UNIT 1
INTRODUCTION TO COMPUTER NETWORK

LH – 6HRS

Er. Sharat Maharjan
Computer Networking (CN)

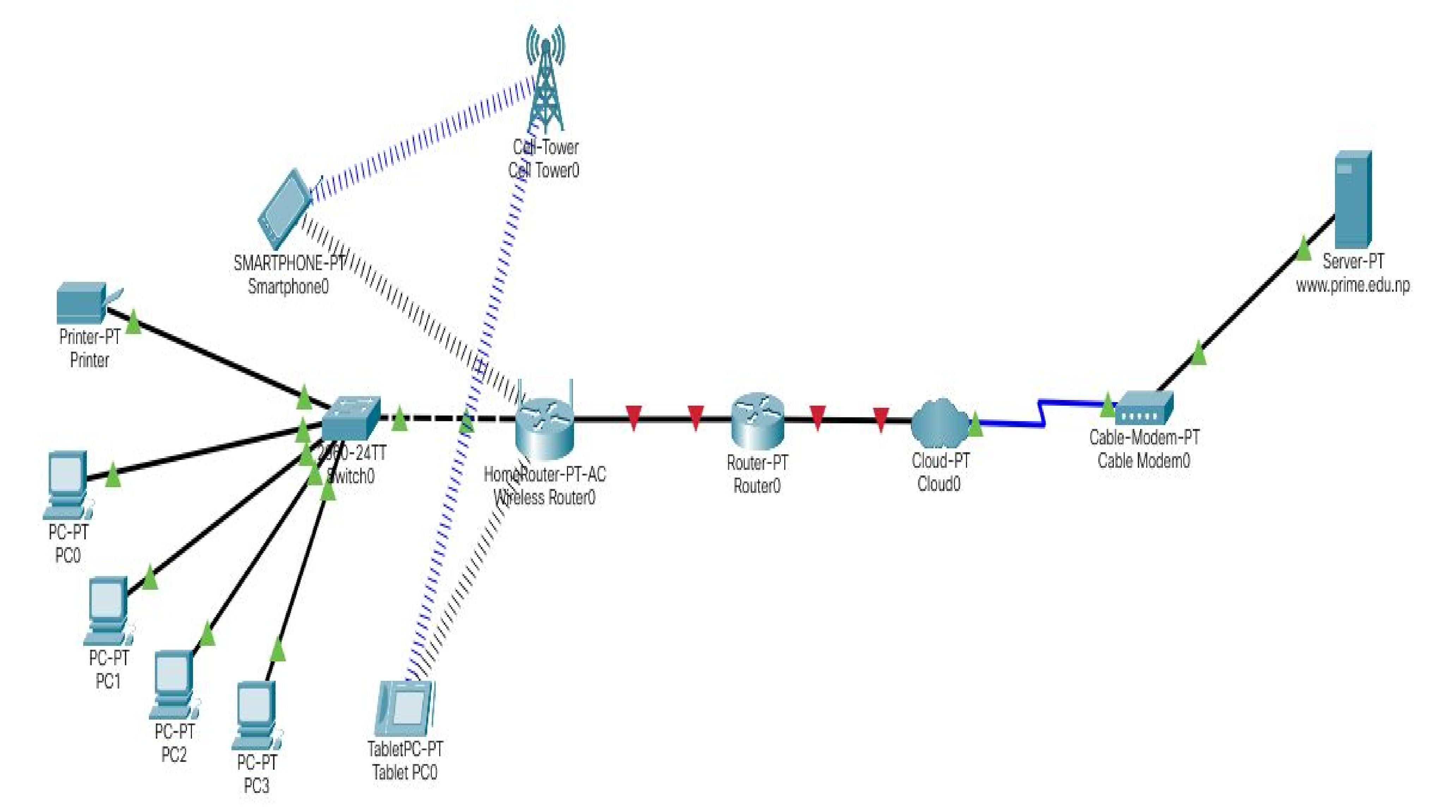
CONTENTS (LH - 6HRS)

- Network as an infrastructure for data communication
- Applications of Computer Network
- Network Architecture
- Types of Computer Networks
- Protocols and Standards
- The OSI Reference Model
- The TCP/IP Protocol Suite
- Comparison between OSI and TCP/IP Reference model
- Critiques of OSI and TCP/IP Reference model

What is Computer Network?

- A computer network is a number of computers (also known as nodes) connected by some communication lines.
- Two computers connected to the network can communicate with each other through the other nodes if they are not directly connected.
- Some of the nodes in the network may not be computers at all but they are network devices(Like switches, routers etc.) to facilitate the communication.

An example of Computer Network:



1.1 Network as an infrastructure for data communication

- Network infrastructure is the hardware and software resources of an entire network that enable network connectivity, communication, operations and management of an enterprise network.
- It enables computing and communication between users, services(e-mail), applications and processes.
- A typical network infrastructure includes:

a. Networking Hardware

b. Networking Software

c. Network Services

Network Infrastructure

a. Networking Hardware:

- Routers
- Switches
- Wireless routers
- Cables

b. Networking Software:

- Network operations and management
- Operating systems
- Firewall
- Network security applications

c. Network Services:

- Wireless Protocols (Bluetooth, Wi-Fi)
- Email
- Hardware Sharing
- IP addressing

- Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable (Guided or wired) or air (Unguided or wireless).
- For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. 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.

2. Accuracy: The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

3. Timeliness: The system must deliver data in a timely manner.

4. 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 millisecond. 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.

DATA COMMUNICATIONS COMPONENTS

A data communications system has five components:

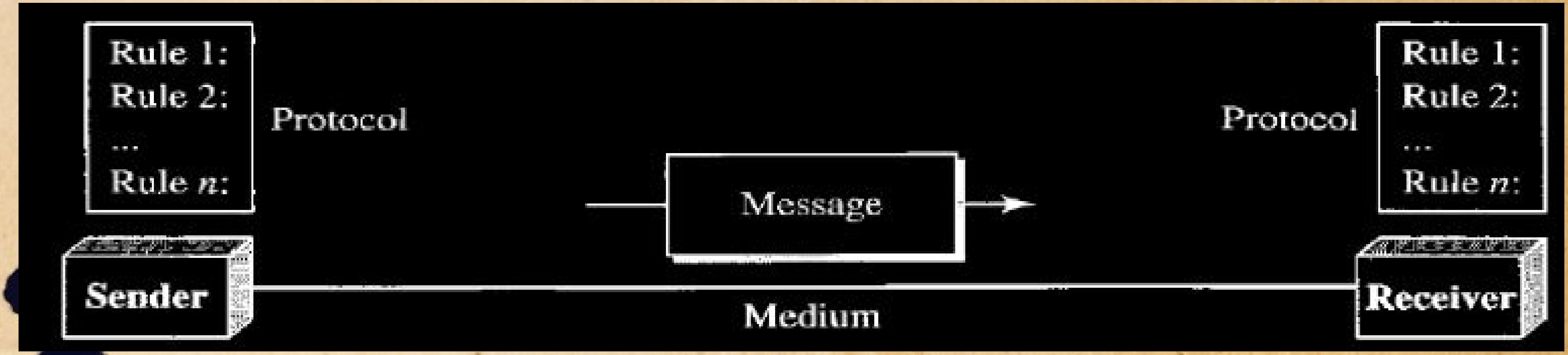
1. Message

2. Sender

3. Receiver

4. Protocol

5. Medium



Prepared By Er. Sharat Maharjan

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. Protocol: A protocol is a set of rules that governs data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating. For eg; HTTP, SMTP, FTP etc.

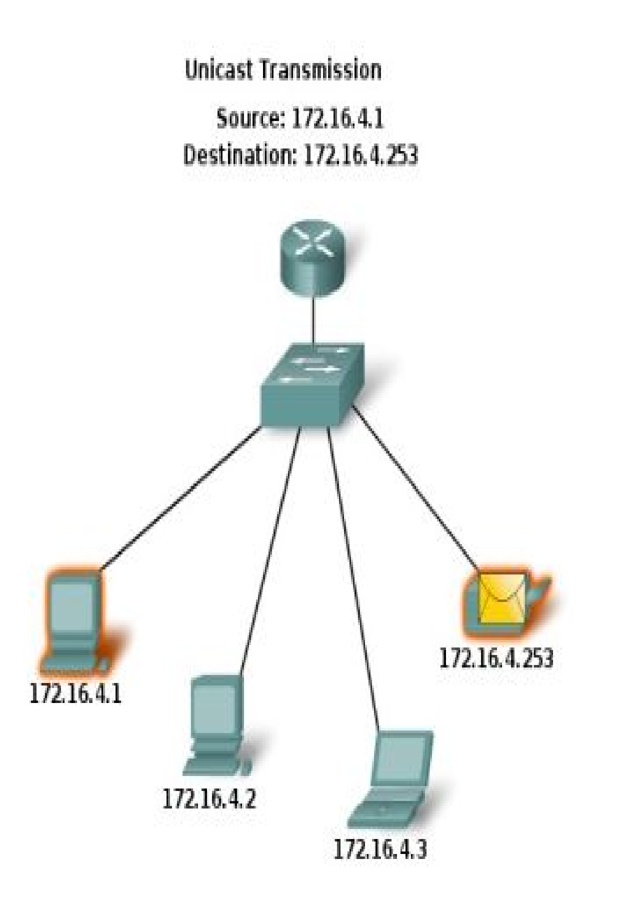
5. Transmission medium: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

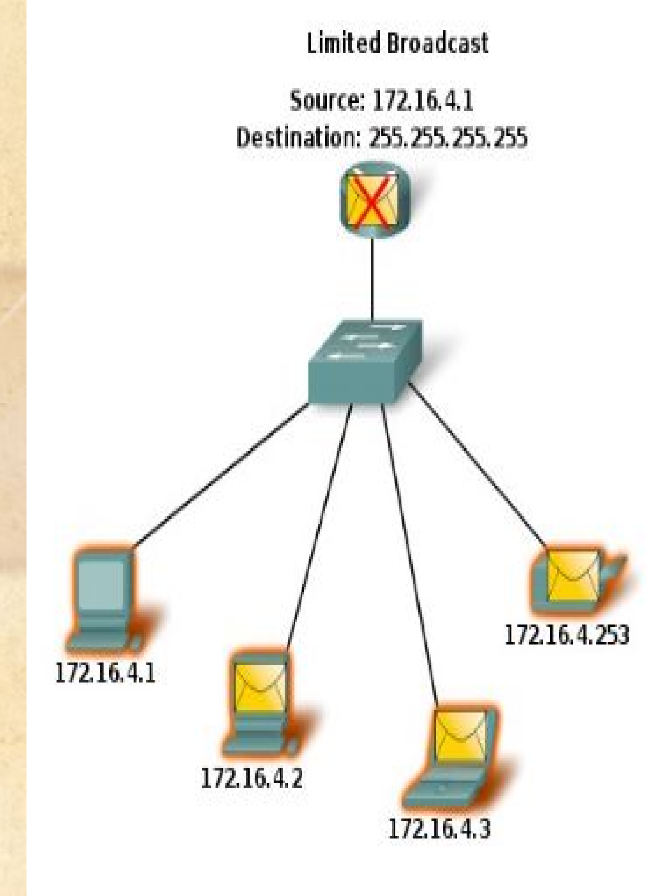
Modes of Communication:

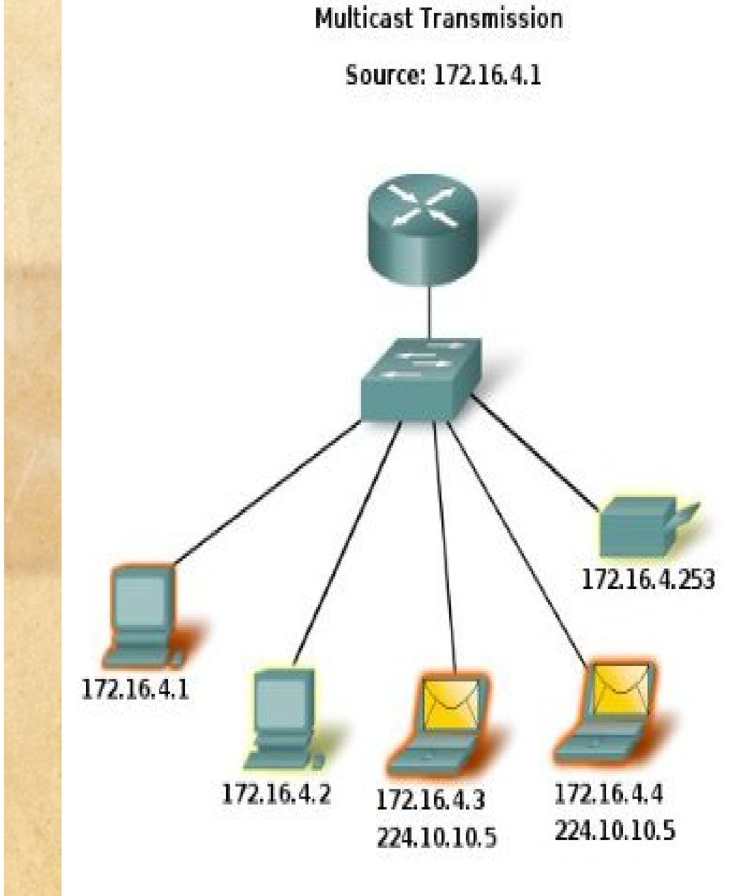
In an IPv4 network, the host can communicate in one of three different ways:

- **Unicast** - the process of sending a packet from one host to an individual host
- **Broadcast** - the process of sending a packet from one host to all hosts in the network
- **Multicast** - the process of sending a packet from one host to a selected group of hosts

Modes of Communication:







Modes of Transmission (Direction of Data Flow)

Communication between two devices i.e. sender & receiver can be of three types:

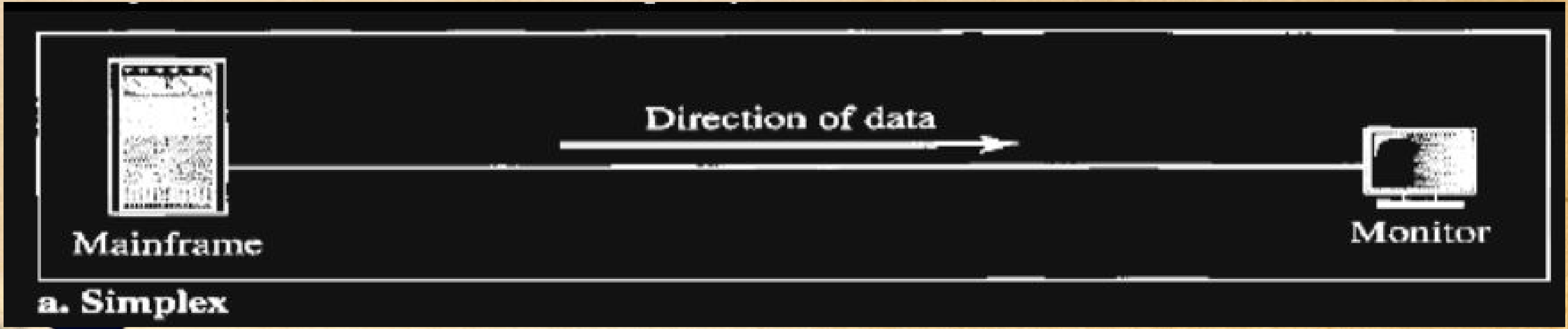
a. Simplex,

b. Half-duplex, or

c. Full-duplex

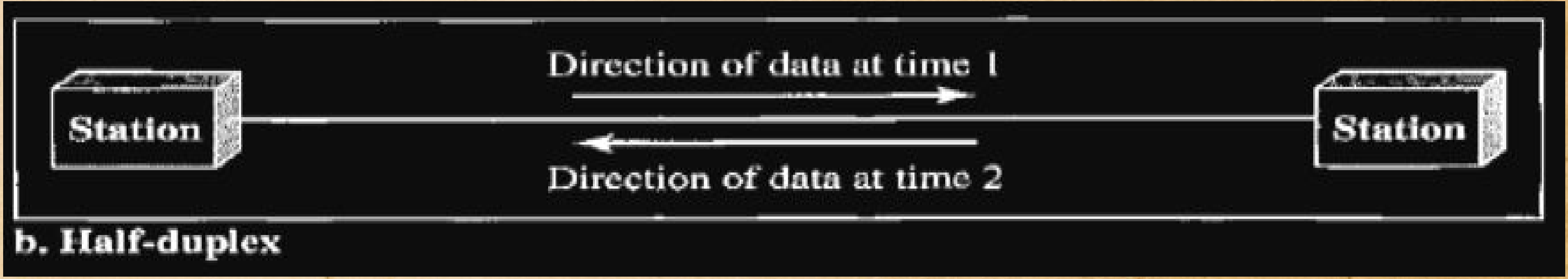
a. Simplex:

- In simplex mode, the communication is unidirectional, as on a one-way street.
- Only one of the two devices on a link can transmit; the other can only receive.
- The simplex mode can use the entire capacity of the channel to send data in one direction.
- Keyboards and traditional monitors are examples of simplex devices.



b. Half-duplex:

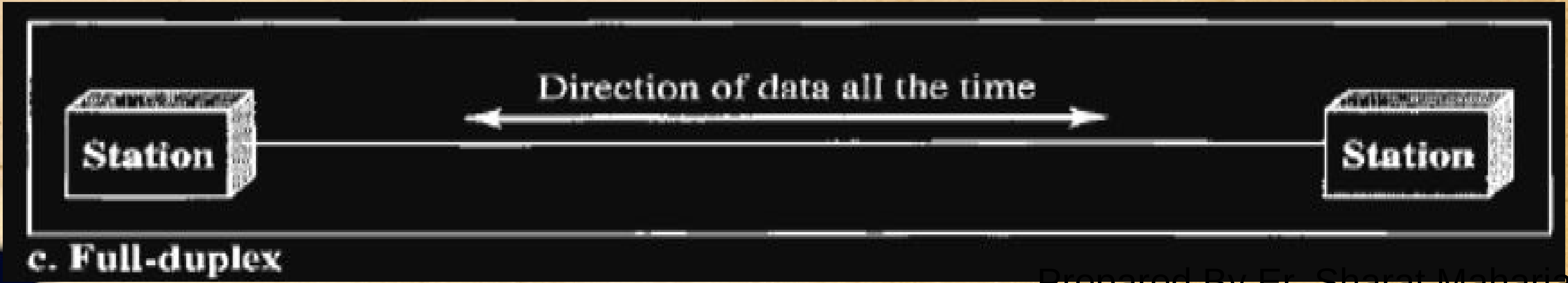
- In half-duplex mode, each station can both transmit and receive information, but not at the same time.
- When one device is sending, the other can only receive, and vice versa.
- The half-duplex mode can use the entire capacity of the channel to send data in both direction but not at the same time.
- Walkie-talkie is an example of half-duplex systems.



b. Half-duplex

c. Full-duplex:

- In full-duplex mode (also called duplex), both stations can transmit and receive information simultaneously.
- In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction.
- This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions.
- One common example of full-duplex communication is the telephone network.



1.2 Applications of Computer Network

1. Information and Resource Sharing: Computer networks allow organizations having units which are placed apart from each other, to share information in a very effective manner. Programs and software in any computer can be accessed by other computers linked to the network. It also allows sharing of hardware equipment, like printers and scanners among varied users.

2. Retrieving Remote Information: Through computer networks, users can retrieve remote information on a variety of topics. The information is stored in remote databases to which the user gains access through information systems like the World Wide Web.

3. E-Commerce: Computer networks have paved way for a variety of business and commercial transactions online, popularly called e-commerce. Users and organizations can buy or sell items, pay bills, manage bank accounts, pay taxes,transfer funds and handle investments electronically.

4. Speedy Interpersonal Communication: Computer networks have increased the speed and volume of communication like never before. Electronic Mail (email) is extensively used for sending texts, documents, images, and videos across the globe. Online communications have increased by many fold times through social networking services.

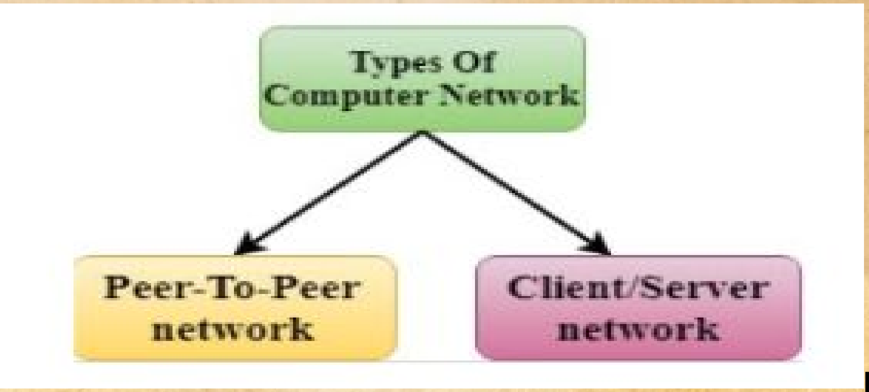
5. Highly Reliable Systems: Computer networks allow systems to be distributed in nature, by the virtue of which data is stored in multiple sources. This makes the system highly reliable. If a failure occurs in one source, then the system will still continue to function and data will still be available from the other sources.

6. Cost–Effective Systems: Computer networks have reduced the cost of establishment of computer systems in organizations. Previously, it was imperative for organizations to set up expensive mainframes for computation and storage. With the advent of networks, it is sufficient to set up interconnected personal computers (PCs) for the same purpose.

7. VoIP: VoIP or Voice over Internet Protocol has revolutionized telecommunication systems. Through this, telephone calls are made digitally using Internet Protocols instead of the regular analog phone lines.

1.3 Network Architecture

- Computer Network Architecture is defined as the physical and logical design of the hardware, software, protocols, and media of the transmission of data.
- Simply we can say that how computers are organized and how tasks are allocated to the computer.
- Architecture also defines how the computers should get connected to get the maximum advantages of a computer network such as better response time, security, scalability etc.
- The two types of network architectures are used:



1. Peer to Peer Architecture:

- In peer to peer architecture, all the computers in a computer network are connected with every computer in the network.
- Every computer in the network uses the same resources as other computers.
- There is no central computer that acts as a server rather all computers acts as a server for the data that is stored in them.

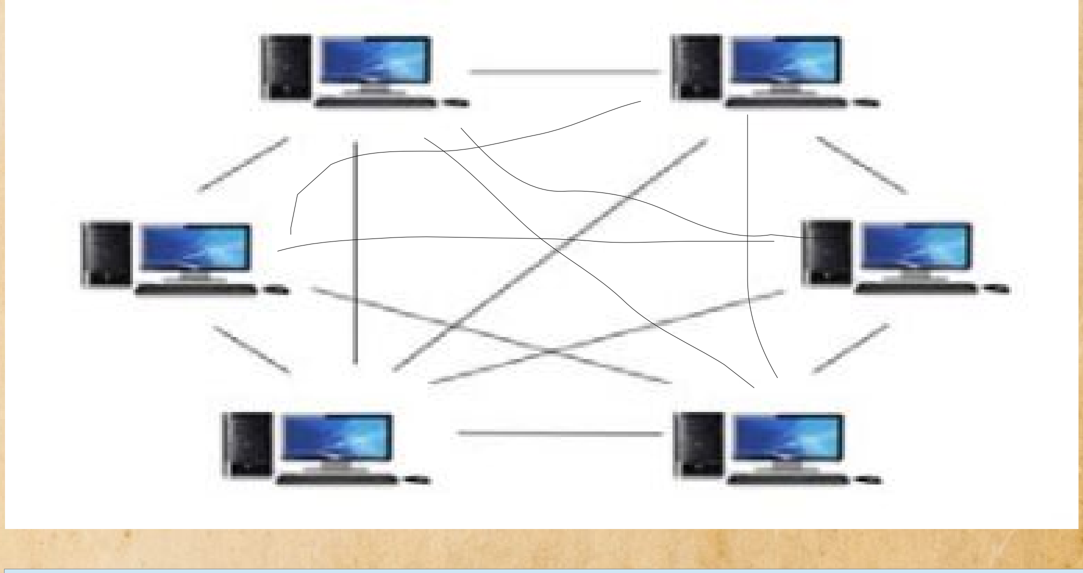


Fig: Peer to Peer Architecture

Advantages of a Peer to Peer Architecture:

- Less costly as there is no central server that has to take the backup.
- In case of a computer failure all other computers in the network are not affected and they will continue to work as same as before the failure.
- Installation of peer to peer architecture is quite easy as each computer manages itself.

Disadvantages of a Peer to Peer Architecture:

- Each computer has to take the backup rather than a central computer and the security measures are to be taken by all the computers separately.
- Scalability is an issue in a peer to peer architecture as connecting each computer to every computer is a headache on a very large network.

2. Client/Server Architecture:

- In Client Server architecture, a central computer acts as a hub and serves all the requests from client computers.
- All the shared data is stored in the server computer which is shared with the client computer when a request is made by the client computer.
- All the communication takes place through the server computer, for example if a client computer wants to share the data with other client computer then it has to send the data to server first and then the server will send the data to other client.
- The central controller is known as a server while all other computers in the network are called clients.

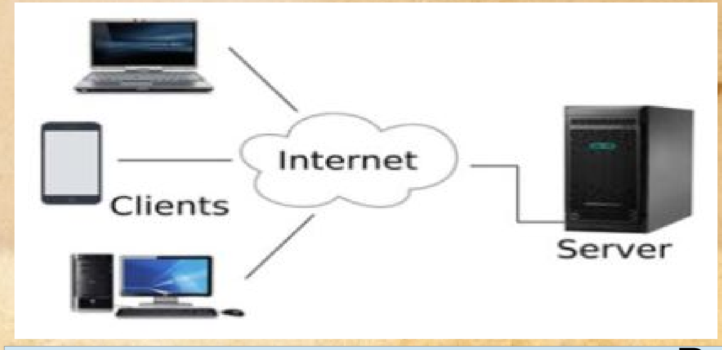


Fig: Client/Server Architecture

Advantages of Client Server Architecture:

- Data backup is easy and cost effective as there is no need to manage the backup on each computer.
- Performance is better as the response time is greatly improves because the server is more powerful computer than the other computers in the network.
- Security is better as unauthorized access are denied by server computer and all the data goes through the server.
- Scalability is not an issue in this Architecture as large number of computers can be connected with server.

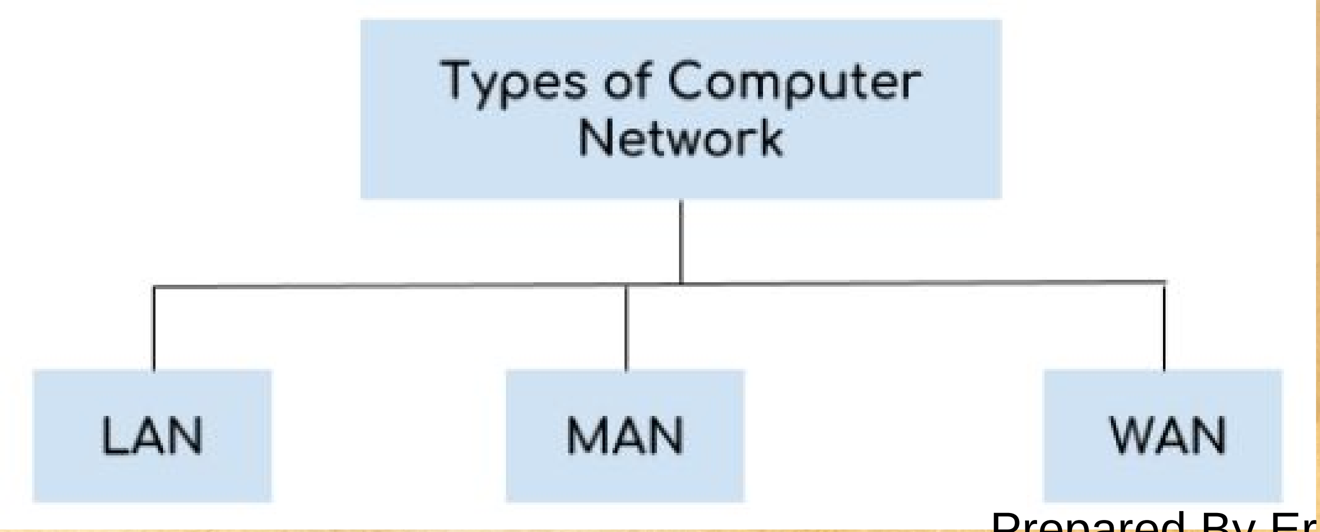
Disadvantages of Client Server Architecture:

- In case of server failure entire network is down.
- Server maintenance cost is high as the server is the main component in this Architecture.
- Cost is high as the server needs more resources to handle that many client requests and to be able to hold large amount of data.

1.4 Types of Computer Networks

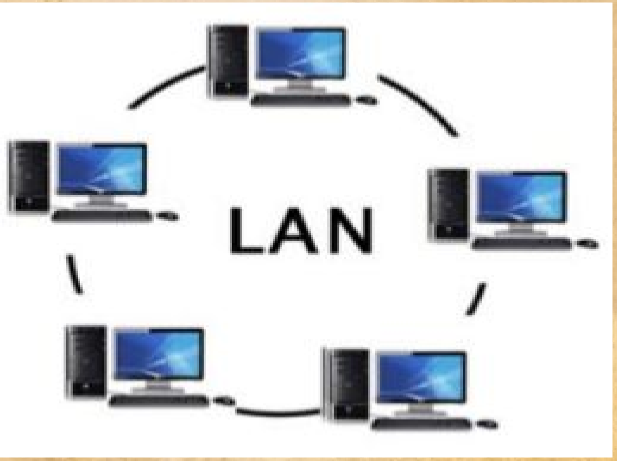
- A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.
- A computer network can be categorized by their size.

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide area network (WAN)



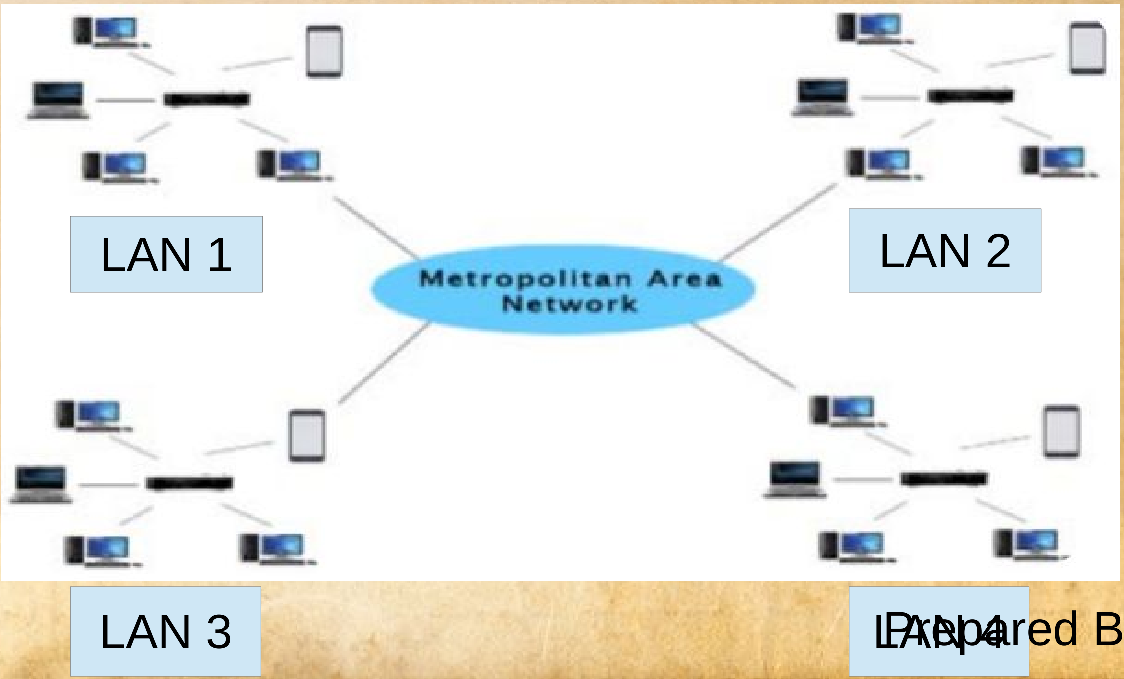
1. Local Area Network (LAN):

- 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, 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.
- Local Area Network provides higher security.



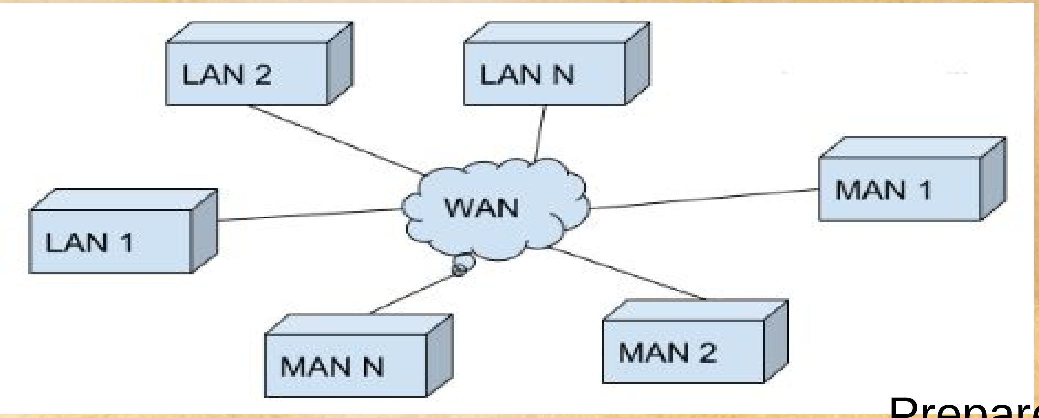
2. MAN (Metropolitan Area Network):

- MAN network covers larger area by connections LANs to a larger network of computers.
- In MAN, various Local area networks are connected with one another.
- The size of the Metropolitan area network is larger than LANs and smaller than WANs (wide area networks), a MANs covers the larger area of a city or town.



3. 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 MAN.
- A Wide Area Network is not limited to a single location, but 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.



Advantages of Wide Area Network (WAN):

- **Geographical area:** A WAN provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype etc.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global Business:** We can do the business over the internet globally.
- **High bandwidth:** The high bandwidth increases the data transfer rate which in turn increases the productivity.

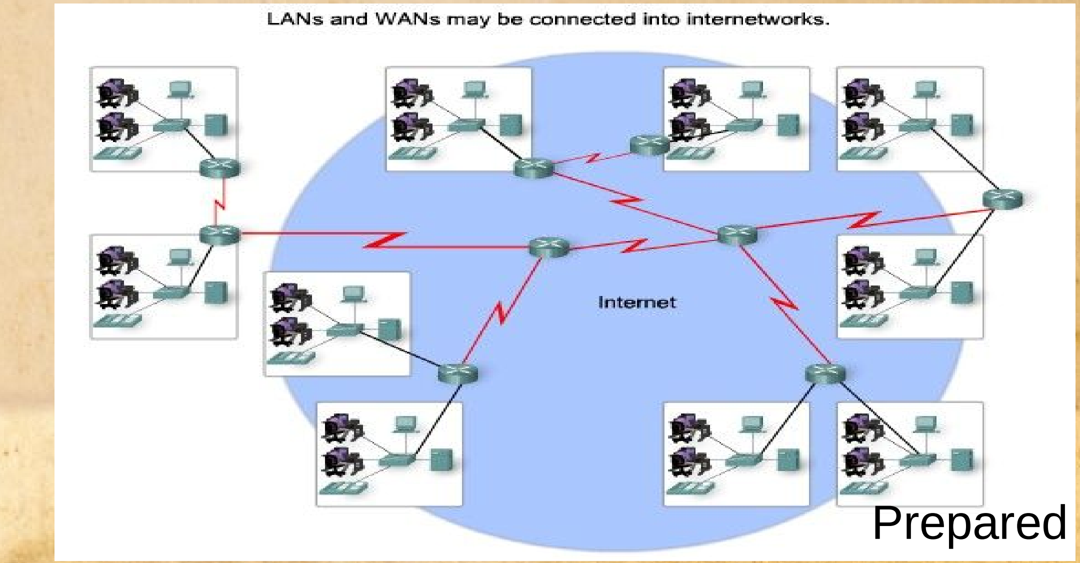
Disadvantages of Wide Area Network (WAN):

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

Internet:

The Internet is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices.

- Network of Networks.
- No one owns the Internet.
- Every person who makes a connection owns a slice of the Internet.
- There is no central administration of the Internet.


LANs and WANs may be connected into internetworks.

Internet comprises of :

- People : who use and develop the network.
- Resources: a collection of resources that can be reached from those networks.
- A setup to facilitate collaboration: among the members of the research and educational communities world wide.
- The connected networks use the TCP/IP protocols.

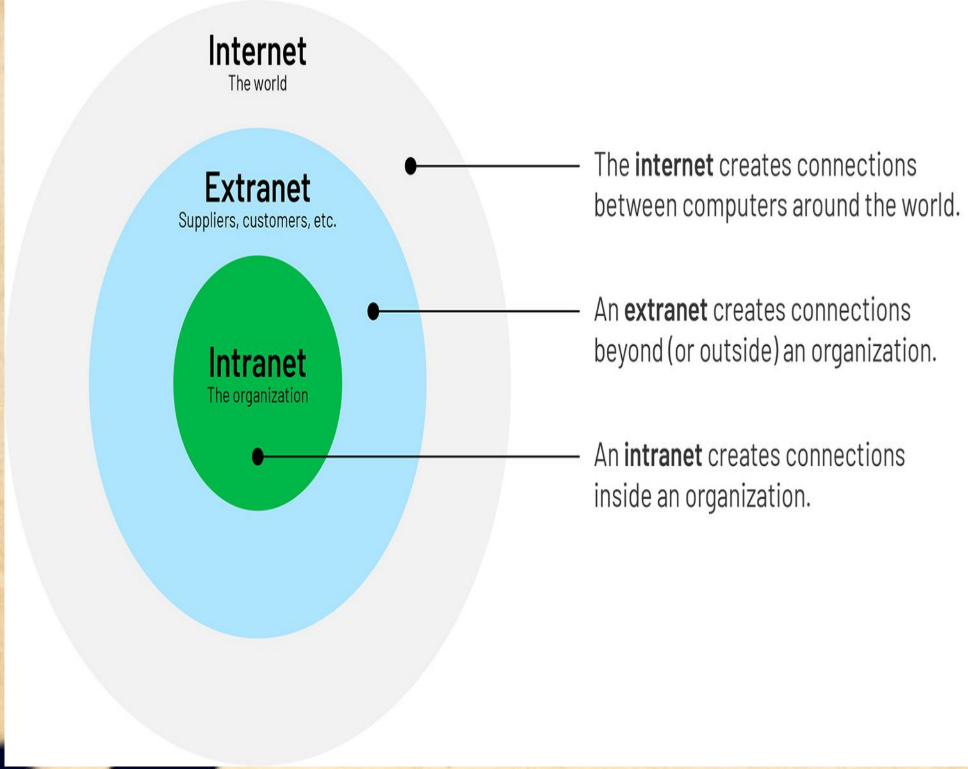
Important Internet applications:

- Sending and receiving email.
- Conducting financial transactions.
- Playing interactive games.
- Video and music streaming.
- Chat or voice communication.

Intranet:

- A private network within an organization (mini internet) that uses internet technologies such as web servers and web browsers for sharing information and collaborating, but is insulated from the global internet.
- Intranets can be used to publish company policies, newsletters etc.
- Intranet web servers differ from public web servers in that the public must have the proper permissions and passwords to access the intranet of an organization.
- Intranets are designed to permit users who have access privileges to the internal LAN of the organization. So it is highly secure than internet.

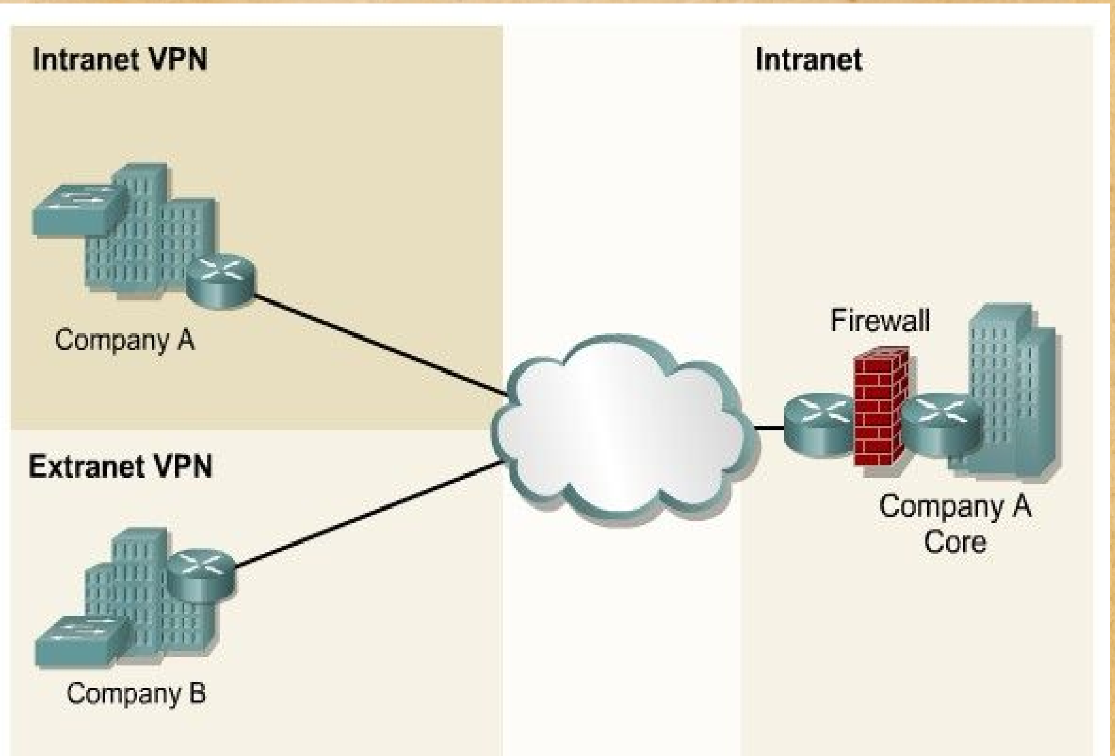
- Within an intranet, web servers are installed in the network.
- Browser technology is used as the common front end to access information on servers such as financial, graphical, or text-based data.
- A good example of an intranet network would be banking network.



The **internet** creates connections between computers around the world.

An **extranet** creates connections beyond (or outside) an organization.

An **intranet** creates connections inside an organization.



Extranet:

- Extranets extend the reach of intranets from internal-only communications to sharing documents, fixing software bugs, and providing information for business-to-business transactions.
- Extranets are a powerful tool because they let businesses share resources on their own private networks over the Internet with suppliers, vendors, business partners, or customers (online bank).
- The power of the extranet is that it leverages(uses) the existing technology of the Internet to increase the power, flexibility, and competitiveness of businesses.
- Extranets also save companies' money by allowing them to establish business-to-business connectivity over the Internet (use of already available cable/lines) instead of using expensive, dedicated leased lines.
- Online banking is an example of an extranet.

Network Topology:

- Network topology is an arrangement of two or more nodes communicating with each other, typically over the internet through a particular medium.
- There are two approaches to network topology: physical and logical.

a. Physical topology: The physical network topology refers to the actual connections (wires, cables, etc.) of how the network is arranged.

b. Logical topology: The logical network topology is a higher-level idea of how the network is set up, including which nodes connect to each other and in which ways, as well as how data is transmitted through the network.

Network Topology Types:

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

1. Bus Topology:

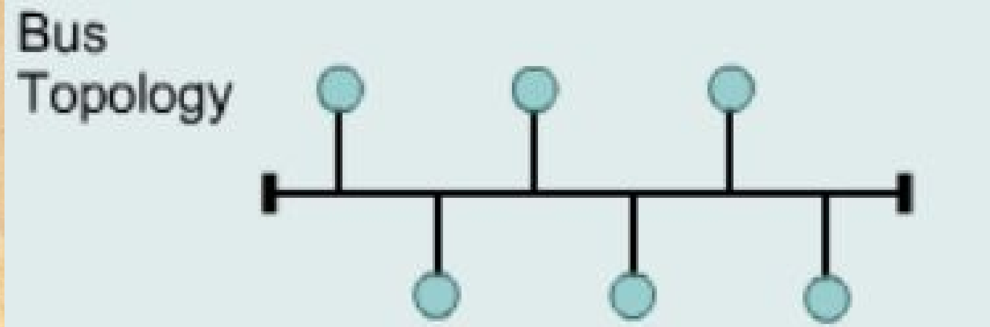
A networking topology that connects networking components along a single cable which is known as the backbone.

Uses:

- It is generally used over a small network such as LAN.

Advantages:

- Easy to install.
- Costs are usually low.
- Easy to add systems to network.
- Great for small networks.



Disadvantages:

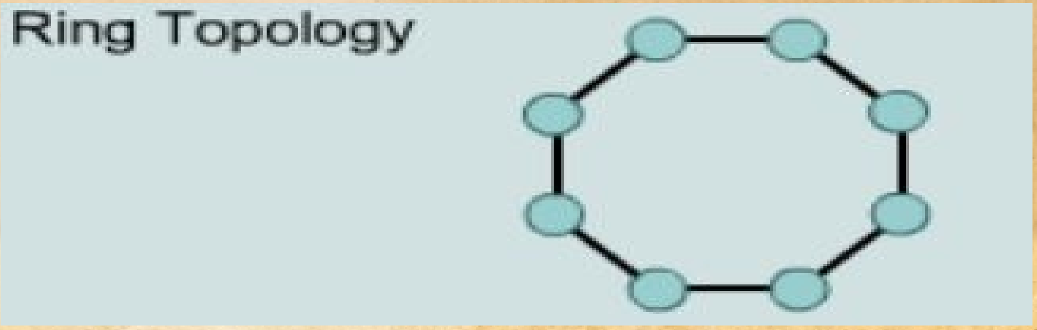
- A single cable break will bring down the bus topology.
- Can be difficult to troubleshoot.
- Unmanageable in a large network.

2. Ring Topology:

- As the name suggests, ring topology forms a ring by connecting participants nodes.
- Nodes are connected in such a way that a single wire forms the path whose ends are joined to form a circle.
- Ring topology uses the token concept where the token is transmitted along with the message for the correct delivery of the message.

Uses:

- A small office with only a few nodes may use a ring network topology.



Advantages:

- No master-slave concept.
- Each node has its own share of responsibility.
- Could work in a high capacity network.

Disadvantage:

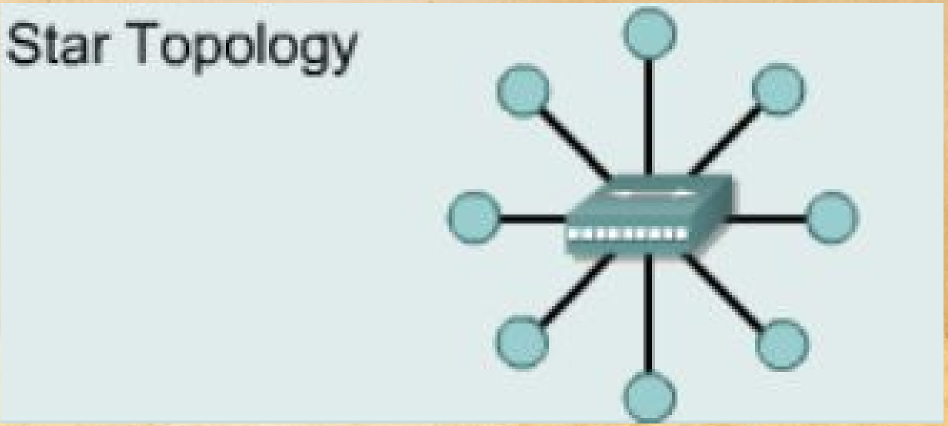
- A single node failure affects the complete network.
- Sometimes it becomes difficult to troubleshoot if the network is too large.
- Adding or manipulating the network affects other participants nodes.

3. Star Topology:

- A star topology generally consists of a central hub.
- Every participant node is directly connected to this hub.
- Hub acts as a central point to receive the message from the sender node and then transmits it to other participant nodes.
- There is no direct connection between nodes.

Uses:

- Used in large organizations, such as educational establishments and businesses, where high performance is a must..



Advantages:

- A single node failure does not affect the complete network.
- The network can run smoothly as far as the centralized hub is running smoothly.
- It is more cost-effective since the centralized network reduces network administration(maintaining network and solving any problem) cost highly.

Disadvantages:

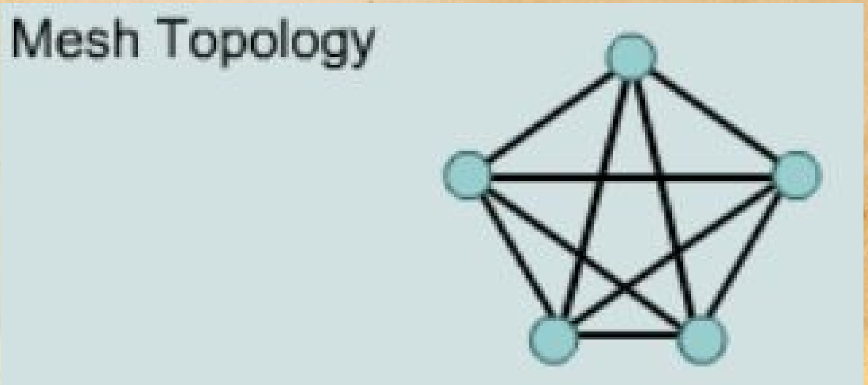
- Failure of the central hub will disrupt the whole topology.
- It is slightly costly when compared to the bus topology.

4. Mesh Topology:

- Mesh Topology generally forms a mesh of all the interconnected nodes.
- Here each node is connected to every other node through a single one-to-one communicating wire.
- There is a one-to-one mapping between each node.

Uses:

- They help organizations provide a consistent connection throughout a physical space..



Advantages:

- Better fault-tolerance capacity(continue working even when a node is down in network).
- Failure of one participant nodes will not affect the complete network.
- If there is a breakdown in one path between two nodes, then an alternate path is always available.

Disadvantages:

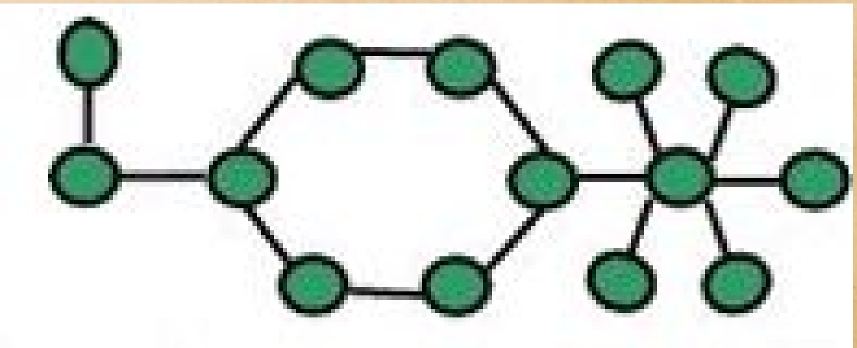
- The network becomes too complex as there are large participants nodes.
- It becomes costly due to the set-up of multiple paths.

5. Hybrid Topology:

- Hybrid topologies combine two or more different topology structures.

Use:

- Hybrid structures are most commonly found in larger companies.



Hybrid Topology

Advantages:

- This type of topology combines the benefits of different types of topologies in one topology.
- Can be modified as per requirement.
- It is extremely flexible.

Disadvantages:

- It is a type of expensive network topology.
- Design of a hybrid network is very complex.
- Installation process is a difficult.

1.5 Protocols and Standards

- Protocols provide us with a medium and set of rules to establish communication between different devices for the exchange of data and other services.
- It specifies what type of data can be transmitted and how data transfers are confirmed.
- Protocol is an agreement between a sender and a receiver, which states how communication will be established, and how to maintain & release it.
- The key elements of the protocol determine what to be communicated, how it is communicated, and when it is communicated.
- There are mainly three key elements of a protocol, they are as follows:
  - Syntax
  - Semantics
  - Timing

Elements of PROTOCOLS:

1. Syntax:

- Syntax refers to the structure or format of data.
- It indicates how to read the data in the form of bits or fields.
- **Example:** A protocol might expect that the size of a data packet will be 16 bits. In which, the first 4 bits are the sender's address, the next 4 bits are the receiver's address, the next 4 bits are the check-sum bits, and the last 4 bits will contain the message(body). So, every communication which is following that protocol should send 16-bit data.

2. Semantics:

- Semantics refers to the interpretation or meaning of each section of bits or fields.

Example: It interprets whether the bits of address identify the route to be taken or the final destination of the message or something else.

3. Timing:

- Timing refers to two characteristics:
  - when the data should be sent?
  - what will be the speed of sending and receiving the data?
- It performs speed matching and flow control(management of data flow) of the data items.
- **Example:** A sender can send the data at a speed of 100 Mbps, but the receiver can consume it only at a speed of 20 Mbps, then there may be data losses. So, proper synchronization must be there between a sender and a receiver.

Functions of protocols

Following are the main functionalities of a protocol:

- **Data Sequencing:** It mainly refers to assign the unique sequence number to segmented data so that the receiver upon receiving can rearrange in that order.
- **Data Flow:** It mainly deals with sending data to the correct destination i.e. the flow of the data is correct or not.
- **Data Routing:** It refers to select the best path for data transmission between a sender and a receiver because there can be many routes from sender to receiver and one should select the best possible route.
- **Encapsulation:** It refers to the process of adding some information on data in each layer and upon receiving message will be de-capsulated.

- **Segmentation & Reassembly:** It deals with segmenting the big data message into segments and reassembly is vice-versa of segmentation i.e. all the segments are recollected in the correct order at the receiver side.
- **Connection Control:** It ensures connection oriented data transfer for lengthy data items.
- **Multiplexing:** It allows combining multiple transmission unit signals of higher-level protocols in one transmission unit of a lower-level protocol.
- **Flow Control**: It facilitates to limit the flow of data so that messages are sent and received as expectedly.
- **Error Control**: It deals with error detection and its control. If any error is detected during the transmission of the data, a request for retransmission of data is sent to the sender by the receiver, and the corrupt data packet is discarded.

Standards

- Standards are the set of rules for data communication that are needed for exchange of information among devices.
- It is important to follow Standards which are created by various Standard Organization like IEEE , ISO , ANSI etc.
- Data communication standards fall into two categories:

1. de facto (meaning "by fact" or "by convention")

2. de jure (meaning "by law" or "by regulation")

Two Categories of Standards

1. De facto: Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards(QWERTY keyboard, Windows operating system).

2. De jure: Those standards by law or by regulation. These are the standards recognized officially by an Organization(SMTP, TCP, IP).

Standards Organizations

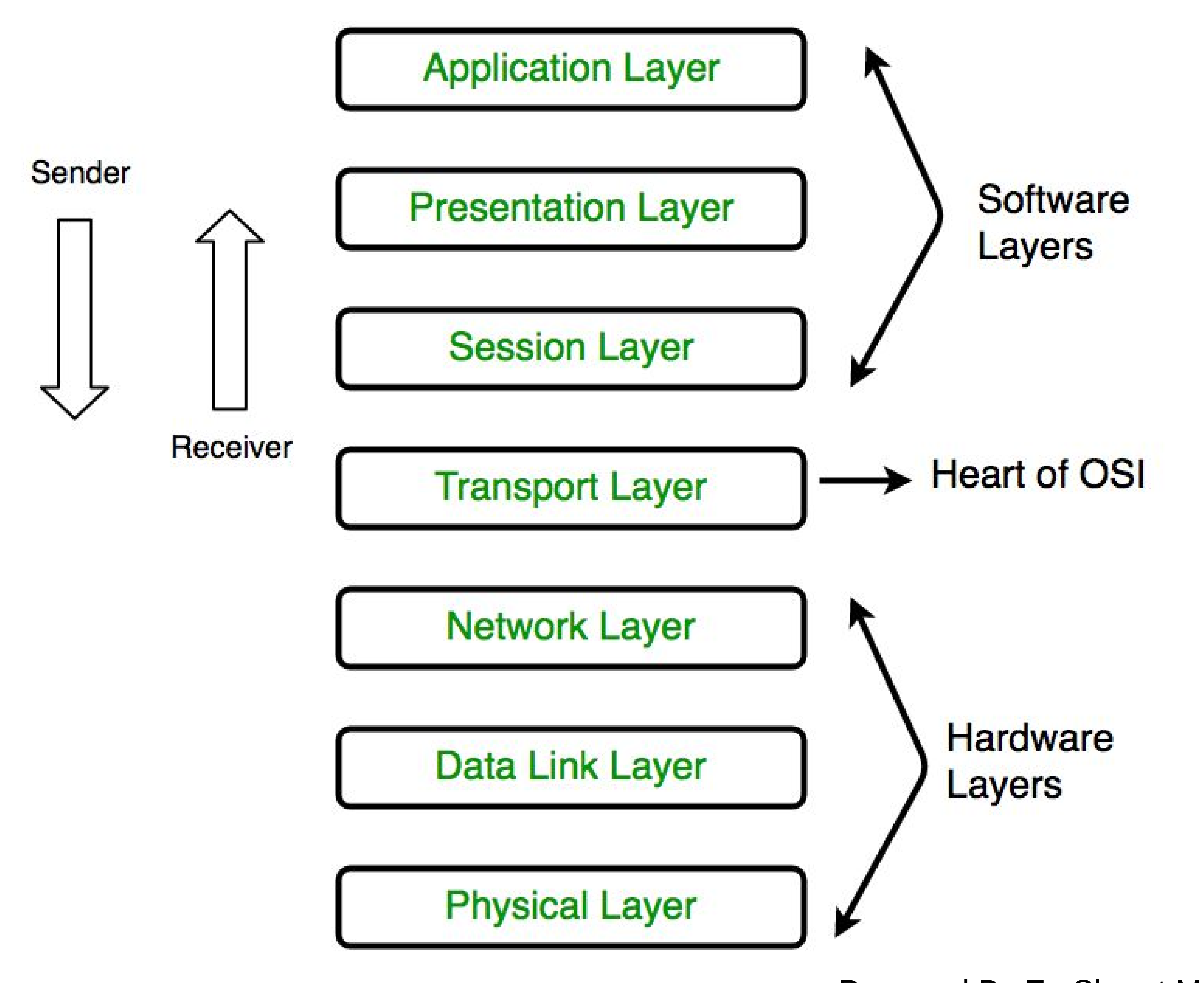
Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

Some of the noted standards organizations are

- International Organization of Standardization(ISO)
- American National Standards Institute(ANSI)
- Electronic Industries Association(EIA)
- Institute of Electrical and Electronics Engineers(IEEE)

1.6 The OSI Reference Model

- OSI stands for Open Systems Interconnection.
- It has been developed by ISO – ‘International Organization for Standardization‘, in the year 1984.
- It is a 7 layer architecture with each layer having specific functionality to perform.
- All these 7 layers work collaboratively to transmit the data from one person to another across the globe.
- The process of breaking up the functions or tasks of networking into layers reduces complexity,easy to troubleshoot and is called layering.



Sender

Receiver

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

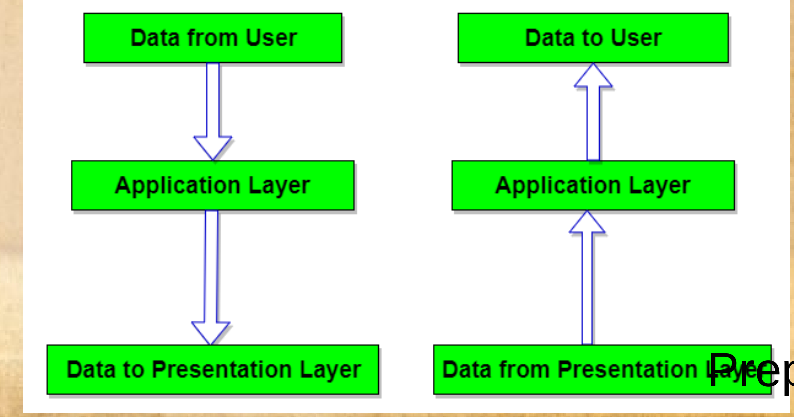
Software Layers

Heart of OSI

Hardware Layers

7. Application Layer:

- It is the top most layer(Layer 7) of OSI model which enables the user to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer etc.
- Web browsers are examples of network application.
- Examples of protocols that run at the application layer include File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP) etc.
- The figure shows the relationship of the application layer to the user and the presentation layer.



Functions of Application Layer:

- **File transfer, access and management:** It provides facilities so that a user can access and retrieve files in a remote computer for local usage, as well as manage and store files on a remote computer from the local computer.
- **Mail services:** It provides e-mail services.
- **Directory services:** It helps to retrieve global information and services by providing access to distributed database resources.

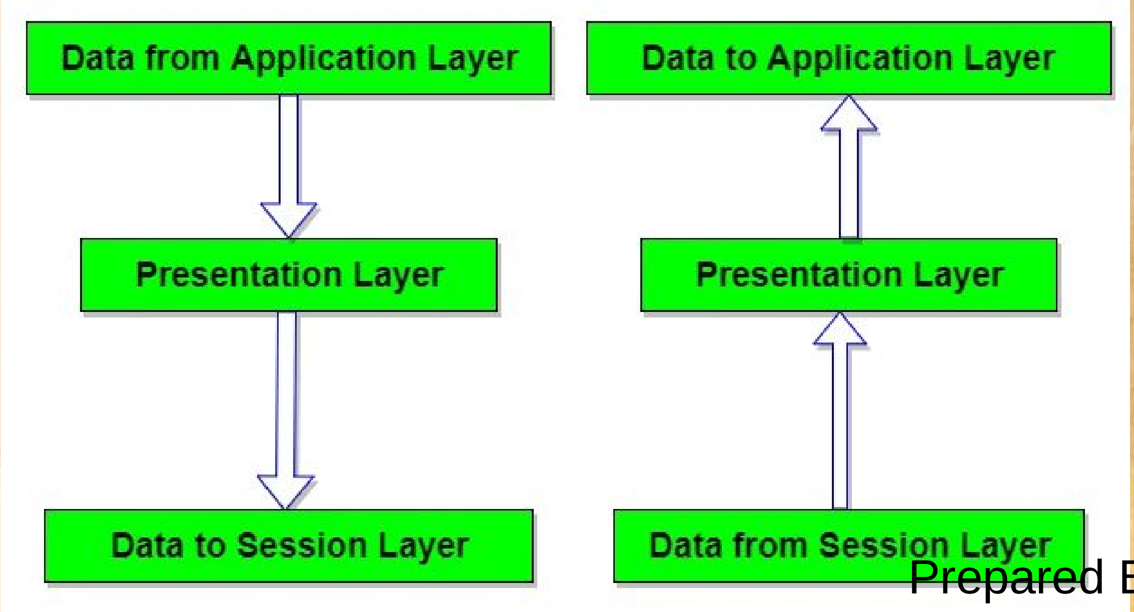
6. Presentation Layer:

- The presentation layer (Layer 6) ensures that the message is presented to the upper layer in a standardized format.
- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems .

Functions of Presentation Layer:

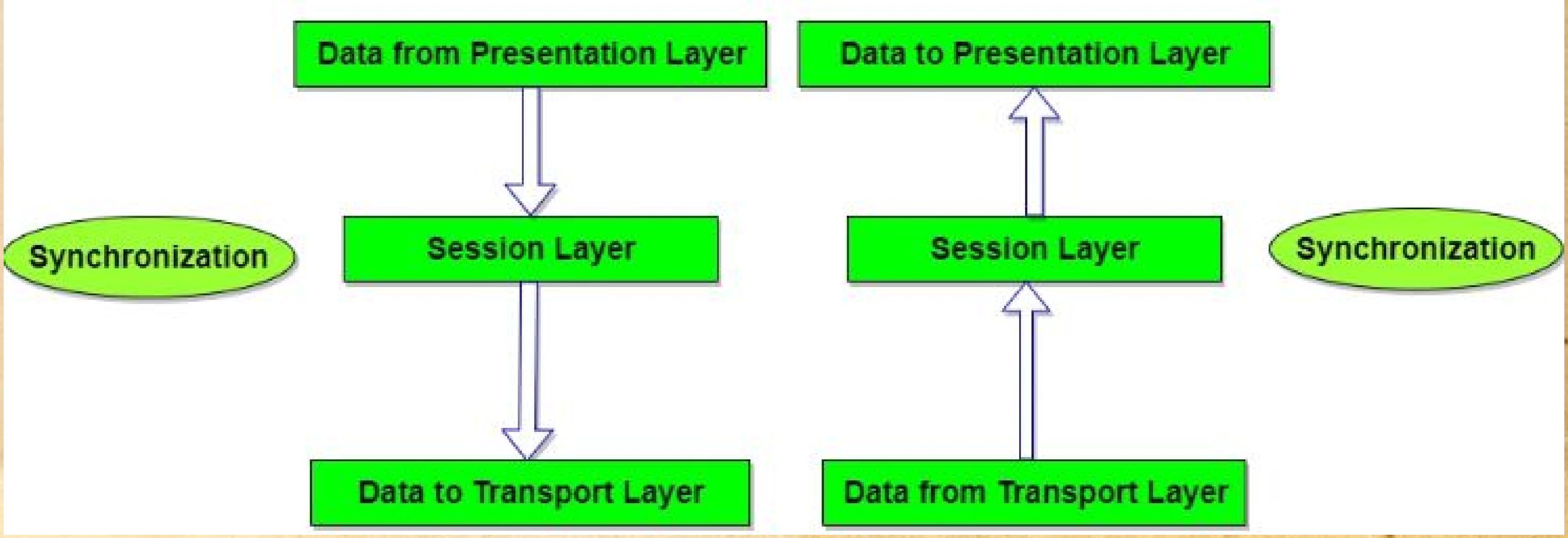
- **Translation:** The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into receiver-dependent format.

- **Encryption:** To carry any sensitive data, the presentation layer encrypts the data at the sender's end and decrypts at the receiver's end.
- **Compression:** Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.
- Example of protocol that run at the presentation layer include SSL.



5. Session Layer:

- Layer 5 of the Open Systems Interconnection (OSI) reference model, which enables sessions between computers on a network to be established and terminated.
- Its main aim is to establish, maintain and synchronize the interaction between communicating systems.
- Examples of protocols that run at the session layer include Password Authentication Protocol(PAP).


Data from Presentation Layer
Data to Presentation Layer
Synchronization
Session Layer
Session Layer
Synchronization
Data to Transport Layer
Data from Transport Layer

Functions:

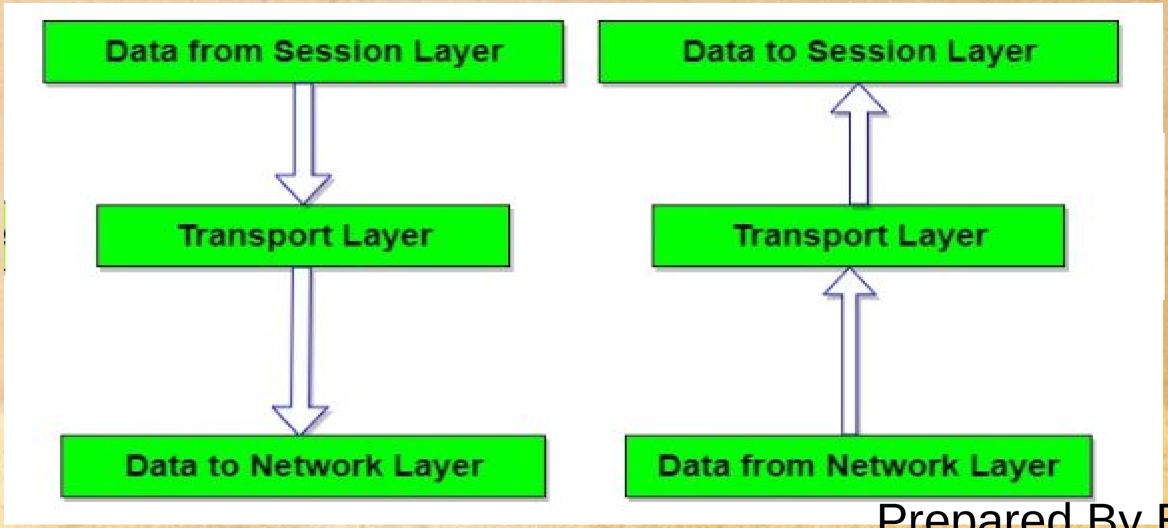
- **Dialog control:** It allows the communication between two processes to take place in either half- duplex (one way at a time) or full-duplex (two ways at a time) mode.
- **Synchronization:** The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

4. Transport Layer:

- Layer 4 of the Open Systems Interconnection (OSI) reference model.
- The basic function of the Transport layer is to accept data from the layer above, split it up into smaller units, pass these data units to the Network layer, and ensure that all the pieces arrive correctly at the other end.

Functions of Transport Layer

- **Port Addressing**: This layer gets the message to the correct process on the computer unlike Network Layer, which gets each packet to the correct computer.



- **Segmentation and Reassembling**: A message is divided into segments; each segment is assigned unique sequence number. Message is reassembled correctly upon arrival at the destination with the help of sequence number.
- **Connection Control**: It includes 2 types:
  - Connectionless Transport Layer : Each segment is considered as an independent packet and delivered to the transport layer at the destination machine.
  - Connection Oriented Transport Layer(3way handshake) : Before delivering packets, connection is made with transport layer at the destination machine.
- **Flow Control**: In this layer, flow control is performed end to end to ensure less packet loss.
- **Error Control**: Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error.
- Examples of protocols that run at the transport layer include Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

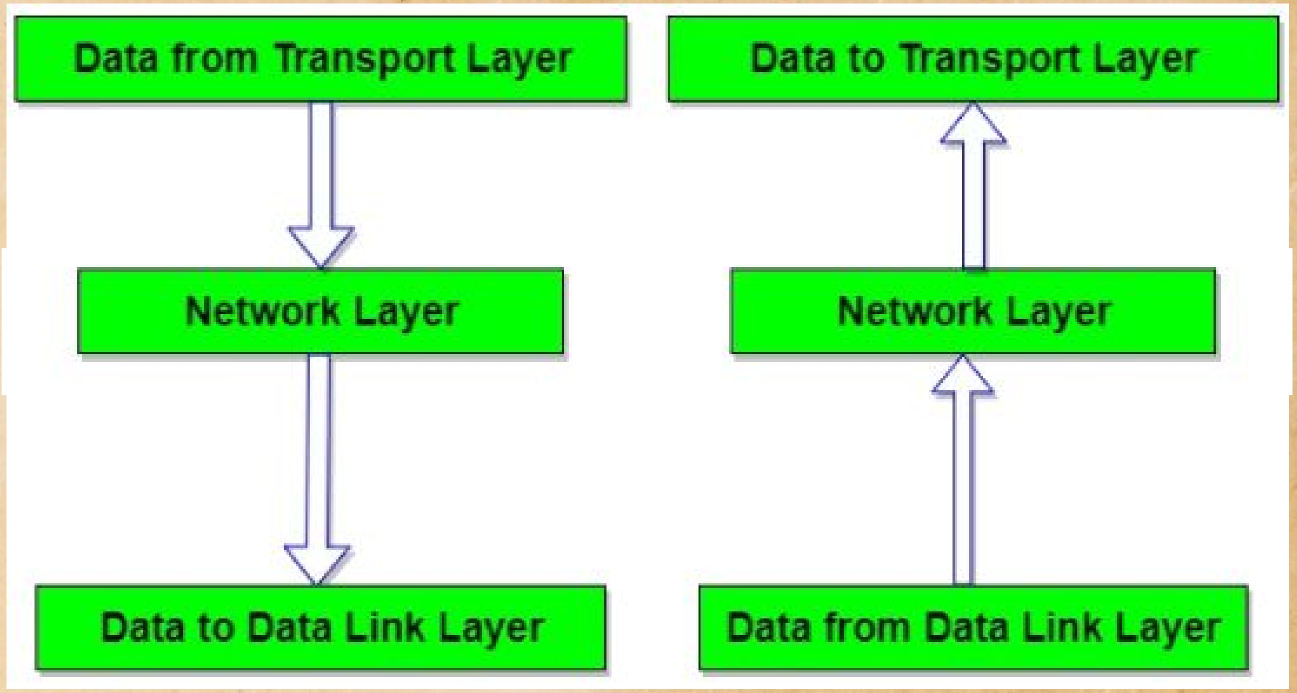
3. Network Layer:

- Layer 3 of the Open Systems Interconnection (OSI) reference model for networking(linking computers).
- The main aim of this layer is to deliver packets from source to destination across multiple links (networks).

Functions of Network Layer

- **Logical addressing:** The network layer adds a header to the packet coming from the upper layer that includes the logical addresses(IP addresses) of the sender and receiver.
- **Routing:** When independent networks or links are connected to create inter-networks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination.

- Examples of protocols that run at the network layer include IPv4, Open Shortest Path First etc.



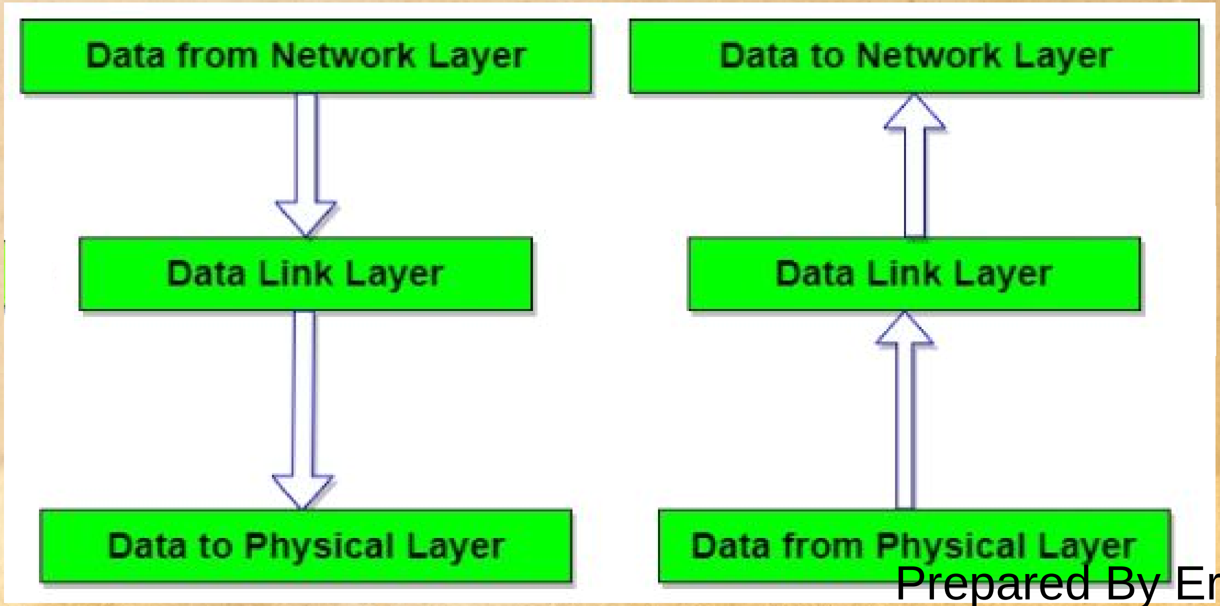
2. Data Link Layer:

- It forms frames from the packets that are received from network layer and gives it to physical layer.

Functions of Data Link Layer

- **Framing:** The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- **Physical addressing:** The data link layer adds a header(MAC address) to the packet which becomes frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.
- **Flow control:** If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

- **Error control:** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. Error control is normally achieved through a trailer added to the end of the frame.
- **Access control:** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.
- Examples of protocols that run at the data link layer include Point-to-Point Protocol (PPP), High-Level Data Link Control(HDLC).



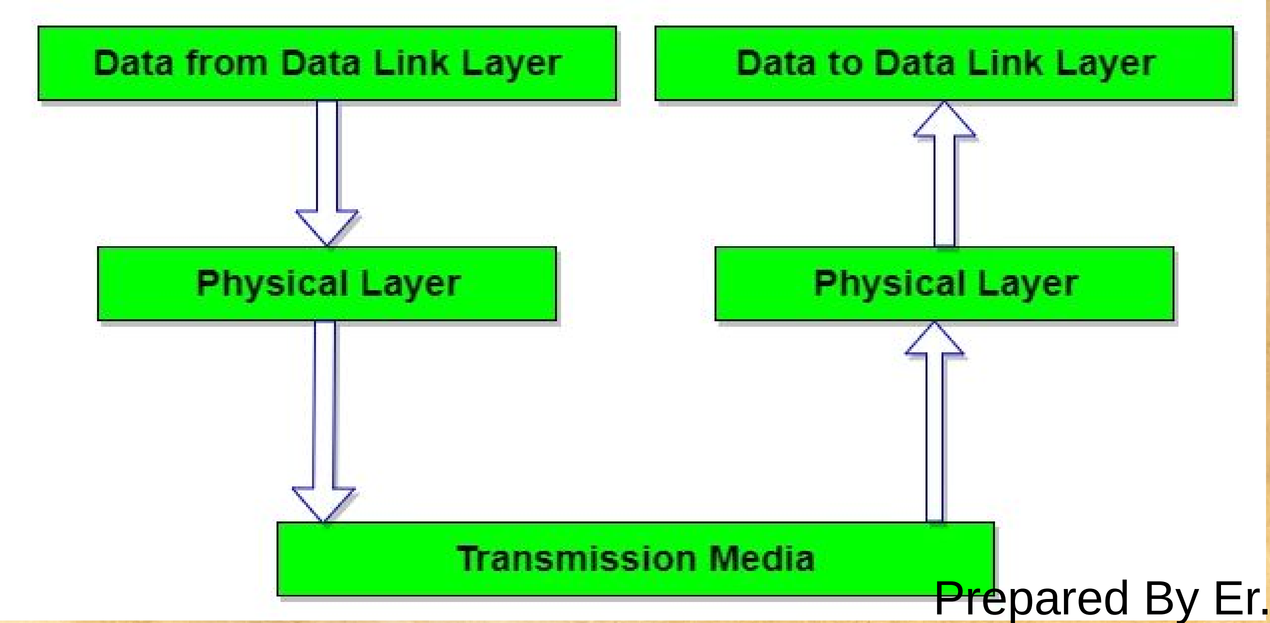
1. Physical Layer:

- Physical layer is the bottom layer(Layer 1) of the OSI reference model.
- It is responsible for sending bits from one computer to another.
- It deals with the setup of physical connection to the network and with transmission and reception of signals.

Functions of Physical Layer

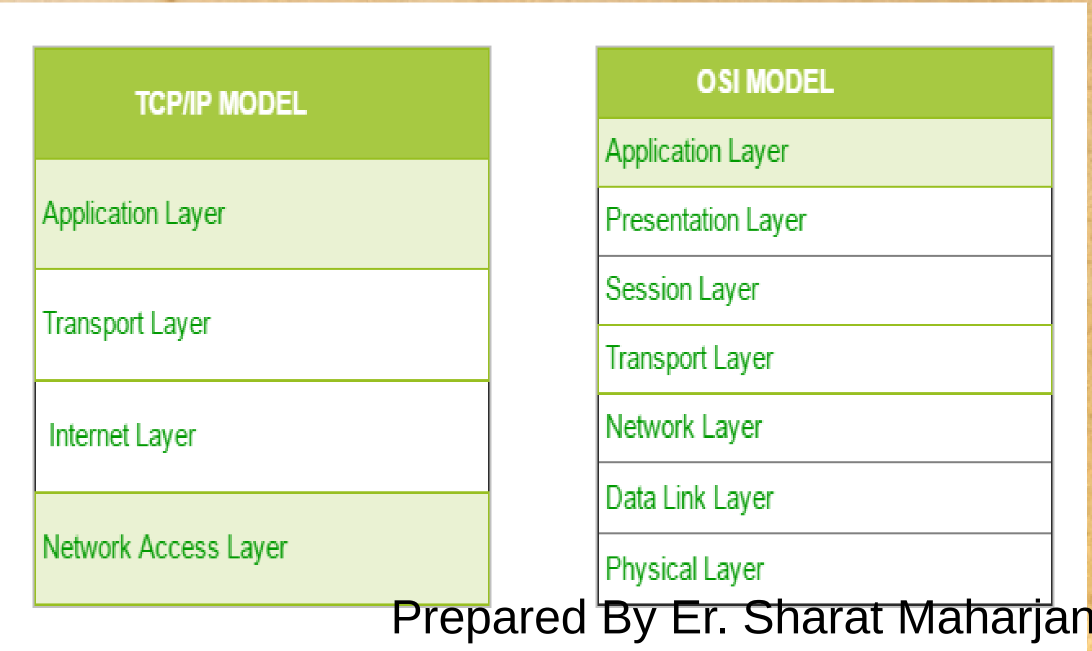
- **Representation of Bits(Encoding)**: Data in this layer consists of stream of bits. The bits must be encoded into signals for transmission. It defines the type of encoding i.e. how 0's and 1's are changed to signal.
- **Data Rate**: This layer defines the rate of transmission which is the number of bits per second.
- **Synchronization**: It deals with the synchronization of the transmitter and receiver. The sender and receiver are synchronized at bit level.
-

- **Line Configuration**: This layer connects devices with the medium: Point to Point configuration and Multipoint configuration.
- **Physical Topology**: The physical topology determines how devices are connected to create a network. Devices can be using a mesh topology, a star topology, a ring topology or a bus topology..
- **Transmission Modes**: Physical Layer defines the direction of transmission between two devices: Simplex, Half Duplex, Full Duplex.
- Example of protocol that run at the physical layer include token ring.



1.7 The TCP/IP Protocol Suite

- TCP/IP stands for Transmission Control Protocol/Internet Protocol.
- It was developed in 1970s.
- It contains four layers, unlike seven layers in the OSI model. The layers are:
  - Application Layer
  - Transport Layer
  - Internet(Network) Layer
  - Network Access Layer



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

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

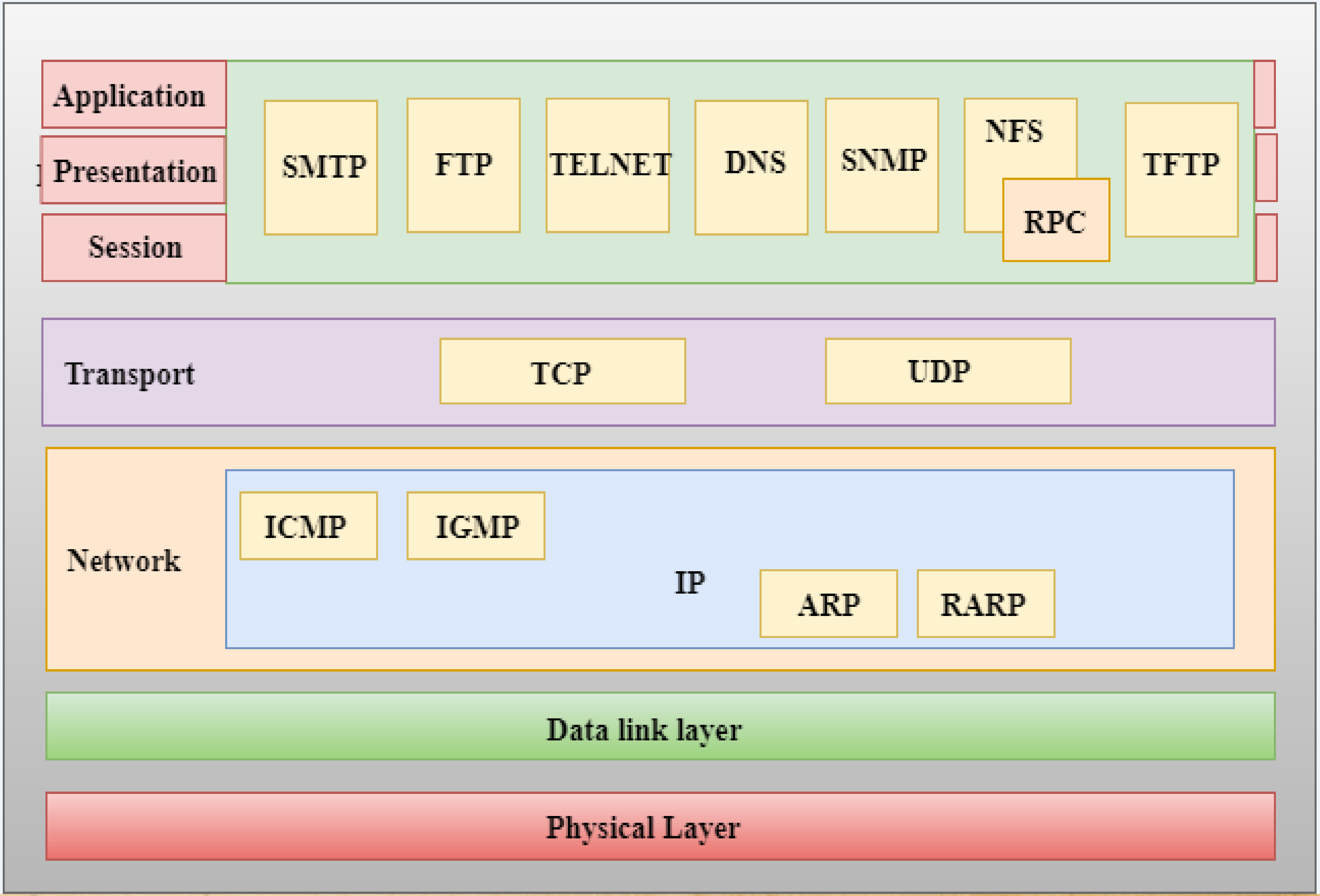


Figure: TCP/IP PROTOCOL SUITE (TCP/IP and OSI model)

Prepared By Er. Sharat Maharjan

<u>4. Application Layer:</u>

- The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model.
- This layer uses a number of protocols, the main among which are as follows −

  a. Hyper Text Transfer Protocol, (HTTP): It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer).

  b. File Transfer Protocol, (FTP): It is a standard internet protocol used for transmitting the files from one computer to another computer.

  c. Simple Mail Transfer Protocol, (SMTP): It is used to send the data to another e-mail address.

3. Transport Layer:

- Three Protocols of transport layer can be explained as:

a. User Datagram Protocol: The User Datagram Protocol (UDP) is the simpler transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

b. Transmission Control Protocol: The TCP provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented i.e; a connection must be established between both ends of a transmission before either can transmit data. At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. At the receiving end, TCP collects each segment as it comes in and reorders the transmission based on sequence numbers.

c. Stream Control Transmission Protocol: It is a transport layer protocol that combines the best features of UDP and TCP.

2. Network Layer:

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

- **Internet Protocol (IP):** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet to identify the device. IP has 2 versions: IPv4 and IPv6.
- **Address Resolution Protocol (ARP):** It is a network layer protocol which is used to find the physical address from the IP address.
- **Internet Control Message Protocol (ICMP):** is mainly used to determine whether or not data is reaching its intended destination in a timely manner.

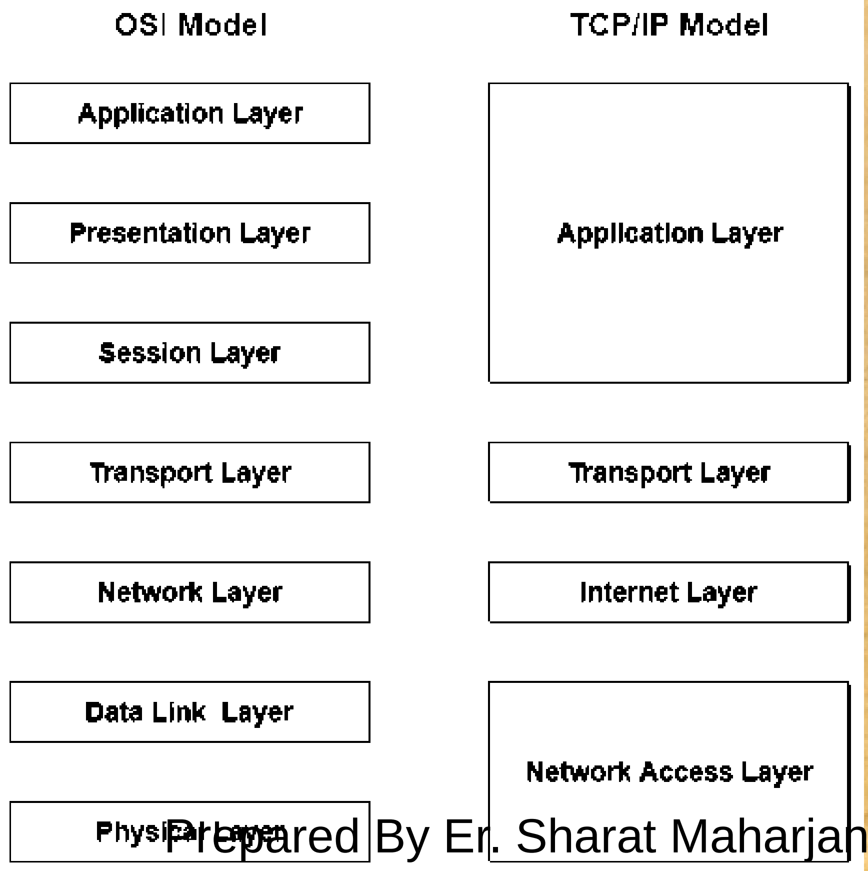
1. Network Access Layer:

- A network layer is the lowest layer of the TCP/IP model.
- A network 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 the data between two devices.
- The functions carried out by this layer are encapsulating the IP datagram into frames and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, X.25, frame relay.

1.8 Comparison between OSI and TCP/IP Reference model

Following are some similarities between OSI Reference Model and TCP/IP Reference Model:

- Both have layered architecture.
- Layers provide similar functionalities.
- Both are protocol stack.



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

Key Differences Between TCP/IP and OSI Model

- TCP/IP is Transmission Control Protocol/ Internet Protocol while OSI is Open System Interconnection.
- TCP/IP is a client server model used for transmission of data over the internet while OSI is a theoretical model which is used for computing system.
- TCP/IP is a four-layered model, whereas, OSI has seven layers.
- TCP/IP was developed by Department of Defense (DoD) while OSI was developed by ISO (International Standard Organization).
- TCP/IP is mostly used while OSI was never used.
- TCP/IP is a standard protocol used for every network including the Internet, whereas, OSI is not a protocol but a reference model used for understanding and designing the system architecture.
- TCP/IP does not have a separate Presentation layer or Session layer whereas OSI does have separate Presentation and Session layer.

1.9 Critiques of OSI and TCP/IP Reference model

- **Bad timing**
  - OSI model was finished and completed after huge and significant amount of research time.
  - TCP/IP model was already receiving huge amounts of investments from companies and manufacturers did not feel like investing in OSI model.
- **Bad technology**
  - OSI model and its protocols are flawed that means both of them have fundamental weakness in performance or design, etc.
  - Documentation of OSI is also highly complex due to which it gets very difficult to implement.
-

- **Bad implementations**
  - Initial implementations of OSI were very slow & huge.
  - Implementations of TCP/IP were more reliable than OSI due to which people started using TCP/IP very quickly which led to large community of users.
- **Bad politics**
  - OSI model was not associated with UNIX.
  - TCP/IP was largely and closely associated with Unix.

THANK YOU!!!