Computer Networks

Syllabus

Dr. Nilesh M. Patil

Associate Professor, DJSCE

Program: Second Year B.Tech. in Computer Engineering									Semester : IV			
Course : Computer Networks									Course Code: DJ19CEC405			
Course : Computer Networks Laboratory									Course Code: DJ19CEL405			
Teaching Scheme (Hours / week)				Evaluation Scheme								
				Semester End Examination Marks (A)			Continuous Assessment Marks (B)				Total marks (A+ B)	
Lectures	Practical	Tutorial	Total Credits	Theory			Term Test 1	Term Test 2	Avg.			
				75			25	25	25		100	
				Laboratory Examination			Term work			Total Term work		50
3	2	--	4	Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project / presentation/ Journal				
				--	-	25	15	10		25		

Objectives:

To get familiar with contemporary issues and challenges of various protocol designing in layered architecture and performance analysis of routing and transport layer protocols for various applications.

Outcomes:

On completion of the course, learner will be able to:

1. Demonstrate the concepts of data communication at physical layer and compare ISO - OSI model & TCP/IP model.
2. Demonstrate the working of networking protocols at data link layer.
3. Design of network using given IP addressing and subnetting / supernetting schemes.
4. Compare and analyze the performance of various routing protocols.
5. Compare and analyze the transport layer protocols and various congestion control algorithms.
6. Explore various protocols at application layer.

Unit	Description	Duration	CO	Marks
I	**Introduction to Networking**: Introduction to computer network, network application, network software and hardware components, Network topology, design issues for the layers. **Reference Models**: Layer details of OSI, TCP/IP models.	04	CO1	15

Unit	Description	Duration	CO	Marks
II	**Physical Layer**: Introduction to Digital Communication System **Guided Transmission Media**: Twisted pair, Coaxial, Fiber optics. **Unguided Media (Wireless Transmission)**: Radio Waves, Microwave, Bluetooth.	06	CO2	15

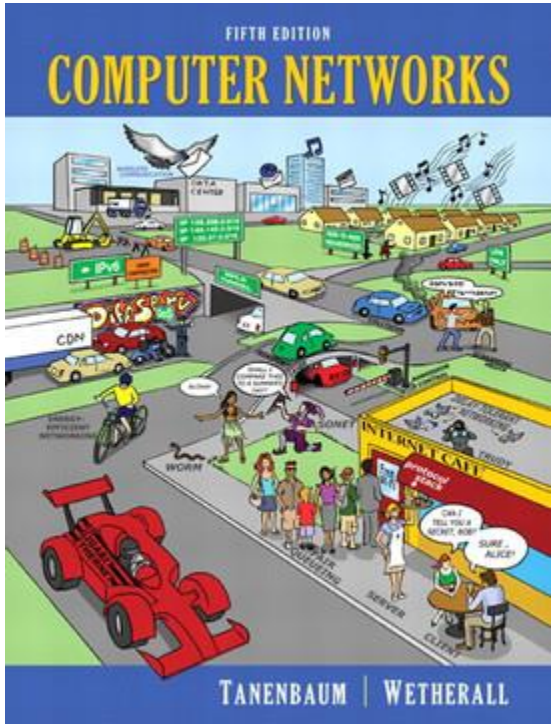
Unit	Description	Duration	CO	Marks
III	**Data Link Layer:** Design Issues: Framing Error Control: Error Detection and Correction (Hamming Code, CRC, Checksum), Flow Control: Stop and Wait, Sliding Window (Go Back N, Selective Repeat), Elementary Data Link protocols, HDLC, PPP. **Medium Access Control Sublayer:** Channel Allocation problem, Multiple Access Protocol (Aloha, Carrier Sense Multiple Access (CSMA/CA, CSMA/CD) **Wired LANS**: Ethernet, Ethernet Standards, Virtual LANs.	10	CO3	25

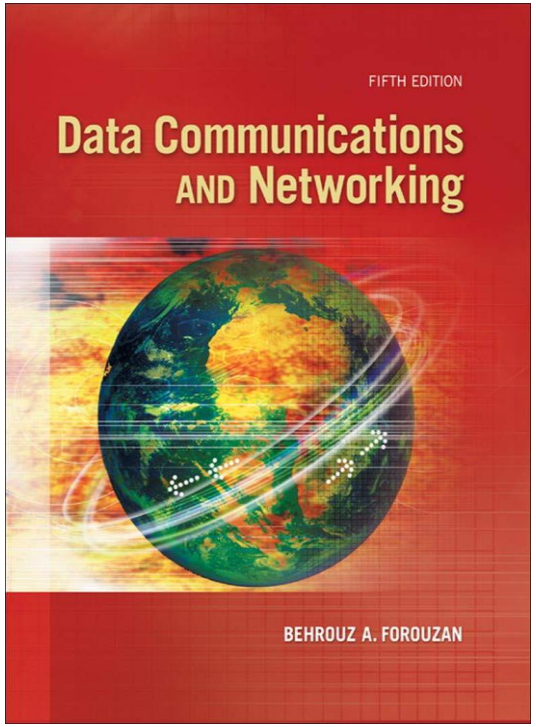
Unit	Description	Duration	CO	Marks
IV	**Network Layer:** Network Layer design issues, Communication Primitives: Unicast, Multicast, Broadcast. IPv4 Addressing (Classfull and Classless), Subnetting, Supernetting design problems ,IPv4 Protocol, Network Address Translation (NAT) **Routing algorithms** : Shortest Path (Dijkastra's), Link state routing, Distance Vector **Routing Protocols :** ARP, RARP, ICMP, IGMP **Congestion control algorithms:** Open loop congestion control, Closed loop congestion control, QoS parameters, Token & Leaky bucket algorithms.	10	CO4	25

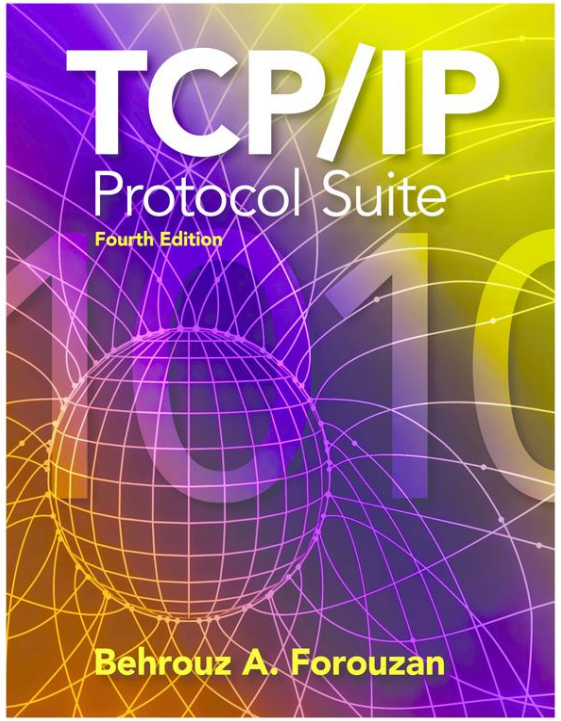
Unit	Description	Duration	CO	Marks
V	**Transport Layer** The Transport Service: Port Addressing, Transport service primitives, Berkeley Sockets, Connection management (Handshake, Teardown), UDP, TCP, TCP state transition, TCP timers, TCP Flow control (sliding Window), TCP Congestion Control: Slow Start .	06	CO5	15

Unit	Description	Duration	CO	Marks
VI	**Application Layer :** DNS: Name Space, Resource Record and Types of Name Server. HTTP, HTTPS, SMTP, Telnet, FTP, DHCP.	06	CO6	15

Books


FIFTH EDITION
COMPUTER NETWORKS
TANENBAUM | WETHERALL


FIFTH EDITION
Data Communications
AND Networking
BEHROUZ A. FOROUZAN


TCP/IP
Protocol Suite
Fourth Edition
Behrouz A. Forouzan

List of Experiments

1. A. Study of LAN topology. B. Study of various Network devices.
2. Installation & Configuration of Network Simulator (NS2) in Linux environment. Study of different topologies and create duplex link in NS2.
3. Building of wired & wireless topology using NS2.
4. Write a program to implement A. Error Detection and Correction B. Framing
5. Implement Stop and Wait protocol in NS2.
6. Write a program to implement Sliding Window Protocols- Selective Repeat, Go Back N.
7. Build Class A & Class B Network using router and Implement subnetting concept.
8. Write a program to implement any one Routing Protocol.
9. Write a program to find out class of a given IP address, subnet mask & first & last IP address of that block.
10. Write a program to implement Congestion Control algorithms.
11. Write a program to build client-server model on different computers. Implement TCP-UDP scenario in NS2/NS3.
12. Install and configure Network Management/ Monitoring Tools.

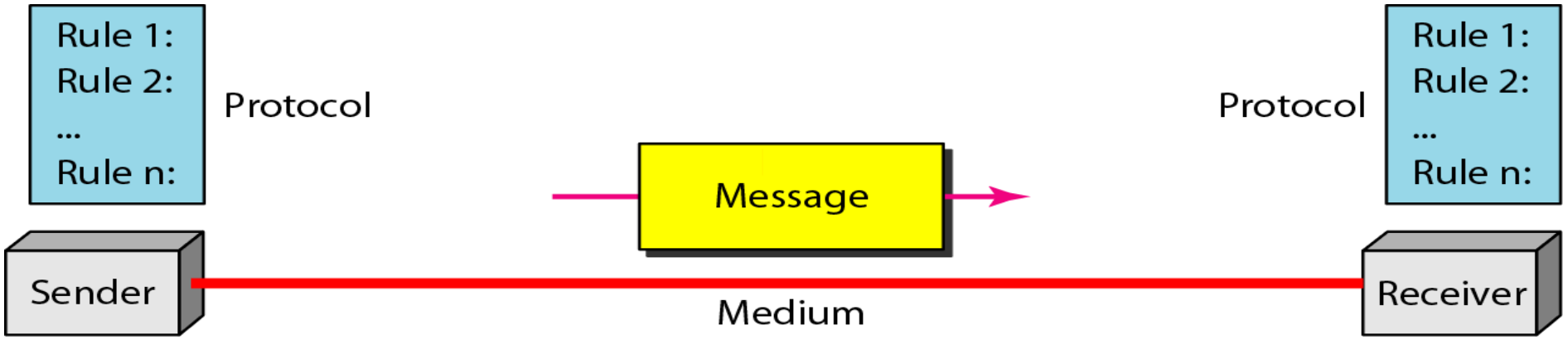
Chapter 1
Introduction to Networking

- *The term telecommunication means communication at a distance.*
- *The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data.*
- *Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.*

Effective Characteristics of Data Communication

- Delivery. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
- Accuracy. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
- Timeliness. The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.
- Jitter. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

Components of a data communication system



Components of a data communication system

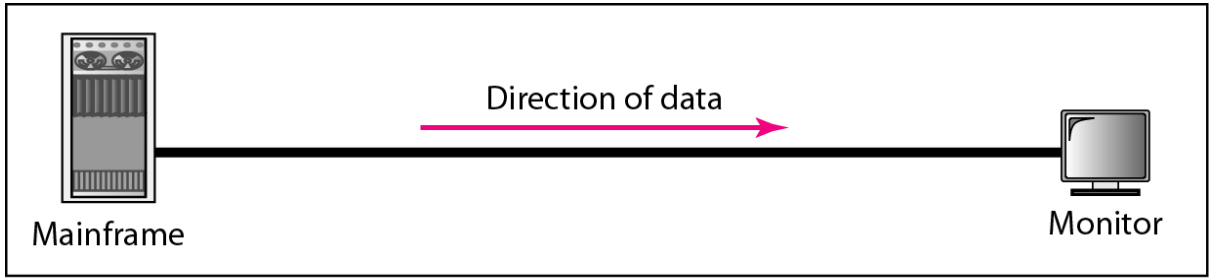
1. Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
5. Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese. The key elements of a protocol are syntax, semantics and timing.

a) Syntax : Refers to the structure or format of the data, means the order in which they are presented.

b) Semantics : Refers to the meaning of each section of bits, means how a particular pattern is to be interpreted, and what action is to be taken based on that interpretation.

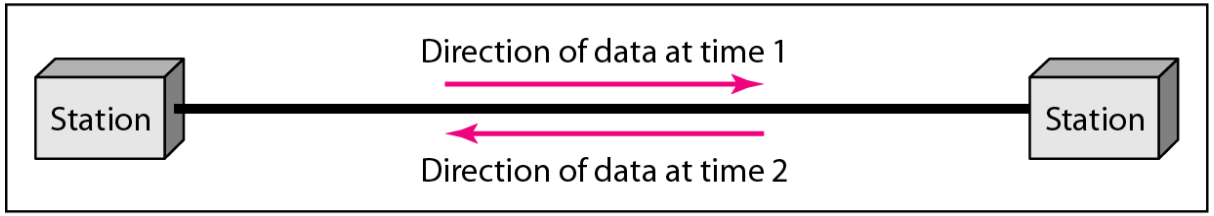
c) Timing : Means that data should be sent and how fast they can be sent.

Data flow (simplex, half-duplex, and full-duplex)



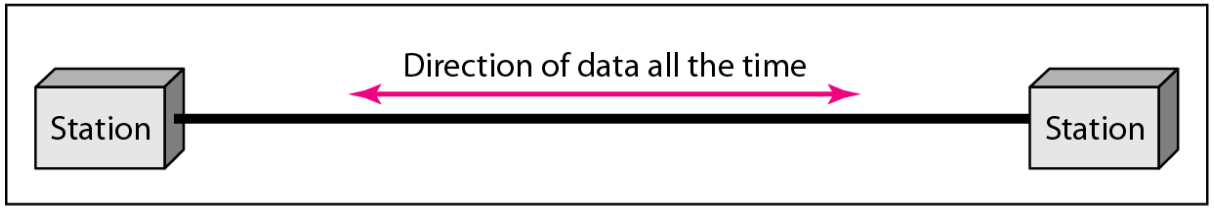
a. Simplex

Example of simplex mode are: Keyboard and monitor.



b. Half-duplex

Example of half duplex mode is: Walkie-Talkies.



c. Full-duplex

Example of full duplex mode is: Telephone.

Networks

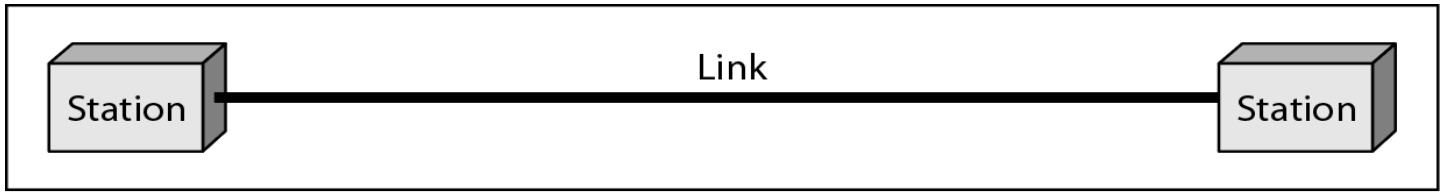
- *A network is a set of devices (often referred to as nodes) connected by communication links.*
- *A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.*
- *A link can be a cable, air, optical fiber, or any medium which can transport a signal carrying information.*

Network Criteria

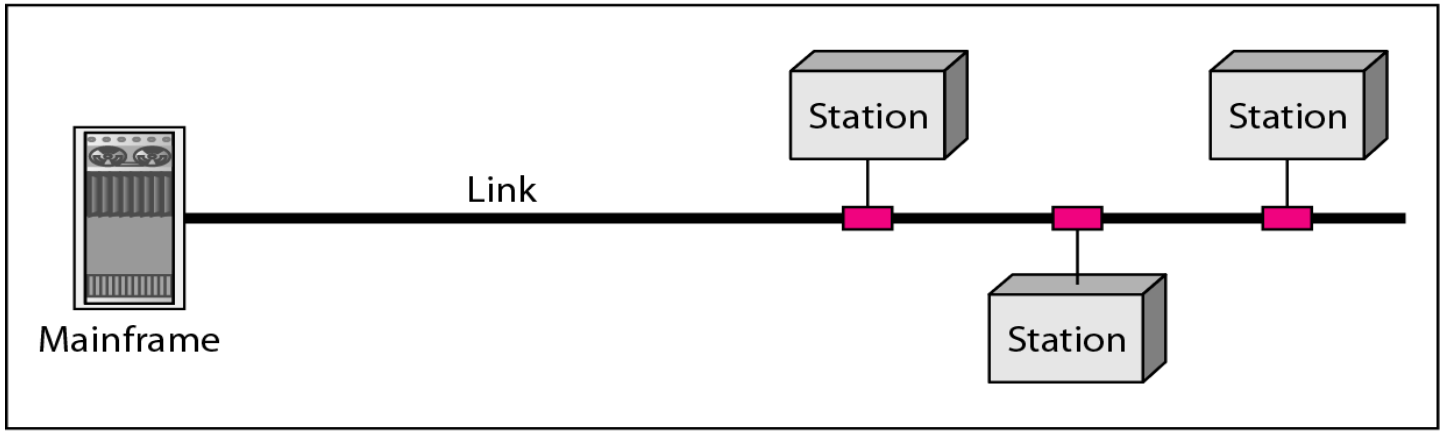
- **Performance**
  - **Depends on Network Elements**
  - **Measured in terms of Delay and Throughput**
- **Reliability**
  - **Failure rate of network components**
  - **Measured in terms of availability/robustness**
- **Security**
  - **Data protection against corruption/loss of data due to:**
    - **Errors**
    - **Malicious users**

Type of Connection

- Point to Point - single transmitter and receiver
- Multipoint - multiple recipients of single transmission



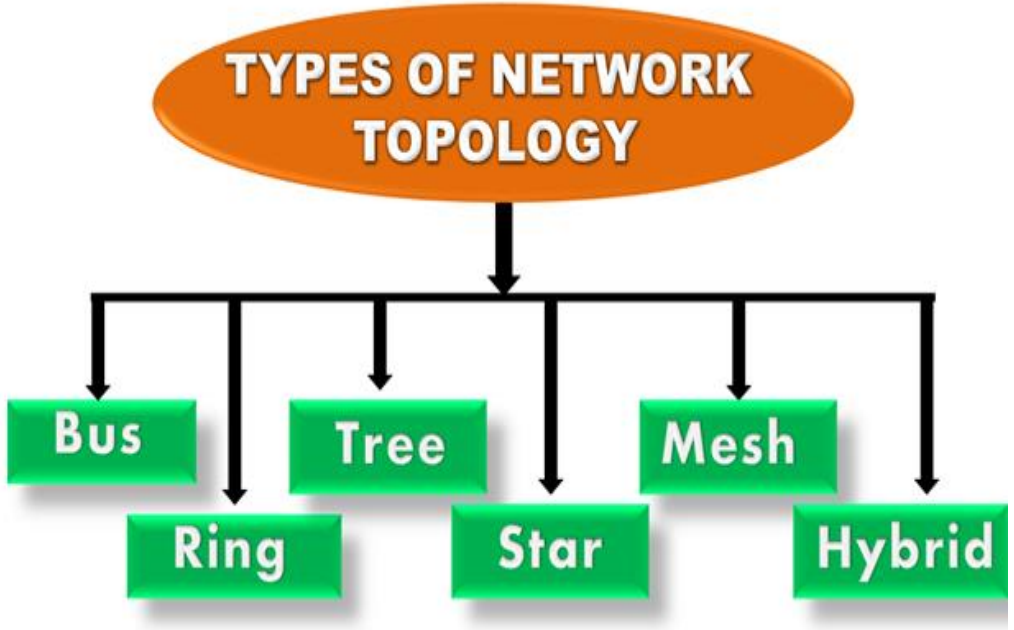
a. Point-to-point



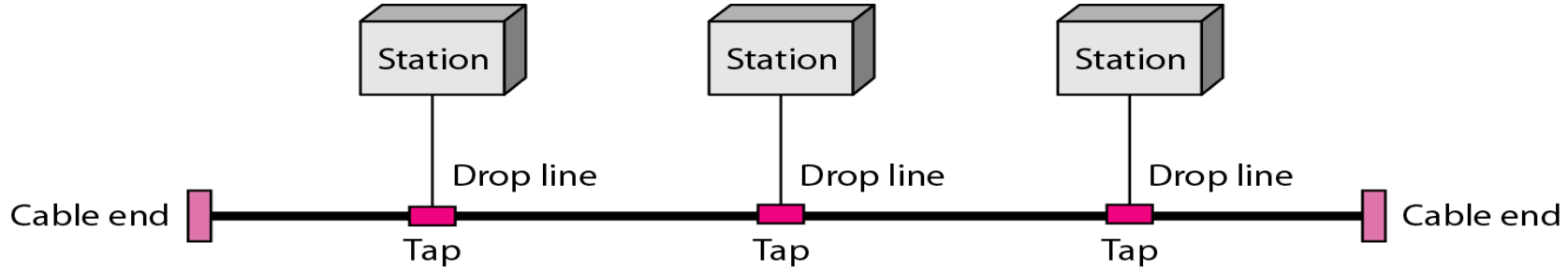
b. Multipoint

Topology

- Network topology refers to the way different computers, devices or nodes connect to each other in a communication network.
- It describes their physical arrangement and explains the logical flow of information throughout the network.
- A computer network topology can consist of one physical topology and several logical topologies.
- A physical topology explains how computers, devices or nodes connect with each other in a network based on their location. It involves assessing the physical layout of network cables and workstations.
- Conversely, a logical topology explains how data flows from one device to another based on network protocols. It assesses the way devices communicate with each other internally.
- Therefore, network topology defines the virtual shape, layout and structure of a network from both a physical and logical viewpoint.



Bus Topology



- The bus topology is designed in such a way that all the stations are connected through a single cable known as a **backbone cable**.
- Each node is either connected to the backbone cable by **drop line** or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network.
- All the stations available in the network will receive the message whether it has been addressed or not.

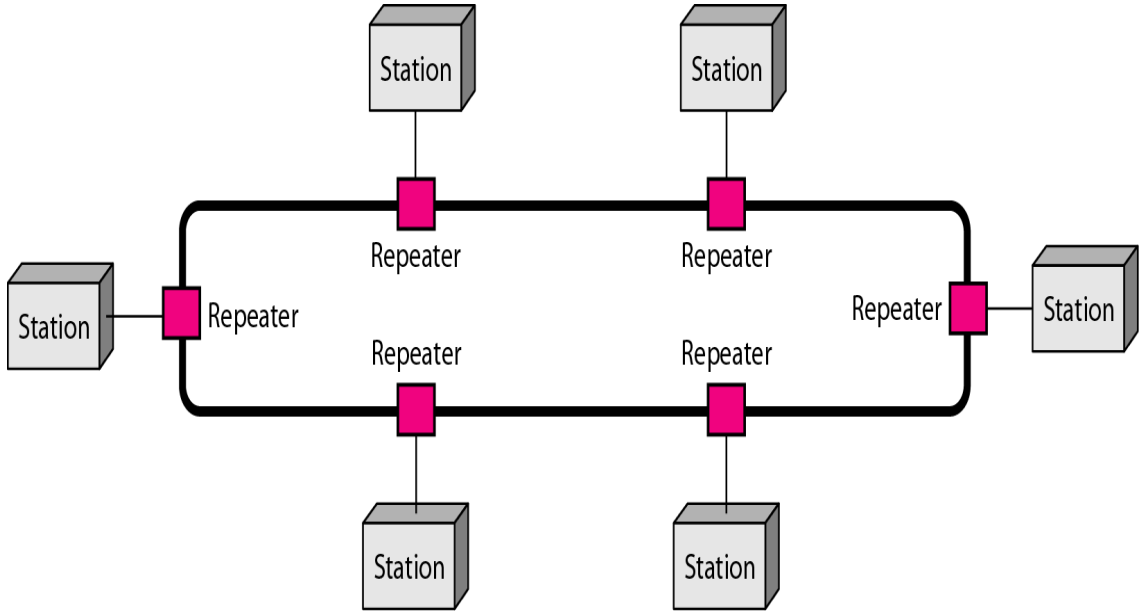
Advantages of Bus Topology:

- Bus topology is easy to install.
- Because of backbone, less cable is required.
- Number of I/O port required is less. Also the hardware is reduced.
- The backbone can be extended by using repeater.
- Cost of the network is low.

Disadvantages of Bus Topology:

- Heavy network traffic can slow a bus considerably.
- Difficult for reconnection, fault isolation or troubleshooting.
- Difficult to add new node/device.
- Failure of backbone affects failure of all devices on the network.

Ring Topology



- Ring Topology is a topology in which each computer is linked to another on both sides.
- The last computer is linked to the first, forming a ring.
- This topology enables each computer to have exactly two neighbors.
- The most common access method of the ring topology is token passing. Token is a frame that circulates around the network.

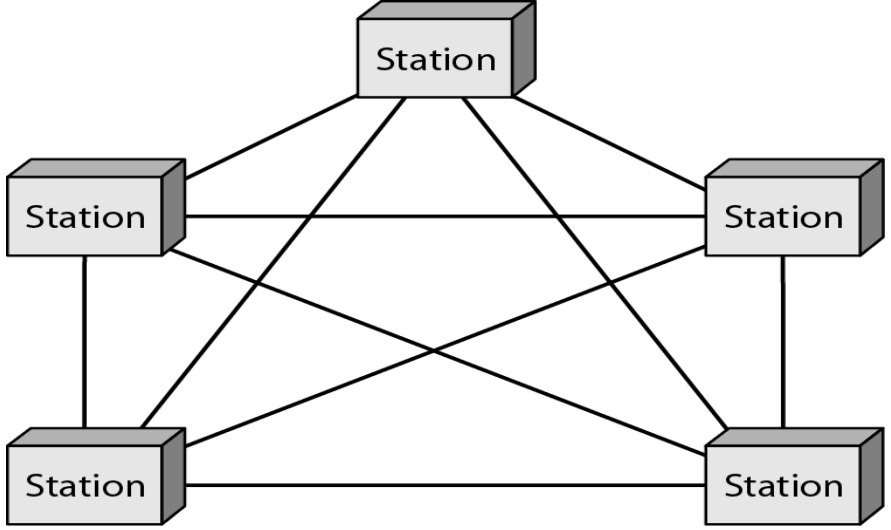
Advantages:

- A ring is relatively easy to install and reconfigure.
- Link failure can be easily found as each device is connected to its immediate neighbors only.
- Because every node is given equal access to the token no one node can monopolize the network.

Disadvantages:

- Maximum ring length and number of devices is limited.
- Failure of one node on the ring can affect the entire network.
- Adding or removing node disrupts the network.

Mesh Topology



- Mesh Topology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- Mesh topology can be formed by using the formula: Number of cables = (n*(n – 1))/2; where n is the number of nodes that represents the network.
- This indicates that each node must have (n – 1) I/O ports.
- The Internet is an example of the mesh topology.

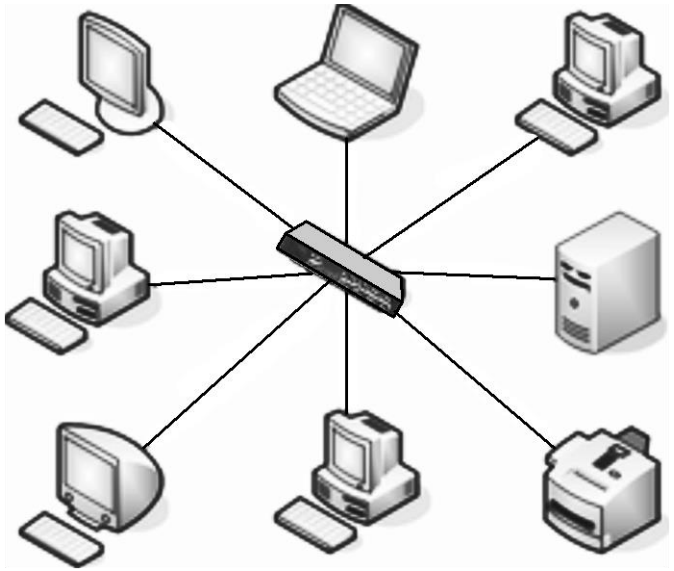
Advantages:

- No traffic because of dedicated link.
- Robust because if one link fails, it does not affect the entire network.
- Privacy and security of data is achieved due to dedicated link.
- Fault identification is easy.

Disadvantages:

- Difficulty of installation and reconfiguration as every node is connected to every other node.
- Costly because of maintaining redundant links.
- The amount of cabling required is large

Star Topology



- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a server, and the peripheral devices attached to the server are known as clients.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a physical star topology.
- Star topology is the most popular topology in network implementation.

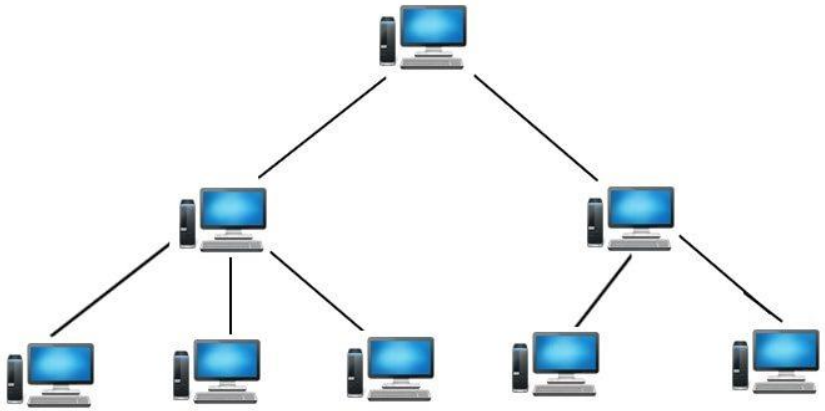
Advantages:

- Each device needs only one link and one I/O port, which makes star topology less expensive, easy to install and easy to configure.
- Robust topology. If any link fails, it does not affect entire network.
- Easy fault identification and fault isolation.
- It is easy to modify and add new nodes to star network without disturbing the rest of the network.

Disadvantages:

- If the central hub fails, the entire network fails to operate.
- Each device requires its own cable segment.
- In hierarchical network, installation and configuration is difficult.

Tree Topology



- Tree topologies are also known as hierarchical topology, as the root node connects all other nodes to form a hierarchy.
- This topology is known as a Star Bus topology because it combines several star topologies into a single bus.
- Data flows from top to bottom in this network topology, from the central hub to the secondary hub and then to the devices, or from bottom to top, from the devices to the secondary hub, which then connects to the central hub.

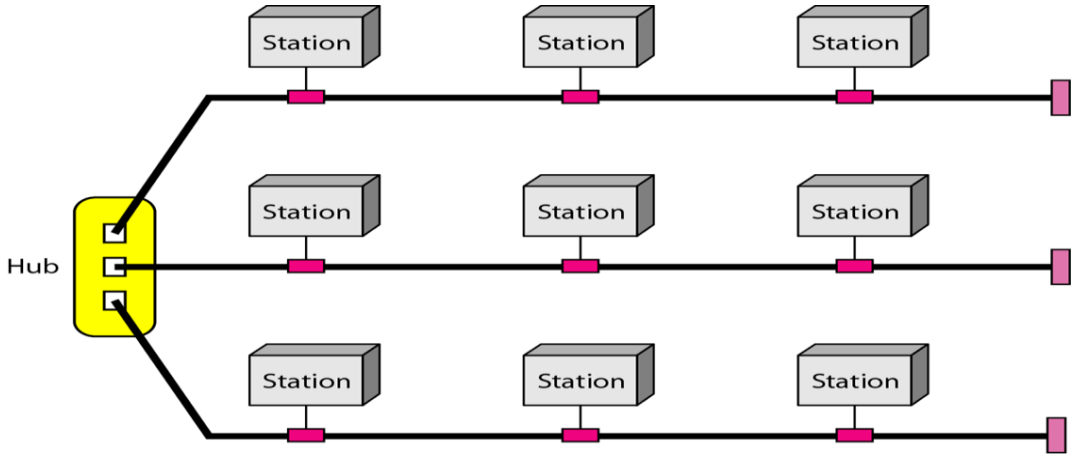
Advantages:

- Support for broadband transmission, i.e., signals are sent over long distances without being attenuated.
- We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- Error detection and error correction are very easy in a tree topology.
- The breakdown in one station does not affect the entire network.

Disadvantages:

- If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- Devices required for broadband transmission are very costly.
- A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.

Hybrid Topology



- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology.
- For example, if there exist a ring topology in one branch of HDFC bank and bus topology in another branch of HDFC bank, connecting these two topologies will result in Hybrid topology.

Advantages:

- **Reliable**: If a fault occurs in any part of the network, it will not affect the functioning of the rest of the network.
- **Scalable**: Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible**: This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective**: Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

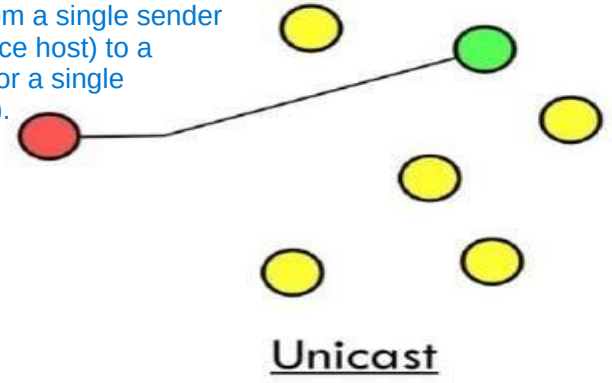
Disadvantages:

- **Complex Design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly Infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

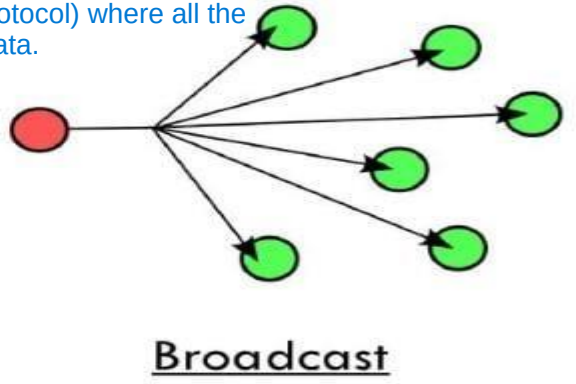
Type of Transmission

- Unicast
- Multicast
- Broadcast
- Anycast

Unicast Transmission
(One-to-One)
In Unicast transmission, the data is transferred from a single sender (or a single source host) to a single receiver (or a single destination host).

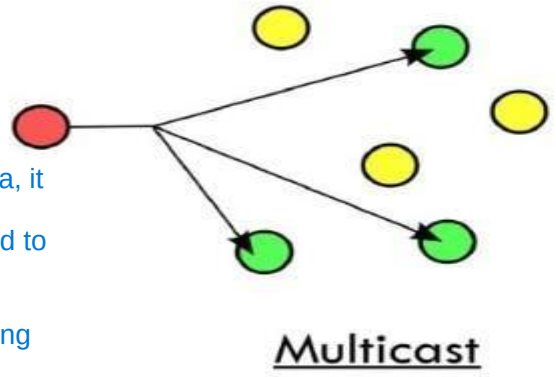


Broadcast Transmission (One-to-All)
In Broadcast transmission, the data is transmitted from one or more senders to all the receivers within the same network or in other networks. This type of transmission is useful in network management packets such as ARP (Address Resolution Protocol) and RIP (Routing Information Protocol) where all the devices must see the data.

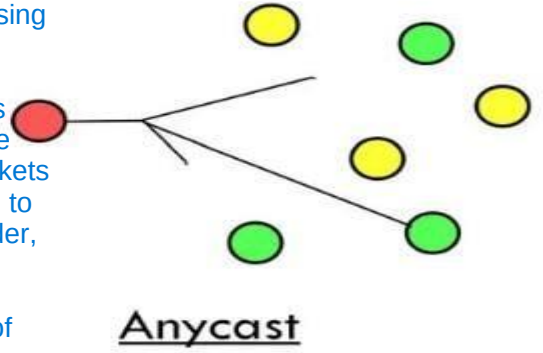


Multicast Transmission (One-to-Many)
When the data is transmitted from a single source host to a specific group of hosts having the interest to receive the data, it is known as multicast transmission. Multicast can be more efficient than unicast when different groups of receivers need to see the same data.

Example Multicast is the technique used in Internet streaming of video or audio teleconference, sending an email to a particular group of people, etc.



Anycast is a network addressing and routing methodology in which a single destination IP address is shared by devices (generally servers) in multiple locations. Routers direct packets addressed to this destination to the location nearest the sender, using their normal decision-making algorithms, typically the lowest number of BGP network hops. Anycast routing is widely used by content delivery networks such as web and DNS hosts, to bring their content closer to end users.



Categories of Networks

- Personal Area Network (PAN)
- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)

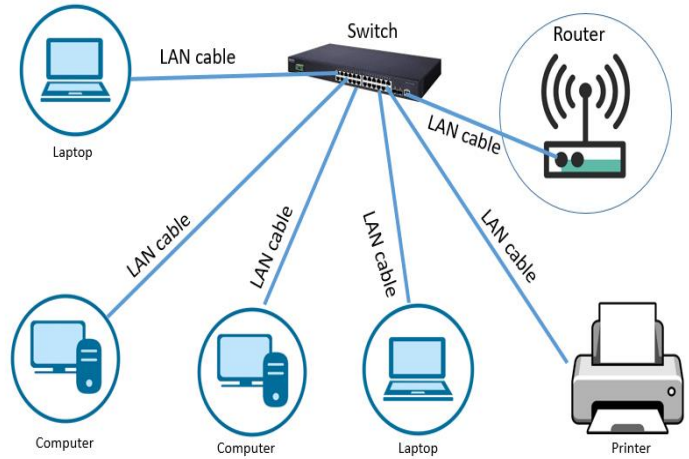
Personal Area Network (PAN)

- It is an interconnection of personal technology devices to communicate over a short distance, which is less than 33 feet or 10 meters or within the range of an individual person, typically using some form of wireless technologies.
- Examples of PAN:

1. Body Area Network
2. Home Network

Local Area Network (LAN)

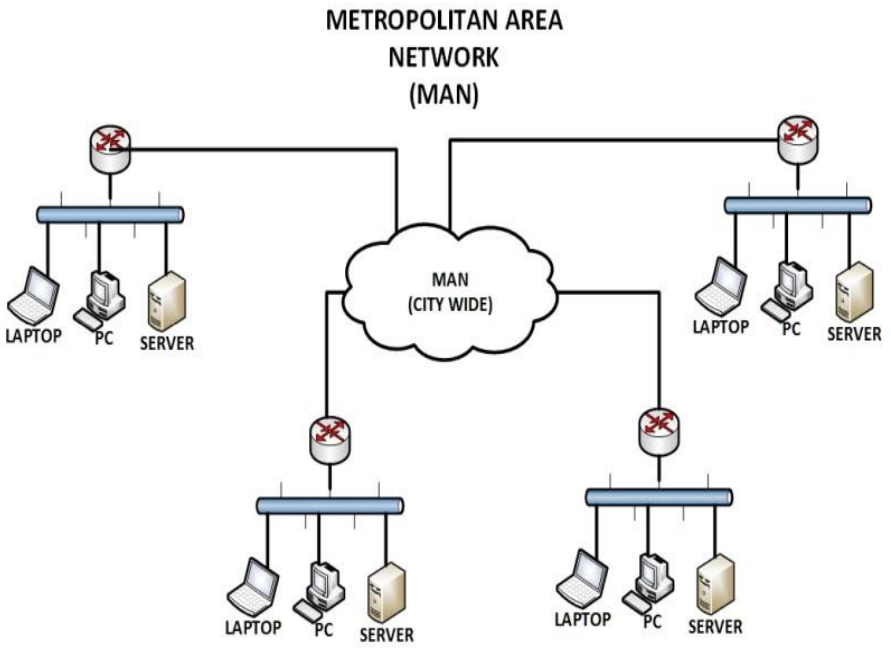
- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and Ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Traditional LANs run at speeds of 10 Mbps to 100 Mbps. Newer LANs operate at upto 10 Gbps.
- Local Area Network provides higher security.



Local Area Network

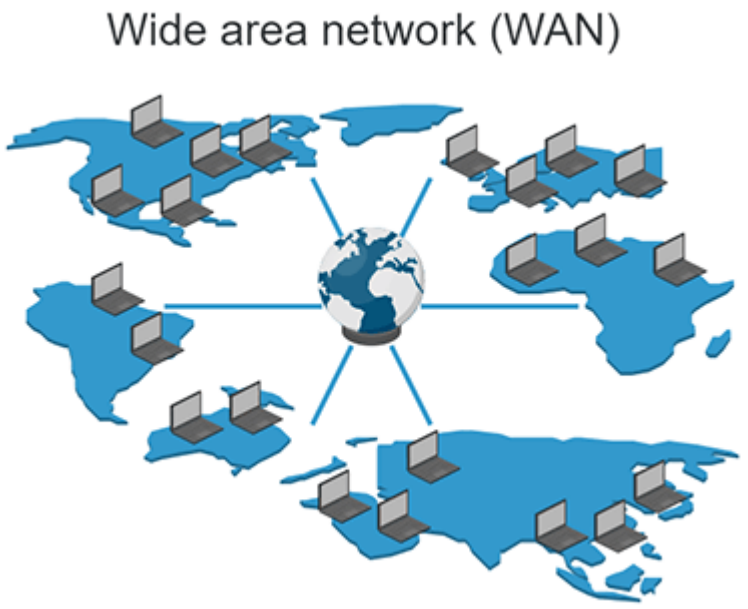
Metropolitan Area Network (MAN)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, ADSL, etc.
- It has a higher range than Local Area Network (LAN).
- Supports both data and voice.
- Speed: 34 to 150 Mbps



Wide Area Network (WAN)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- It spans over a large geographical area through a telephone line, fiber optic cable or satellite links.
- The Internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.

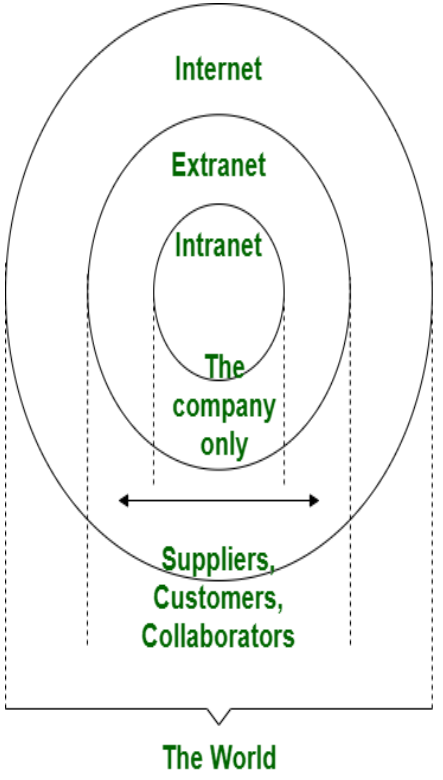


Comparison of LAN, MAN and WAN

Basis of Comparison	LAN	MAN	WAN
1. Expands to	Local Area Network	Metropolitan Area Network	Wide Area Network
2. 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.
3. Ownership of Network	Private	Private or Public	Private or Public
4. Design and maintenance	Easy	Difficult	Difficult
5. Propagation Delay	Short	Moderate	Long
6. Speed	High	Moderate	Low
7. Fault Tolerance	More Tolerant	Less Tolerant	Less Tolerant
8. Congestion	Less	More	More
9. Used for	College, School, Hospital.	Small towns, City.	Country/Continent.
10. Allows	Single pair of devices to communicate.	Multiple computers can simultaneously interact.	A huge group of computers communicate at the same time.

Intranet and Extranet

S.NO	Intranet	Extranet
1.	Intranet is a tool for sharing information throughout the organization.	Extranet is a tool for sharing information between the internal members and external members.
2.	Intranet is owned and managed by a single organization.	Extranet is owned and managed by either a single or a many organization.
3.	In intranet, security is implemented through a firewall.	In extranet, security is implemented through a VPN.
4.	Intranet has a limited number of connected devices.	In extranet, connected devices are more as compared with the intranet.
5.	Intranet is a private network type for an organization.	Extranet is also a private network in which public network is used in order to share the information to the suppliers and customers.
6.	Intranet is used in order to get employee information, telephone directory etc.	Extranet is used to check status, access data, send mail, place order etc.
7.	Intranet is the limited and compromised version of Extranet.	Extranet is the limited and compromised version of Internet.
8.	A particular organization is the regulating authority for intranet.	Extranet is regulated by multiple organizations.
9.	Intranet is accessible to only the members of organization.	Extranet is accessible to members of organization as well as external members with logins.
10.	Intranet's restricted area is up to an organization.	Extranet's restricted area is up to an organization and some of its stakeholders.
11.	Example: WIPRO using internal network for its business operations.	Example: DELL and Intel using network for business related operations.



Client-Server Network Vs Peer-to-Peer Network

S.NO	Client-Server Network	Peer-to-Peer Network
1.	In Client-Server Network, Clients and server are differentiated, Specific server and clients are present.	In Peer-to-Peer Network, Clients and server are not differentiated.
2.	Client-Server Network focuses on information sharing.	Peer-to-Peer Network focuses on connectivity.
3.	In Client-Server Network, Centralized server is used to store the data.	In Peer-to-Peer Network, each peer has its own data.
4.	In Client-Server Network, Server respond the services which is request by Client.	In Peer-to-Peer Network, each and every node can do both request and respond for the services.
5.	Client-Server Network are costlier than Peer-to-Peer Network.	Peer-to-Peer Network are less costlier than Client-Server Network.
6.	Client-Server Network are more stable than Peer-to-Peer Network.	Peer-to-Peer Network are less stable if number of peer is increased.
7.	Client-Server Network is used for both small and large networks.	Peer-to-Peer Network is generally suited for small networks with fewer than 10 computers.

Network Application

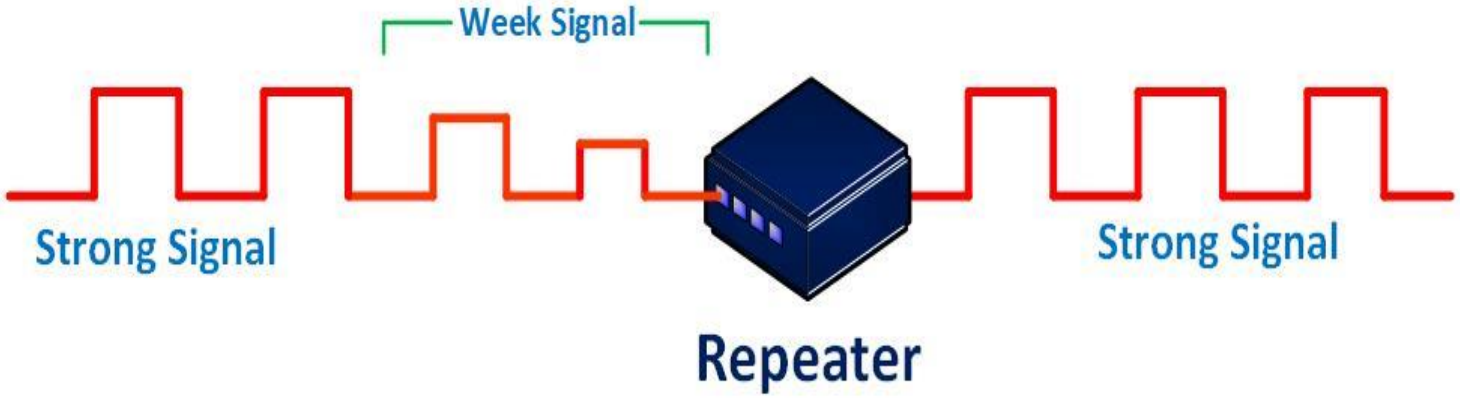
- **Resource sharing**: Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.
- **Server-Client model**: Computer networking is used in the server-client model. A server is a central computer used to store the information and maintained by the system administrator. Clients are the machines used to access the information stored in the server remotely.
- **Communication medium**: Computer network behaves as a communication medium among the users. For example, a company contains more than one computer having an email system which the employees use for daily communication.
- **E-commerce**: Computer network is also important in businesses. We can do the business over the internet. For example, amazon.com is doing their business over the internet, i.e., they are doing their business over the internet.

Networking Devices

- Repeater
- Hub
- Switch
- Bridge
- Router
- Gateway

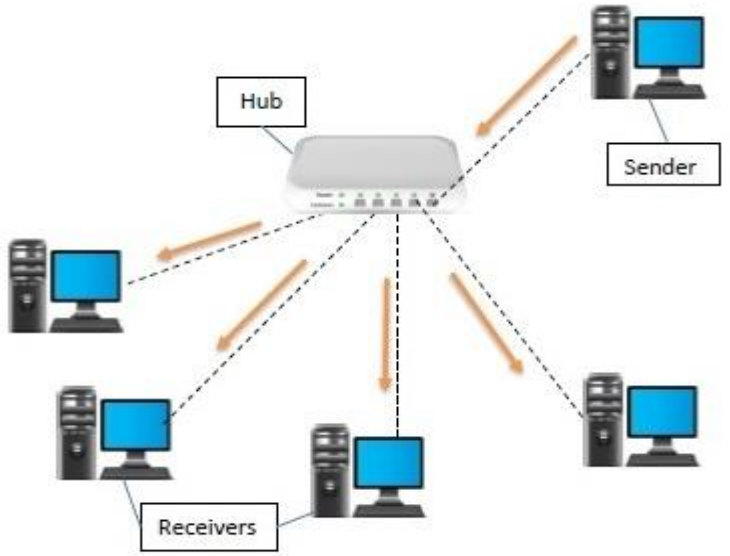
Repeater

- Also called a regenerator.
- Operates only in the physical layer of the ISO-OSI model.
- Simply regenerates the weak signal and transmit the regenerated signal.
- Provides signal amplification.



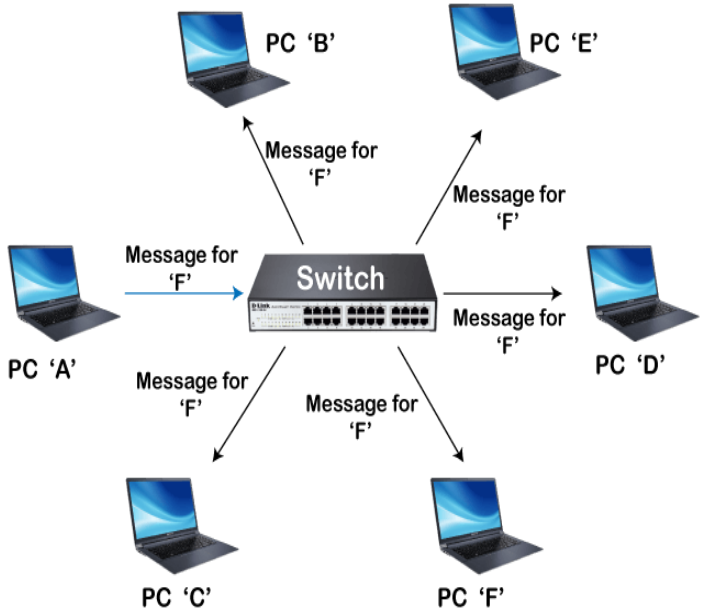
Hub

- Also called the central concentrator or controller.
- Operates in the physical layer of the ISO-OSI model.
- It simply transmits the incoming signals to the other media segments.
- Provides central management.
- Do not amplify the incoming signal.



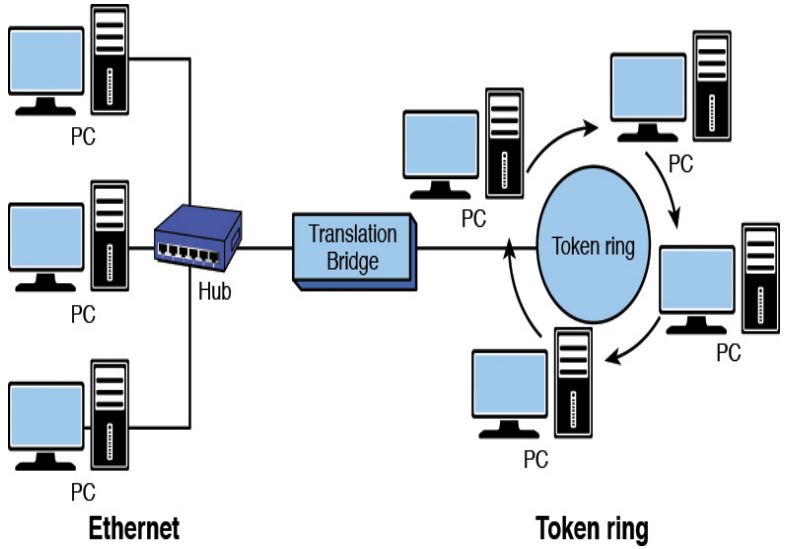
Switch

- Operates in the data link layer of the ISO-OSI model.
- Buffer the incoming packet.
- Check the address and decide the outgoing line.
- Retransmit the packet only if the line is idle.



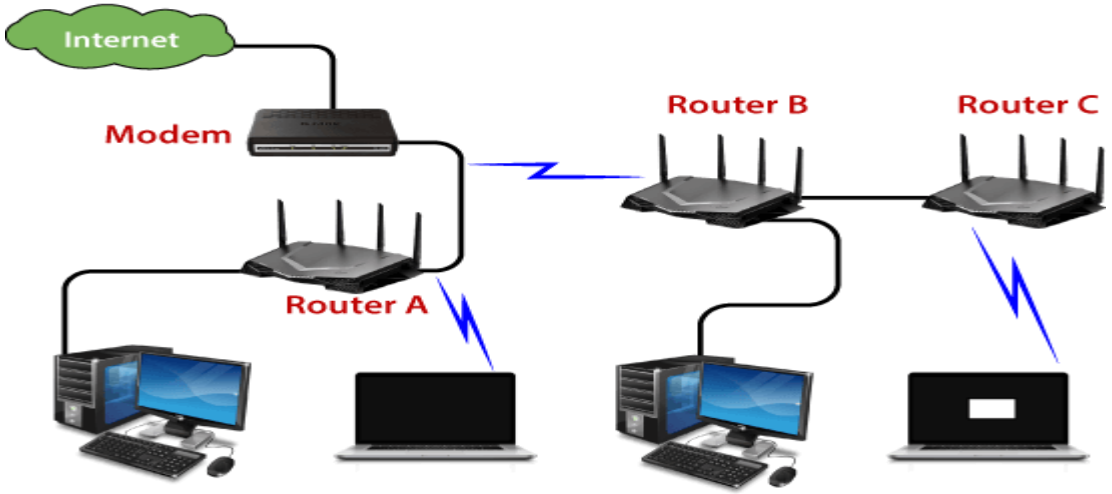
Bridge

- Operates in the data link layer of the ISO-OSI model.
- A bridge connects two or more LANs.
- When a frame arrives, software in the bridge extracts the destination address from the frame header and looks it up in the bridge table to see where to send the frame.
- Can divide the busy network into segments and reduce the network traffic.



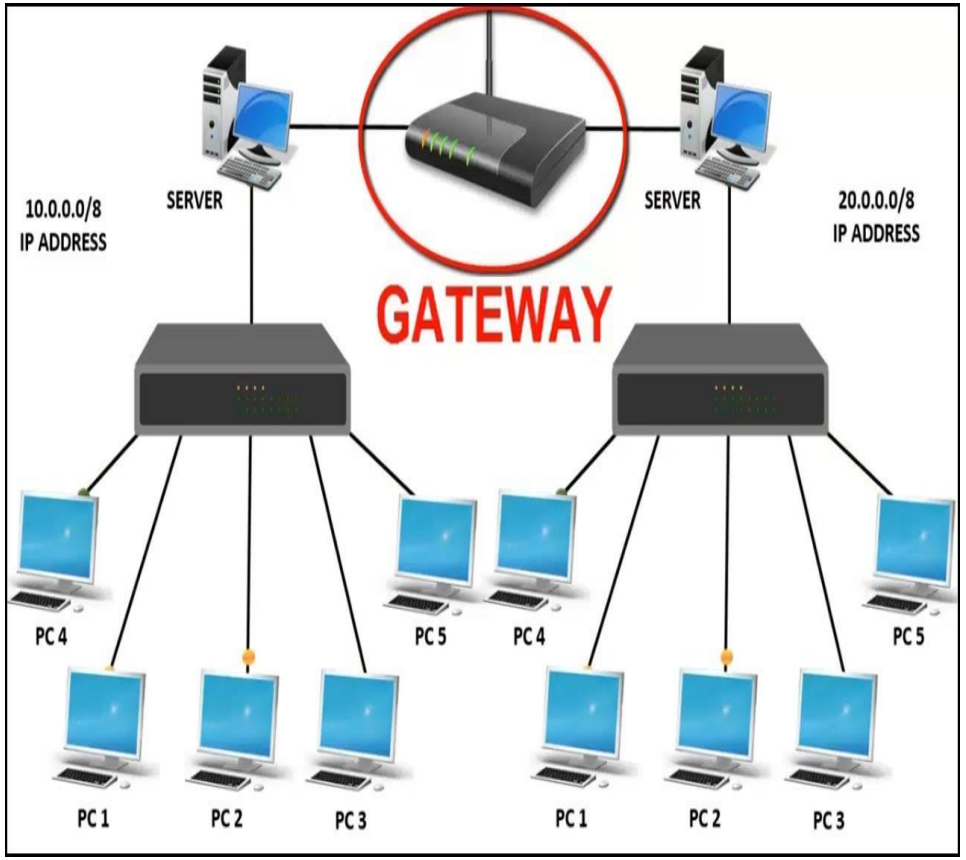
Router

- Operates at the network layer of the ISO-OSI model.
- Interconnects two or more networks which can be heterogeneous.
- They decide on the most efficient path that the packets should take while flowing from one network to another.



Gateway

- Operates at all the seven layers of the ISO-OSI model.
- It is a protocol converter.
- A gateway can accept a packet formatted for one protocol and can convert it into a packet formatted for another protocol before forwarding it.
- Gateway must adjust data rate, size, and data format.
- Gateway is generally a software installed within a router.



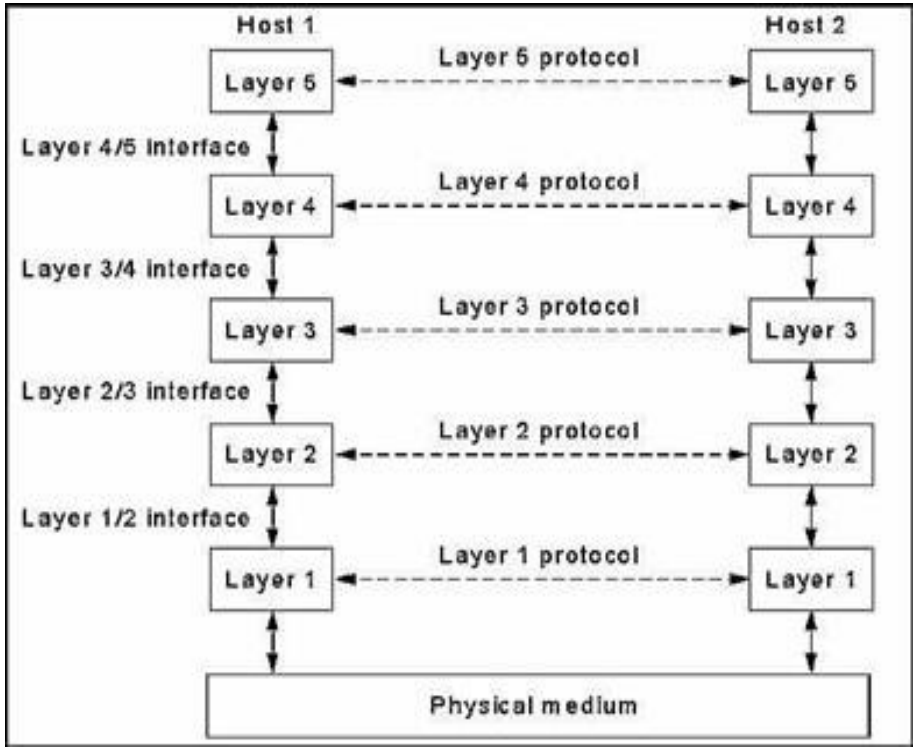
Network Software

- Software components are the programs or applications that run on these networking devices.
- Software includes things like operating systems, antivirus software, and networking tools.
- Functions of network software

1. **User management** allows administrators to add or remove users from the network. This is particularly useful when hiring or relieving users.
2. **File management** lets administrators decide the location of data storage and control user access to that data.
3. **Access** enables users to enjoy uninterrupted access to network resources.
4. **Network security systems** assist administrators in looking after security and preventing data breaches.

Protocol Hierarchies

- Most networks are organized as a series of layers or levels.
- To reduce the design complexity, networks are organized as a series of layers or levels, one above the other.
- The number of layers, the name of each layer, the contents of each layer and the function of each layer differ from network to network.
- The purpose of each layer is to offer certain services to the higher layers.
- Layer n on one machine (sender) carries a conversation with layer n on another machine (receiver).
- The rules and conventions used in this conversation are collectively known as the layer n protocol.
- If the protocol is violated, communication will be difficult.
- The entities comprising the corresponding layers on different machines are called as **peers**.
- The communication actually takes place between the peers using the protocol.
- The dotted lines show the virtual communication and the physical communication is shown by solid lines.
- Between each pair of adjacent layers is interface. The **interface** defines which primitive operations and services the lower layer offers to the upper layer.
- A set of layers and protocols is called a **network architecture**.



Design Issues for the Layers

1. Mechanism for identifying senders and Receivers (addressing).
2. Rule for data transfer: Simplex, Half-Duplex, and Full-Duplex.
3. Error control (Detection and Correction).
4. Preserving order of messages (Sequencing).
5. How to keep a fast sender from swamping a slow receiver (flow control).
6. Inability of all processes to accept arbitrarily long messages. (Dismantling – Transmit – Reassembling)
7. Multiplexing and demultiplexing is to be used to share the same channel by multiple sources simultaneously.
8. In the case of multiple paths, Routing Algorithms are required to choose the optimal path.
9. Connection Establishment, maintenance, and termination once the session is over.

Connection-Oriented and Connectionless Service

Parameter	Connection-oriented	Connectionless
Related System	It is based on the telephone system in its architecture and development.	It is a postal system-based service.
Definition	It is used to establish an end-to-end connection between senders and receivers prior to transferring data across the same or a separate network.	It is used to transport data packets from senders to receivers without establishing a connection.
Virtual Path	It establishes a virtual connection between the sender and the recipient.	It does not establish a virtual link between the sender and the recipient.
Authentication	Before transferring data packets to the recipient, it requires authentication.	Before sending data packets, it does not require authentication.
Data Packets Path	All data packets are received in the same sequence as they were transmitted.	Same sequence of data packets is not guaranteed.
Bandwidth requirement	It takes more bandwidth to send data packets.	The data packets are sent using very low bandwidth.
Data Reliability	It is a more reliable connection service since it assures data packets travel from one end of a connection to the other.	It is not a reliable connection service since it does not ensure the passage of data packets from one end to the other in order to establish a connection.
Congestion	There is no congestion since it establishes an end-to-end link between sender and recipient during data transfer.	Congestion may occur as a result of not establishing an end-to-end connection between the source and receiver for data packet transmission.
Examples	A connection-oriented service is the Transmission Control Protocol (TCP).	Connectionless services include User Datagram Protocol (UDP), Internet Protocol (IP), and Internet Control Message Protocol (ICMP).

Service Primitives

- A service is formally specified by a set of **primitives** (operations) available to a user process to access the service.
- There are **five types** of service primitives:

1. **LISTEN:** When a server is ready to accept an incoming connection it executes the LISTEN primitive. It blocks waiting for an incoming connection.

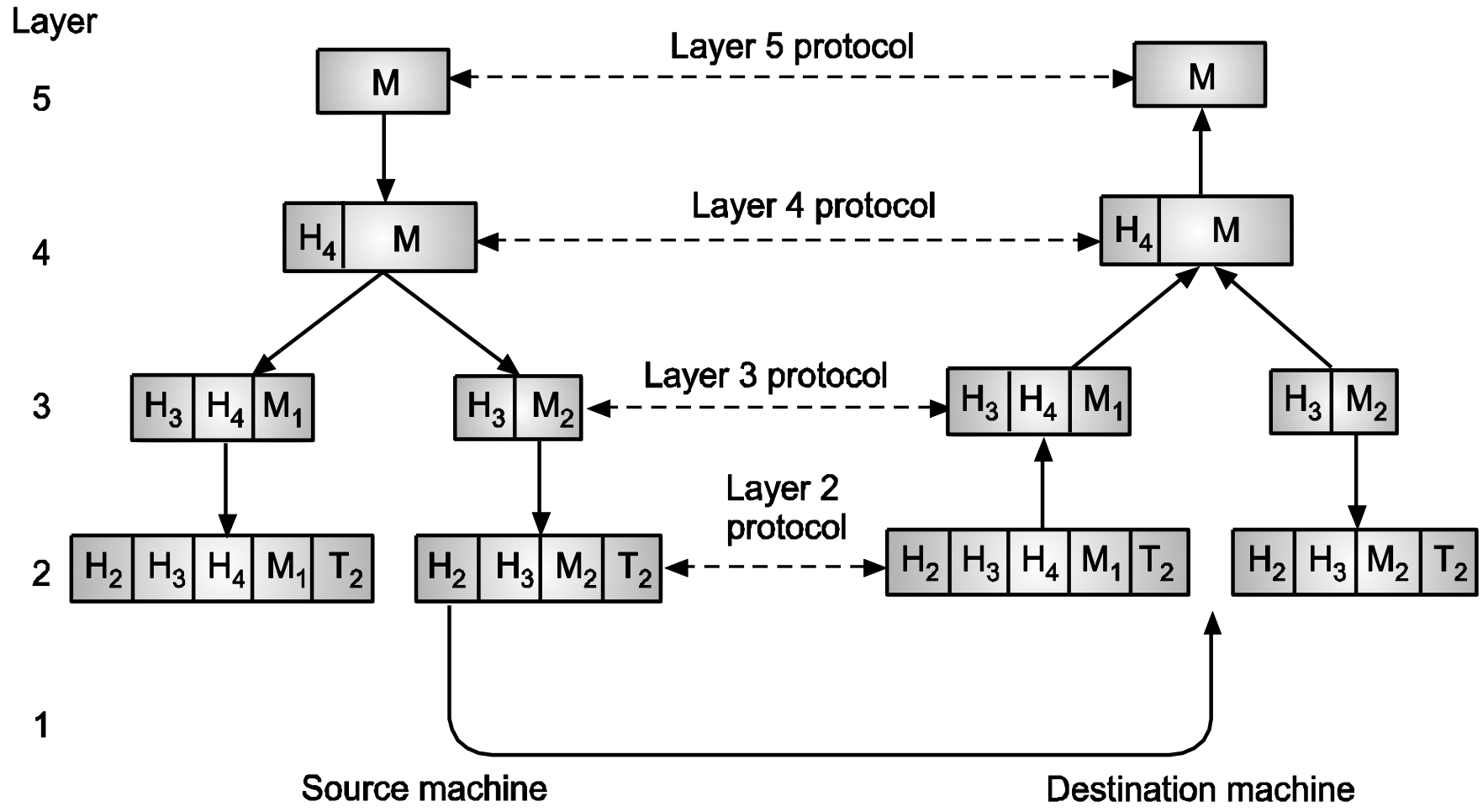
2. **CONNECT:** It connects the server by establishing a connection. The response is awaited.

3. **RECEIVE:** Then the RECEIVE call blocks the server.

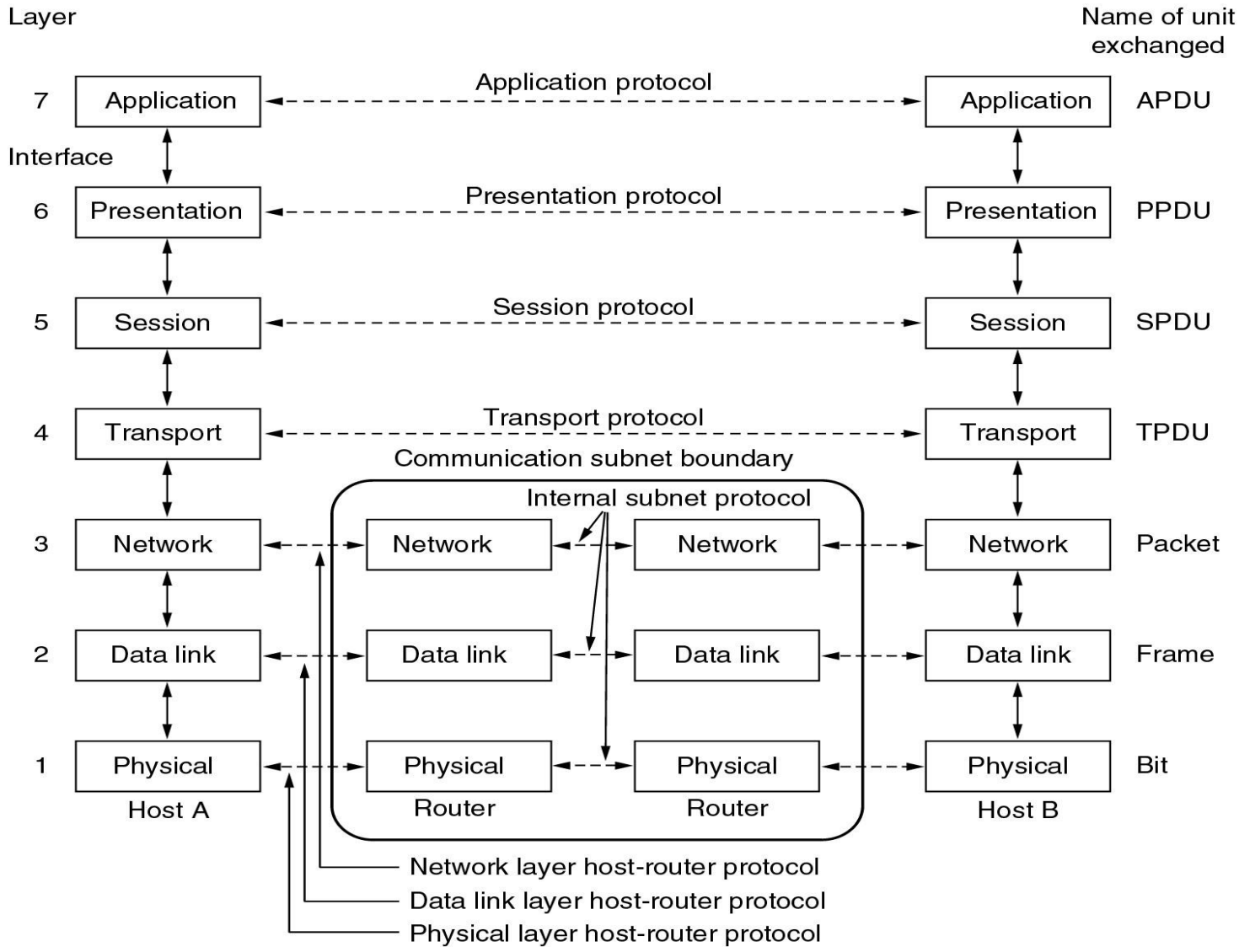
4. **SEND:** Then the client executes SEND primitive to transmit its request followed by the execution of RECIEVE to get the reply. Send the message.

5. **DISCONNECT:** This primitive is used for terminating the connection. After this primitive one can't send any message. When the client sends DISCONNECT packet then the server also sends the DISCONNECT packet to acknowledge the client. When the server package is received by client then the process is terminated.

Communication Between Layers



ISO-OSI Model



1. **Physical Layer:**

- It deals with the physical layout of the network.
- It deals with transmitting raw bits (0's and 1's) over the communication channel.
- The design issues here deal with the mechanical, electrical and timing interfaces and the physical transmission medium which lies below the physical layer.

2. **Data Link Layer:**

- It breaks the data into frames and passes it to the network layer.
- It deals with error control mechanism during transmission.
- It deals with the flow control mechanism to prevent the drowning of the slow receiver by the fast transmitter.
- It controls access to the shared medium.

3. Network Layer:

- It determines the network path on which to route the packet.
- Helps to reduce network congestion.
- Establishes virtual circuits.
- Routes frames to other network, resequencing packet transmission when needed.

4. Transport Layer

- Ensures reliability of packet transmission from node to node.
- Ensures data is sent and received in the same order.
- Provides acknowledgment when a packet is received.
- Monitors for packet transmission errors, and resends the damaged packets.

5. Session Layer

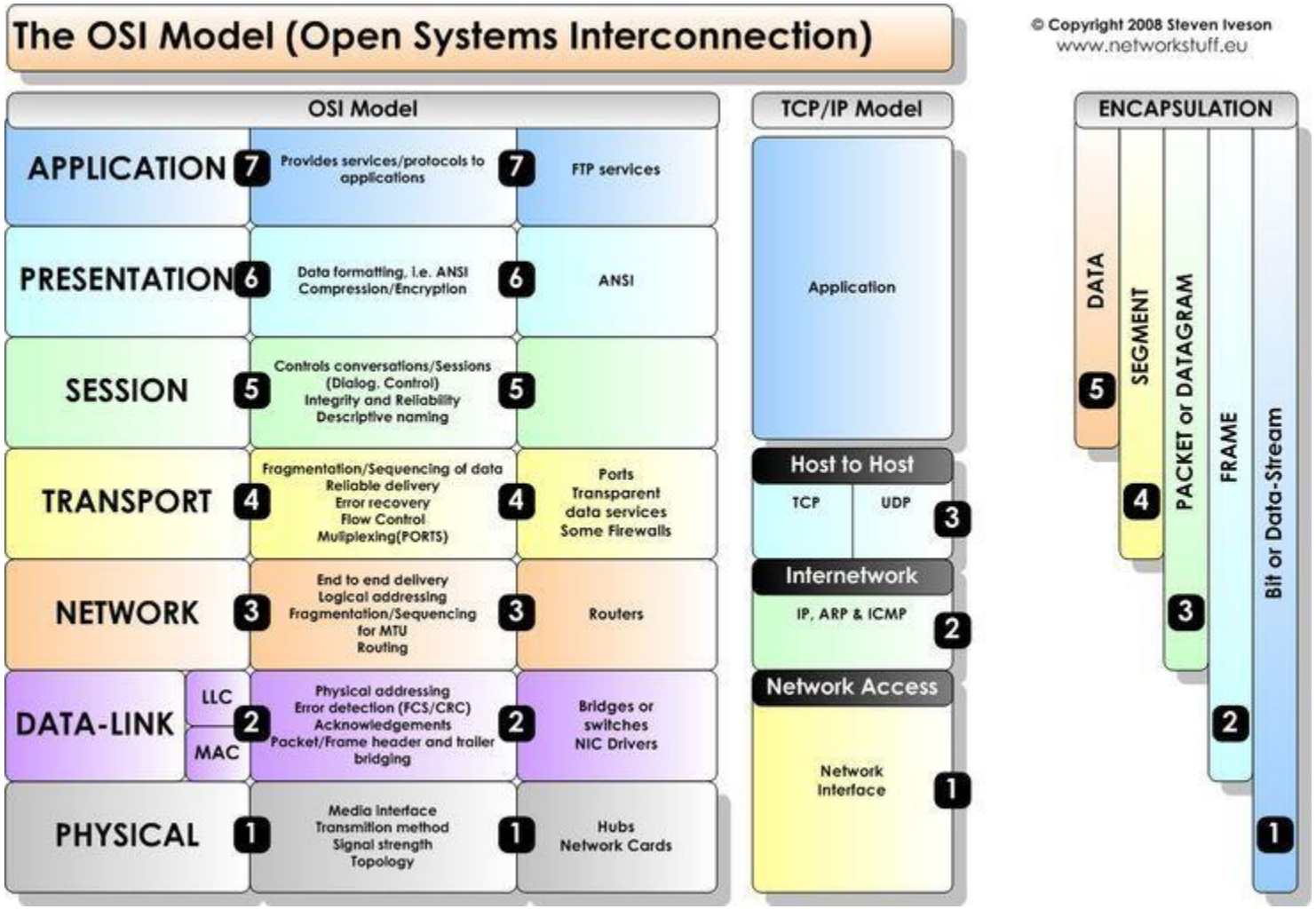
- It deals with dialogue control and synchronization to keep track of whose turn is it to transmit.
- It deals with token management to prevent two parties from attempting the same critical operation at the same time.
- It deals with check-pointing long transactions to allow them to continue from where they were after a crash.

6. Presentation Layer

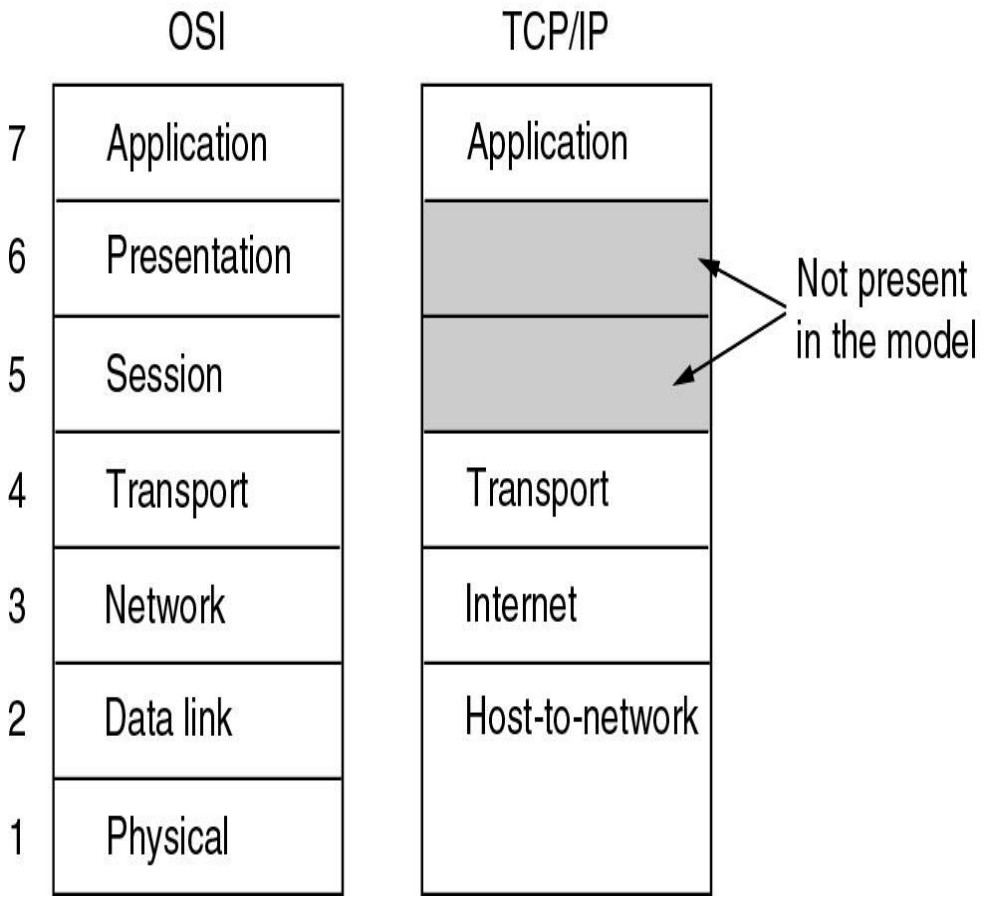
- It deals with syntax of information.
- It deals with semantics of information.
- It deals with compression of information.
- It also deals with encoding of information.

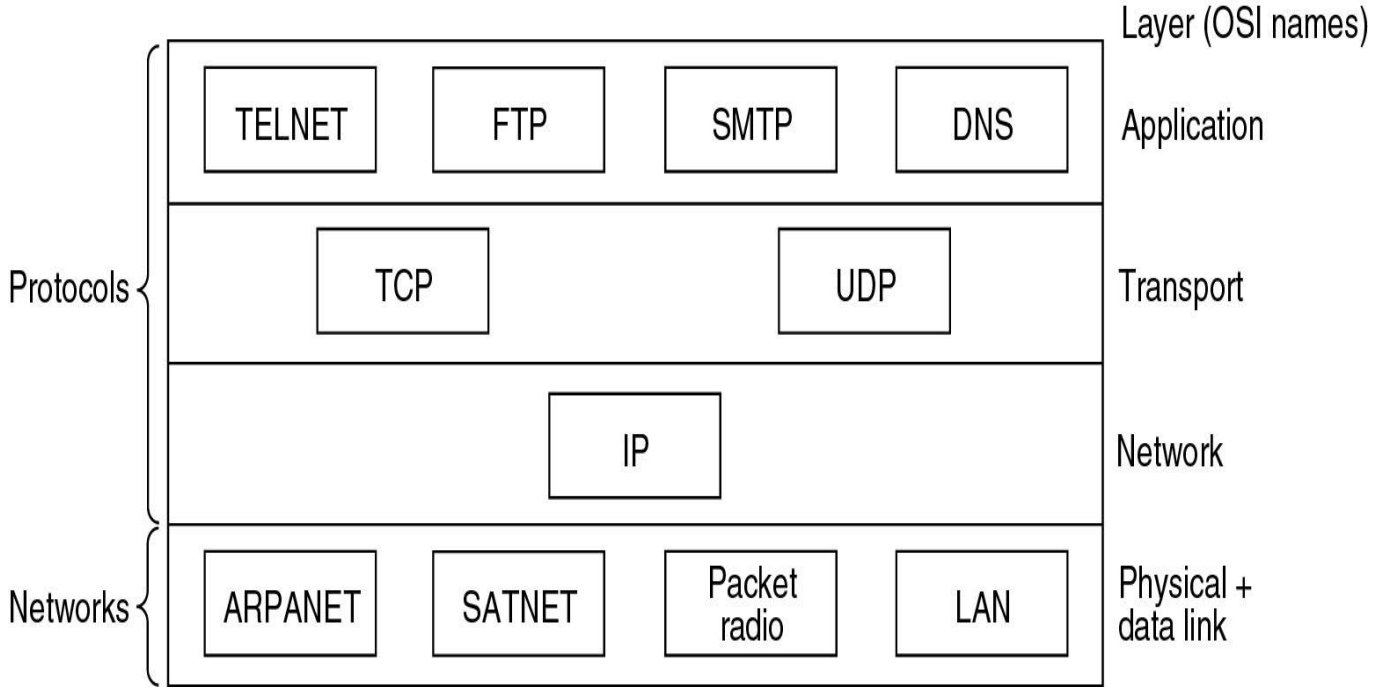
7. Application Layer

- Provides user interfaces.
- Support for services like Email, File transfer, Database Management, Remote File access.


The OSI Model (Open Systems Interconnection)
© Copyright 2008 Steven Iveson
www.networkstuff.eu
OSI Model
APPLICATION 7
Provides services/protocols to applications 7
FTP services
PRESENTATION 6
Data formatting, i.e. ANSI Compression/Encryption 6
ANSI
SESSION 5
Controls conversations/Sessions (Dialog. Control) Integrity and Reliability Descriptive naming 5
TRANSPORT 4
Fragmentation/Sequencing of data Reliable delivery Error recovery Flow Control Multiplexing(PORTS) 4
Ports Transparent data services Some Firewalls
NETWORK 3
End to end delivery Logical addressing Fragmentation/Sequencing for MTU Routing 3
Routers
DATA-LINK 2
LLC
MAC
Physical addressing Error detection (FCS/CRC) Acknowledgements Packet/Frame header and trailer bridging 2
Bridges or switches NIC Drivers
PHYSICAL 1
Media Interface Transmition method Signal strength Topology 1
Hubs Network Cards
TCP/IP Model
Application
Host to Host
TCP
UDP
3
Internetwork
IP, ARP & ICMP
2
Network Access
Network Interface
1
ENCAPSULATION
DATA
5
SEGMENT
4
PACKET or DATAGRAM
3
FRAME
2
Bit or Data-Stream
1

TCP/IP Model


OSI
TCP/IP
7
Application
6
Presentation
5
Session
4
Transport
3
Network
2
Data link
1
Physical
Application
Transport
Internet
Host-to-network
Not present
in the model


Layer (OSI names)
TELNET
FTP
SMTP
DNS
Application
Protocols
TCP
UDP
Transport
IP
Network
Networks
ARPANET
SATNET
Packet
radio
LAN
Physical +
data link

1. Network Access Layer (Host-to-Network Layer):

- A network access layer is the lowest layer of the TCP/IP model.
- A network access layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping IP addresses into physical addresses.
- The protocols used by this layer are Ethernet, Token ring, FDDI, X.25, and Frame relay.

2. Internet Layer:

- It permits hosts to inject packets into the network and make these packets reach their destination.
- It defines the packet format and protocol called the Internet Protocol (IP).
- Main focus is on packet routing.

3. Transport Layer:

- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
- It has two main protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- **TCP:**

(i) Reliable, connection-oriented.

(ii) Allows byte stream from one machine to be delivered to any other machine on the network.

(iii) Handles error control and flow control.

- **UDP:**

(i) Unreliable, connectionless.

(ii) Used for client-server type queries, where prompt delivery is more than reliability.

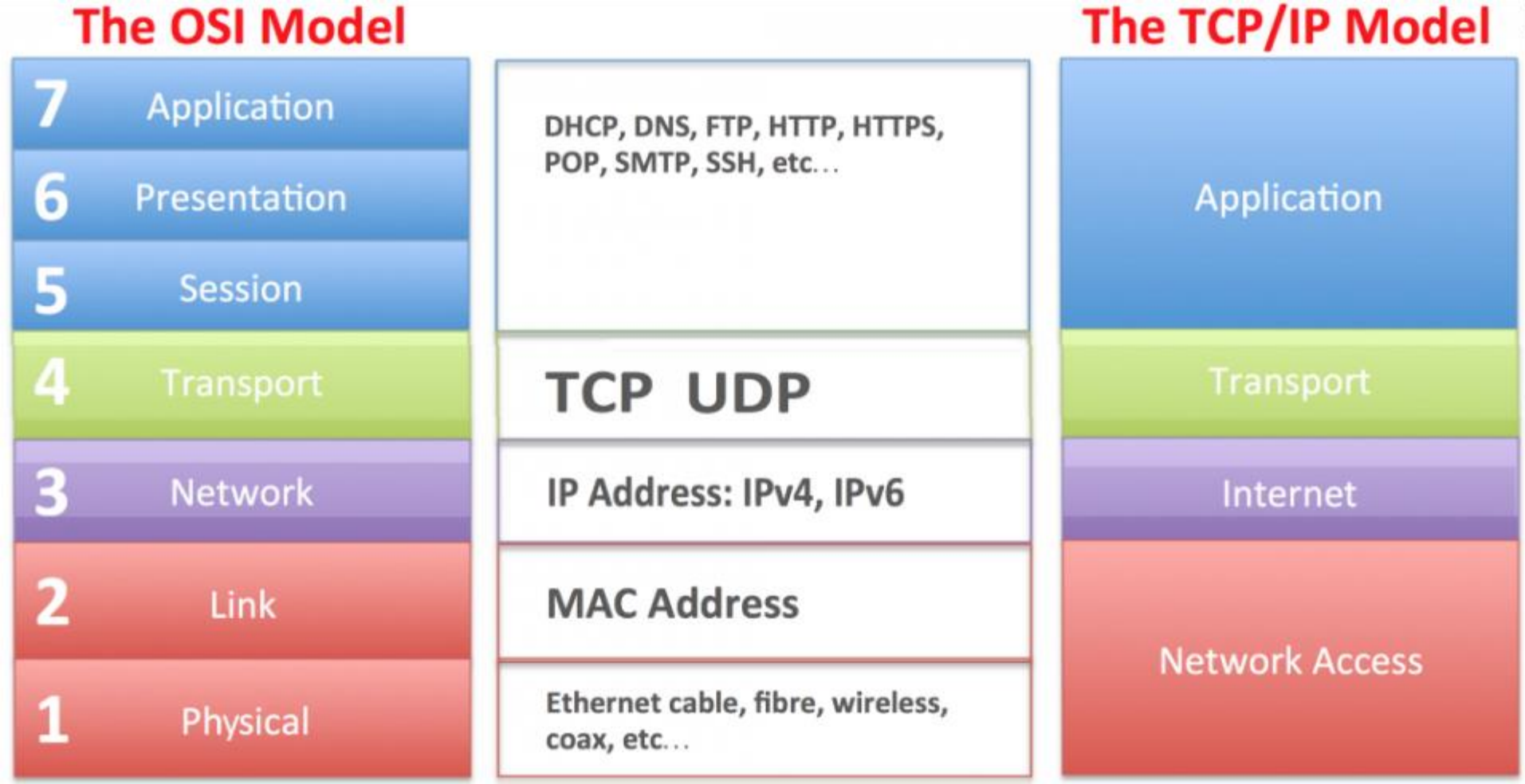
(iii) Does not implement flow or error control.

4. Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- Contains protocols like FTP, SMTP, HTTP, DNS, Telnet.

ISO-OSI Model Vs TCP/IP Model

OSI Model	TCP/IP Model
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI layers have seven layers.	TCP/IP has four layers.
In the OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In the OSI model, the data link layer and physical are separate layers.	In TCP, physical and data link are both combined as a single host-to-network layer.
Session and presentation layers are a part of the OSI model.	There is no session and presentation layer in the TCP model.
It is defined after the advent of the Internet.	It is defined before the advent of the internet.


The OSI Model
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Link
1 Physical
DHCP, DNS, FTP, HTTP, HTTPS, POP, SMTP, SSH, etc…
TCP UDP
IP Address: IPv4, IPv6
MAC Address
Ethernet cable, fibre, wireless, coax, etc…
The TCP/IP Model
Application
Transport
Internet
Network Access