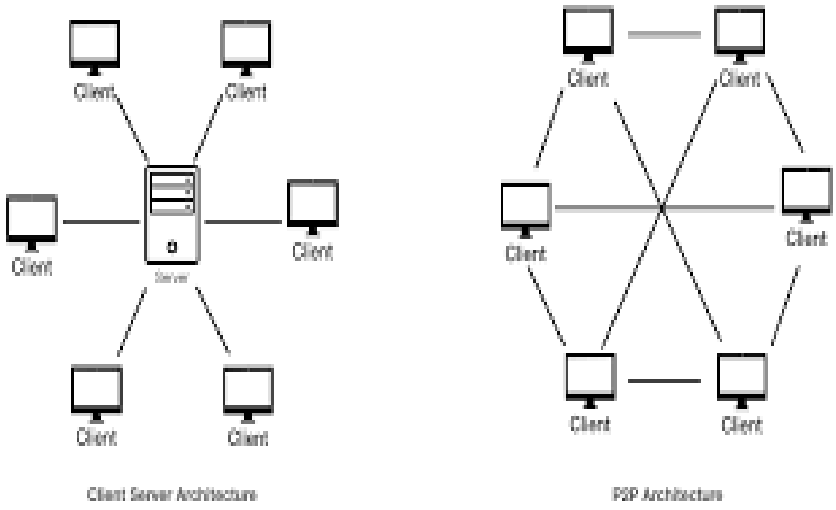
• It is also known as centralized computing.

• In this type of system, multiple computers are joined to one powerful mainframe computer.

• The server or mainframe computer has huge storage and processing capabilities.

• The computers that are connected to the mainframe or server are called Clients or Nodes.

• These nodes are not connected to each other; they are only connected to server.



Client Server Architecture

P2P Architecture

Peer-to-Peer Network Model (P2P)

In its simplest form, 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. Peer-to-peer networks are quite common in small offices that do not use a dedicated file

server. All client versions of Windows, Mac and Linux can function as nodes in a peer-to-peer network and allow their files to be shared.
It is easy to install and so is the configuration of computers on this network. P2P is more reliable as central dependency is eliminated. Failure of one peer doesn't affect the functioning of other peers.
In case of Client –Server network, if server goes down whole network gets affected. The over-all cost of building and maintaining this type of network is comparatively very less.
In this network, the whole system is decentralized thus it is difficult to administer. Security in this system is very less viruses, spywares, Trojans, etc. Malwares can easily transmit over this P-2-P architecture.
Peer-to-peer (P2P) is a decentralized communications model in which each party has the same capabilities and either party can initiate a communication session. Unlike the client/server model, in which the client makes a service request and the server fulfills the request, the P2P network model allows each node to function as both a client and server.

2.5 Overview of Protocols and Standards

Protocols and Standards in Computer Networking
A protocol is a set of rules which define:

- How to establish communication between the machines
- The format of any data which is to be exchanged between the machines
- How errors in the data will be detected
- How errors will be corrected
- Methods of compressing the data to transmit it faster and more efficiently
- How the connection between the machines is to be terminated

Network standards are also ground rules that are set by commissions so that hardware is compatible among similar computers and assures interoperability. This is done to ensure that backwards compatibility and compatibility from vendor to vendor. It is necessary to have standards because if each company had its own protocol standards and didn't allow it to talk with other protocols there would be a lack of communication from different machines and would result in one company being hugely successful and the other running out of business due to lack of being able to communicate with other machines.

Connection Oriented Protocols

These protocols require that a logical connection be established between two devices before transferring data. This is generally accomplished by following a specific set of rules that specify how a connection should be initiated, negotiated, managed and eventually terminated. Usually one
device begins by sending a request to open a connection, and the other responds. They pass control information to determine if and how the connection should be set up. If this is successful, data is sent between the devices. When they are finished, the connection is broken. The process is much like a telephone call, where a virtual circuit is established--the caller must know the person's telephone number and the phone must be answered--before the message can be delivered. TCP is an example of a connection-oriented protocol.

Connection less Protocols

Connectionless protocols, in contrast, allow data to be exchanged without setting up a link between processes. These protocols do not establish a connection between devices. As soon as a device has data to send to another, it just sends it. Each unit of data, with

all the necessary information to route it to the intended destination, is transferred independent of other data packets and can travel over different paths to reach the final destination. Some data packets might be lost in transmission or might arrive out of sequence to other data packets. UDP is a connectionless protocol. It is known as a datagram protocol because it is analogous to sending a letter where you don't acknowledge receipt.

2.6 OSI Reference Model

OSI (Open Systems Interconnection) is reference model for how applications can communicate over a network. A reference model is a conceptual framework for understanding relationships.

The OSI reference model architecture divides network communication into seven layers. The seven layers of function are provided by a combination of applications, operating systems, network card device drivers and networking hardware that enable a system to put a signal on a network cable or out over Wi-Fi or other wireless protocol). Each layer covers different network activities, equipment, or protocols. The OSI layers may be summarized by:

1. Physical Layer:

The physical layer is the actual cable, fibers, cards, switches, and other mechanical and electrical equipment that make up a network. This is the layer that transforms digital data into signals that can be sent down a wire to transmit data. These signals are often electrical but, as in the case of fiber optics, they can also be non-electrical signals such as optics or any other type of pulse that can be digitally encoded. It activates, maintain and deactivate the physical connection. Voltages and data rates needed for

transmission is defined in the physical layer. It converts the digital bits into electrical signal.

2. Data Link Layer:

Data link layer synchronizes the information which is to be transmitted over the data. Error controlling is easily done. The encoded data are then passed to physical. Error detection bits are used by the data link on layer. It also corrects the errors. Outgoing messages are assembled into frames. Then the system waits for the acknowledgements to be received after the transmission. It is reliable to send message. This layer has two sub-layers, the Logical Link Control Layer and the Media Access Control Layer.

3. The Network Layer:

It routes the signal through different channels to the other end. It acts as a network controller. It decides by which route data should take. It divides the outgoing messages into packets and to assemble incoming packets into messages for higher levels. This layer also determines the route from the source to the destination computer. It determines which path the data should take based on network conditions, priority of service, and other factors. It also manages traffic problems on the network, such as switching and routing of packets and controlling the congestion of data.

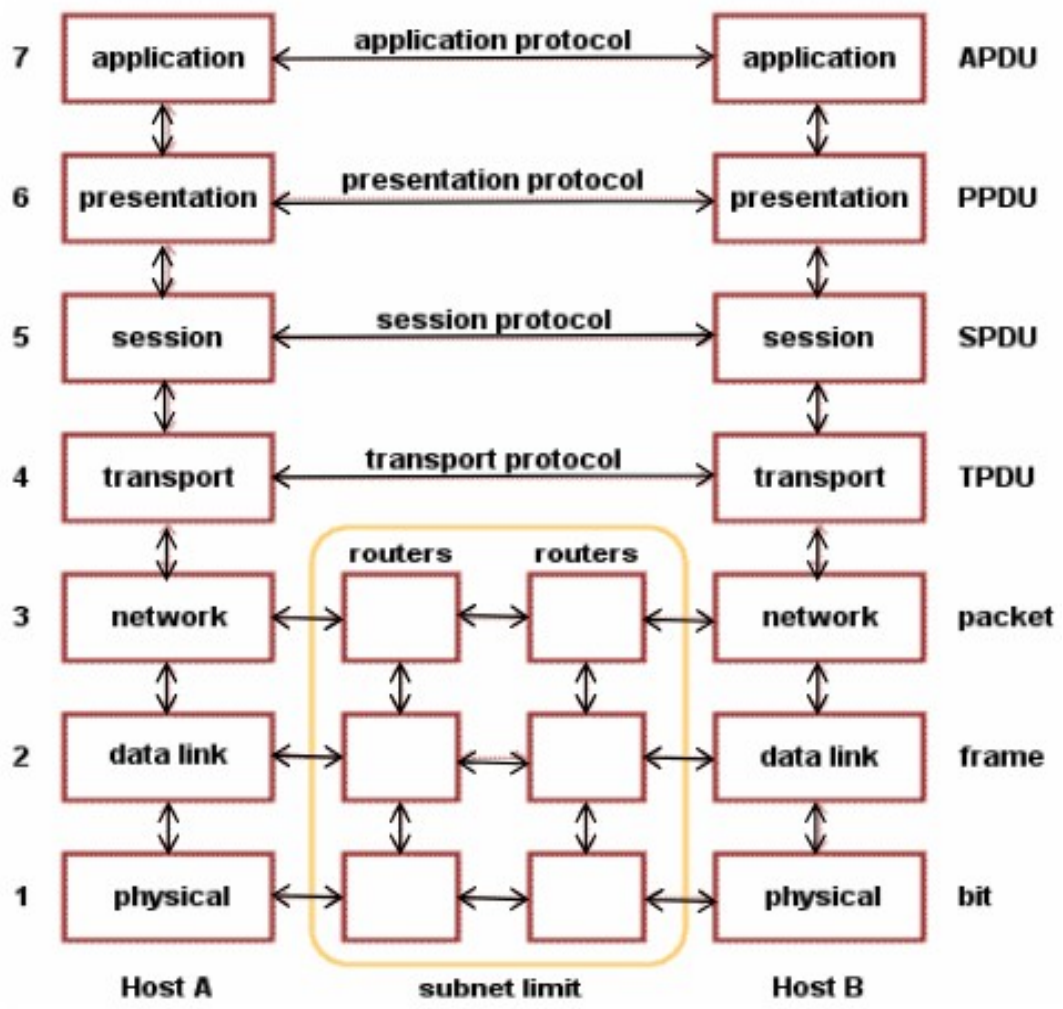


Fig: ISO-OSI Reference Model

4. The Transport Layer:

The transport layer is responsible for streaming data across the network. It decides if data transmission should be on parallel path or single path. The network layer and the transport layer work together like a postal system. The network layer addresses the data, much like a person addresses an envelope. Then, the transport layer acts as the sender's local postal branch, sorting and grouping all similarly addressed data into larger shipments bound for other local branches, where they will then be delivered.

Functions such as multiplexing, segmenting or splitting on the data done by layer four that is transport layer. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer. Ex. SPX, TCP, UDP.

5. Session Layer:

Session layer manages and synchronize the conversation between two different applications. Transfer of data from one destination to another session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided. This layer sets up, coordinates and terminates conversations. Services include authentication and reconnection after an interruption.

6. The Presentation Layer:
Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data. The presentation layer is where received data is converted into a format that the application it is destined for can understand. Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role translator.

7. Application Layer:

It is the top layer. It supports application and end-user processes. Everything at this layer is application-specific. Manipulation of data (information) in various ways is done in this layer. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc. are services provided by application layer. Layer 7 Application examples include WWW browsers, NFS, SNMP, Telnet,HTTP, FTP, etc.

Advantages of OSI model

It is standard legalized by International Standards Organization (ISO).
All OSI layers providing error checking and handling.
Provides connection-oriented and connectionless model.
OSI protocols are well hidden and can be replaced easily as the technology changes.
Emphasis on providing reliable data transfer service.

Disadvantages of OSI model

OSI is complex and costly
Not so widespread as TCP/ IP

2.7 TCP/IP Models and its Comparison with OSI

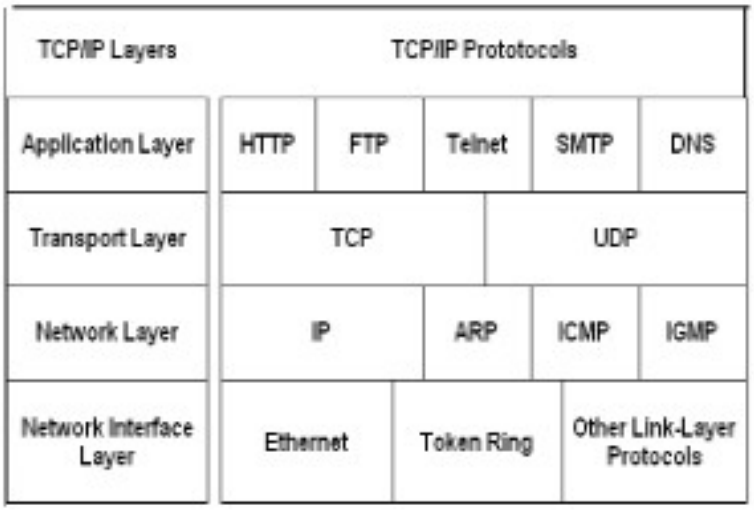
TCP/IP Reference Model
TCP/IP that is transmission control protocol and the internet protocol was developed by Department of Defense's Project Research Agency (ARPA, later DARPA) under the project of network interconnection.
Originally it was created to connect military networks together, later it was used by government agencies and universities. It is robust to failures and flexible to diverse networks. Most widely used protocol for interconnecting computers and it is the protocol of the internet. The following were seen as major design goals:

+ability to connect multiple networks together seamlessly

+ability for connections to remain intact as long as the source and destination machines were functioning

+to be built on flexible architecture

OSI Model	TCP / IP Model
Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data -Link Layer	Link Layer
Physical Layer	



1. Link Layer (or Host-To-Network Layer)

The network interface layer, also called the link layer or the data-link layer or Host to Network Layer, is the interface to the actual network hardware. This is the lowest layer in TCP/IP model. The host has to connect to network using some protocol, so that it can send IP packets over it. This protocol varies from host to host and network to network.

2. Internet Layer
The function of this layer is to allow the host to insert packets into network and then make them travel independently to the destination. However, the order of receiving the packet can be different from the sequence they were sent. The internetwork layer, also called the internet layer or the network layer, provides the “virtual network” image of an internet this layer shields the higher levels from the physical network architecture below it. Internet Protocol (IP) is the most important protocol in this layer.

3. Transport Layer

It does the same functions as that of transport layer in OSI model. Here are the key points regarding transport layer:

It decides if data transmission should be on parallel path or single path.

Functions such as multiplexing, segmenting or splitting on the data done by layer four that is transport layer.

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

Functions of the transport layer are same as the OSI model.

Transport layer also arrange the packets sent in sequence.

4. Application Layer

This layer is same as that of the OSI model and performs the following functions:

It provides different services such as manipulation of information in several ways, retransferring the files of information, distributing the results etc.

The functions such as LOGIN or password checking are also performed by the application layer.

TELNET, FTP, SMTP, DN, HTTP, NNTP are the protocols employed in this layer.

Merits of TCP/IP

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

Demerits of TCP/IP

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

Comparison of OSI Reference Model and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model.

S.N.	OSI (Open System Interconnection)	TCP/IP Model
1	OSI provides layer functioning and also defines functions of all the layers.	TCP/IP model is more based on protocols and protocols are not flexible with other layers.
2	In OSI model the transport layer guarantees the delivery of packets.	In TCP/IP model the transport layer does not guarantees delivery of packets.
3	Follows horizontal approach	Follows vertical approach.
4	OSI model has a separate presentation layer	TCP/IP does not have a separate presentation layer
5	OSI is a general model.	TCP/IP model cannot be used in any other application.
6	Network layer of OSI model provide both connection oriented and connectionless service.	The Network layer in TCP/IP model provides connectionless service.
7	OSI model has a problem of fitting the protocols in the model	TCP/IP model does not fit any protocol
8	Protocols are hidden in OSI model and are easily replaced as the technology changes.	In TCP/IP replacing protocol is not easy.
9	OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them.	OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them.
10	It has 7 layers	It has 4 layers

2.8 Networking Hardware: NIC, Hub, Repeater, Switch, Bridge, Router)

Networking hardware refers to the physical components that enable devices to connect and communicate within a network. This includes devices like routers, switches, modems, and network interface cards (NICs), each playing a specific role in data transmission and network management.

NIC

NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique ID that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC is a layer 2 device which means that it works on both the physical and data link layers of the network model.

Hub

A hub works in the physical layer of the OSI model. It is basically a non-intelligent device, and has no decision making capability. What a Hub basically does is take the input data from one of the ports and broadcast the information to all the other ports connected to the network.
So, there is a lack of security in the Hub. The Network Hubs are outdated and are out of the market.

Repeaters

A repeater is a device similar to the Hub, but has additional features. It also works in the Physical layer. The repeaters are used in places where amplification of input signal is necessary. But, the kind of amplification done by the repeater is different from the regular amplification by amplifiers. The regular amplifies everything fed into it. That means, if the input signal has noise induced into it, both the desired signal and noise signal are together amplified. But, in the case of a repeater, it regenerates the input signal, and amplifies only the desirable signal. Hence, the noise component of the signal is eliminated.

The repeaters are necessary since, during the transmission of the signals over long distances, the signal has attenuation, delay distortions and noise, which lead in loss of data. Hence, in order to prevent this, the regenerative repeaters are used.

Switches

A switch is an intelligent device that works in the data link layer. The term intelligent refers to the decision making capacity of the Switch. Since it works in the Data link layer, it has knowledge of the MAC addresses of the ports in the network. If data has to be sent from Computer A to Computer B, then, the data is transferred to the Computer B only, and not to any other computers connected on the network. Hence, it establishes a link between the sender and the receiver based on the MAC addresses. This also means that when data is being sent from A to B, Computer C can establish a link with Computer D and communication can take place between them. So, simultaneous data transfer is possible in a switch.

It is also to be noted that a switch is a secure device, because it sends information only to the desired destinations, and also certain security features such as firewalls can be implemented in the Switches.

Bridge

A bridge is also a device which works in the Data Link Layer, but is more primitive when compared to a switch. Initial bridges were used to connect only 2 LAN’s, but the most recent ones perform similar operation as the switches. It also works on the principle of transfer of information using the MAC addresses of the ports.
It can be noted is that the normal ADSL modem can be connected via bridging also. The only difference is that, when bridging is used, each time the device has to be connected to the internet; it has to dial to the internet and establish a connection. Also, a bridge alone cannot be used to connect to the internet, because, the bridge works in the Data Link Layer, and has no knowledge of the IP Addresses, which are used in the Internet.

Router

The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is a device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect.
A router may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. Typically, a packet may travel through a number of network points with routers before arriving at its destination. Routing is a function associated with the Network layer (layer 3) in the standard model of network programming, the Open Systems Interconnection (OSI) model.
Static routers: These must have their routing tables configured manually with all network addresses and paths in the internetwork.

Dynamic routers: These automatically create their routing tables by listening to network traffic.

Gateway

A gateway is a device used to connect networks using different protocols. Gateways operate at the network layer of the OSI model. In order to communicate with a host on another network, an IP host must be configured with a route to the destination network. If a configuration route is not found, the host uses the gateway (default IP router) to transmit the traffic to the destination host. The default gateway is where the IP sends packets that are destined for remote networks.
If no default gateway is specified, communication is limited to the local network. Gateway receive data from a network using one type of protocol stack, removes that protocol stack and repackages it with the protocol stack that the other network can use.
A gateway is a network point that acts as an entrance to another network. E-mail gateways-for example, a gateway that receives Simple Mail Transfer Protocol (SMTP) e-mail, translates it into a standard X.400 format, and forwards it to its destination.

2.9 Basic Networking Command

Networking commands are essential tools used to configure, troubleshoot, and manage network connections in an operating system (Windows/Linux).

1. `ipconfig` / `ifconfig`

Windows (`ipconfig`) / Linux (`ifconfig`)

- Displays network configuration such as IP address, subnet mask, and default gateway.

- Useful for diagnosing network issues.

2. `ping`

- Checks connectivity between your system and another host (IP or domain).
- Syntax: `ping google.com`
- Measures packet loss and response time.

3. `tracert` / `traceroute`

Windows (`tracert`) / Linux (`traceroute`)

- Shows the path packets take to reach a destination.
- Helps identify where network delays occur.

4. `netstat`

- Displays active connections, listening ports, and routing tables.
- Helps monitor network traffic and detect suspicious activity.

5. `nslookup`

- Queries DNS to obtain domain name or IP address mapping.
- Useful for diagnosing DNS problems.

6. `hostname`

- Displays or sets the system's hostname (computer name).