

Introduction to Computer Network

Prepared by: Hiranya Prasad Bastakoti

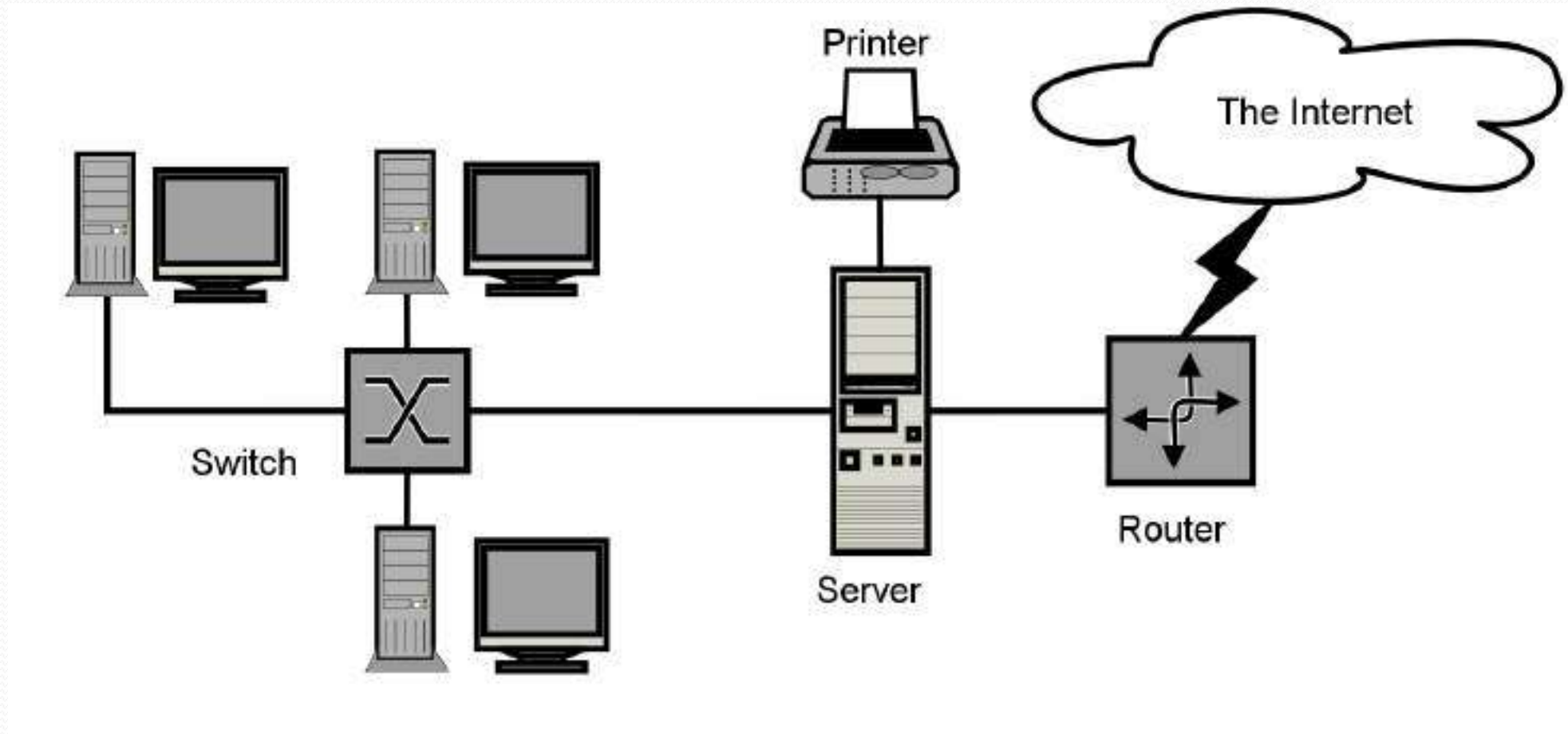
Contents

- Definitions, Uses and Benefits of Network
- Overview of Network Topologies
- Overview of Network Types(LAN,MAN...
- Networking Types(Client/Server,P2P)
- Overview of Protocols and Standards
- OSI Reference Model
- TCP/IP Model and Comparision with OSI
- Connection and Connectionless –Oriented Network Services
- Internet,ISPs,Backbone Network Overview

Introduction

- A network is a group of computers and other devices, such as printers and modems, connected to each other. This enables the computers to effectively share data and resources.
- A **computer network**, often simply referred to as a network, is a collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information
- A collection of computing devices connected in order to communicate and share resources
- Connections between computing devices can be physical using wires or cables or wireless using radio waves or infrared signals
- By definition, a computer network is a group of computers that are linked together through a communication channel.

Basic Structure of Network



Description of Network Structure

- All the computer devices are called **hosts** or **end systems**. Hosts sending requests are called **clients** while hosts receiving requests are called **servers**.
- End systems are connected together by a network of **communication links** and **packet switches**.
- Communication links are made up of different types of physical media, including coaxial cable, copper wire, optical fiber, and radio spectrum.
- Different links can transmit data at different rates, with the **transmission rate** of a link measured in bits/second.
- When one end system has data to send to another end system, the sending end system segments the data and adds header bytes to each segment.
- The resulting packages of information, known as **packets**, are then sent through the network to the destination end system, where they are reassembled into the original data.
- A packet switch takes a packet arriving on one of its incoming communication links and forwards that packet on one of its outgoing communication links. Common packet switches are **routers** and **link-layer switches**.

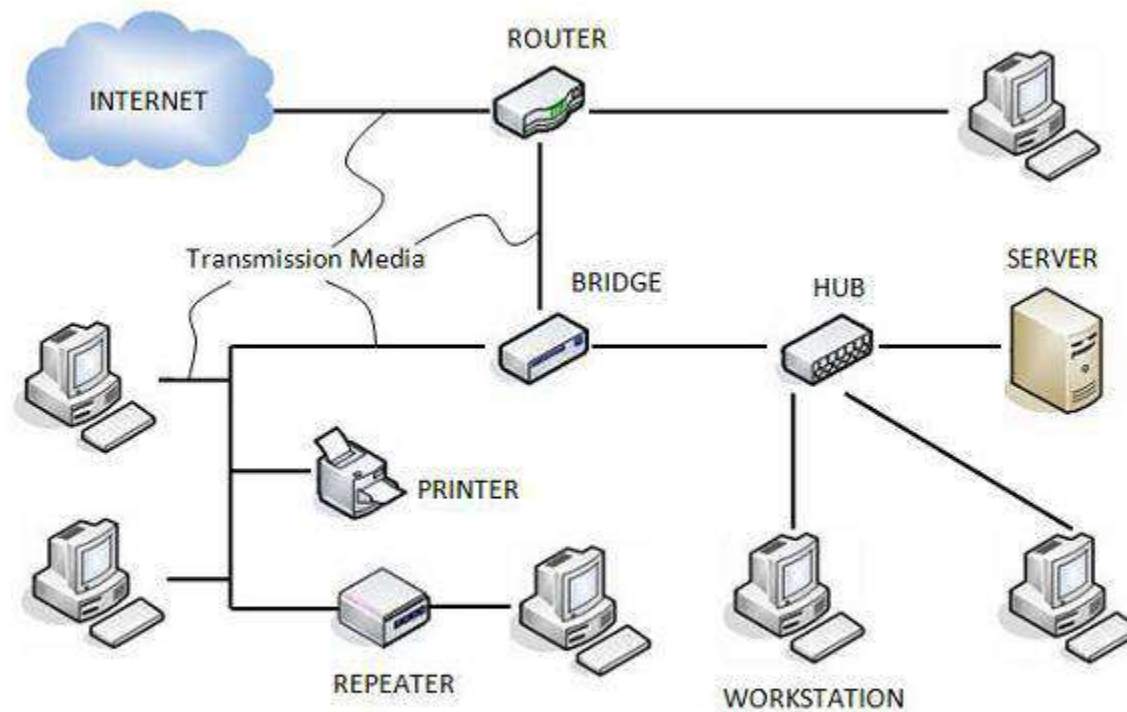
Purpose of Network

A network can be defined as two or more computers connected together in such a way that they can share resources.

The purpose of a network is to share resources.

A resource may be:

- A file
- A folder
- A printer
- A disk drive
- Or just about anything else that exists on a computer.



COMPUTER NETWORK COMPONENTS

Network Components

Hardware Components

Servers: Servers are high-configuration computers that manage the resources of the network. The network operating system is typically installed in the server and so they give user accesses to the network resources. Servers can be of various kinds: file servers, database servers, print servers etc.


Clients: Clients are computers that request and receive service from the servers to access and use the network resources.

Peers: Peers are computers that provide as well as receive services from other peers in a workgroup network.

Transmission Media: Transmission media are the channels through which data is transferred from one device to another in a network. Transmission media may be guided media like coaxial cable, fibre optic cables etc; or maybe unguided media like microwaves, infra-red waves etc.

Connecting Devices: Connecting devices act as middleware between networks or computers, by binding the network media together. Some of the common connecting devices are:

- a. Routers
- b. Bridges
- c. Hubs
- d. Repeaters
- e. Gateways
- f. Switches



Networking Operating System: Network Operating Systems is typically installed in the server and facilitate workstations in a network to share files, database, applications, printers etc.

Protocol Suite: A protocol is a rule or guideline followed by each computer for data communication. Protocol suite is a set of related protocols that are laid down for computer networks. The two popular protocol suites are:

- a. OSI Model (Open System Interconnections)
- b. TCP / IP Model

Basic Elements of Network

- Basic elements of a computer network include hardware, software, and protocols.
- The interrelationship of these basic elements constitutes the infrastructure of the network.
- A network infrastructure is the topology in which the nodes of a local area network (LAN) or a wide area network (WAN) are connected to each other. These connections involve equipment like routers, switches, bridges and hubs using cables (copper, fiber, and so on) or wireless technologies (Wi-Fi).

Network Services

- A computer network provides several network services.
- network services examples: distributed database, Web , file transfer, remote login,email,news, talk, remote processing, resource sharing (file servers, printers, modems), network time, name service.



A computer network is made of **two distinct** subsets of components

- **distributed applications** are programs running on interconnected computers; a web server, a remote login server, an email exchanger are examples. This is the visible part of what people call “the Internet”.
- **the network infrastructure** is the collection of systems which are required for the interconnection of computers running the distributed applications.

Advantages of Networking

- **Connectivity and Communication**
- **Data Sharing**
- **Hardware Sharing**
- **Internet Access**
- **Internet Access Sharing**
- **Data Security and Management**
- **Performance Enhancement and Balancing**
- **Entertainment**

Applications

❏ Resource Sharing

- ❏ Hardware (computing resources, disks, printers)
- ❏ Software (application software)

❏ Information Sharing

- ❏ Easy accessibility from anywhere (files, databases)
- ❏ Search Capability (WWW)

❏ Communication

- ❏ Email
- ❏ Message broadcast

❏ Remote computing

❏ Distributed processing (GRID Computing)

Disadvantages of Networking

- **Network Hardware, Software and Setup Costs**
- **Hardware and Software Management and Administration Costs**
- **Undesirable Sharing**
- **Illegal or Undesirable Behavior**
- **Data Security Concerns**

Network Topology

- Computer network topology is the way various components of a network (like nodes, links, peripherals, etc) are arranged.
- Network topologies define the layout, virtual shape or structure of network, not only physically but also logically. The way in which different systems and nodes are connected and communicate with each other is determined by topology of the network.
- *Physical Topology* is the physical layout of nodes, workstations and cables in the network.
- *Logical topology* is the way information flows between different components.

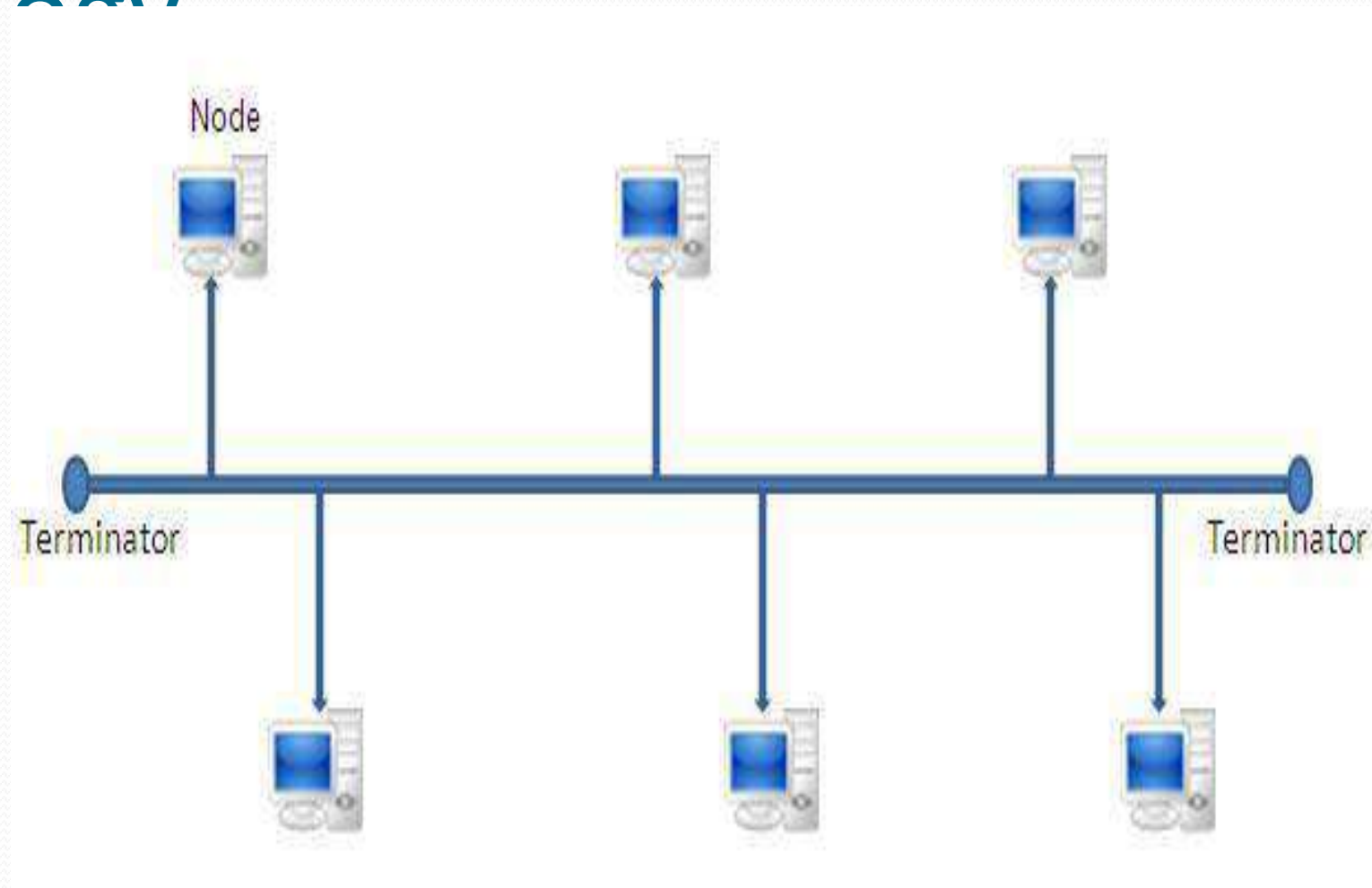
Types of Physical Topology

- Bus Topology
- Star Topology
- Ring Topology
- Mesh Topology
- Tree Topology
- Hybrid Topology

Bus Topology

- In the bus topology, the computers are connected through a common communication media.
- A special type of central wire is used as communication media. This central wire is called Bus.
- The computer are attached through the bus the ends of the bus are closed with the terminator .The terminators are used to absorb signals.

Bus topology



Advantages and Disadvantages

Advantages:

- 1) Easy to implement and extend
- 2) Well suited for temporary networks that must be set up in a hurry
- 3) Typically the least cheapest topology to implement
- 4) Failure of one station does not affect others

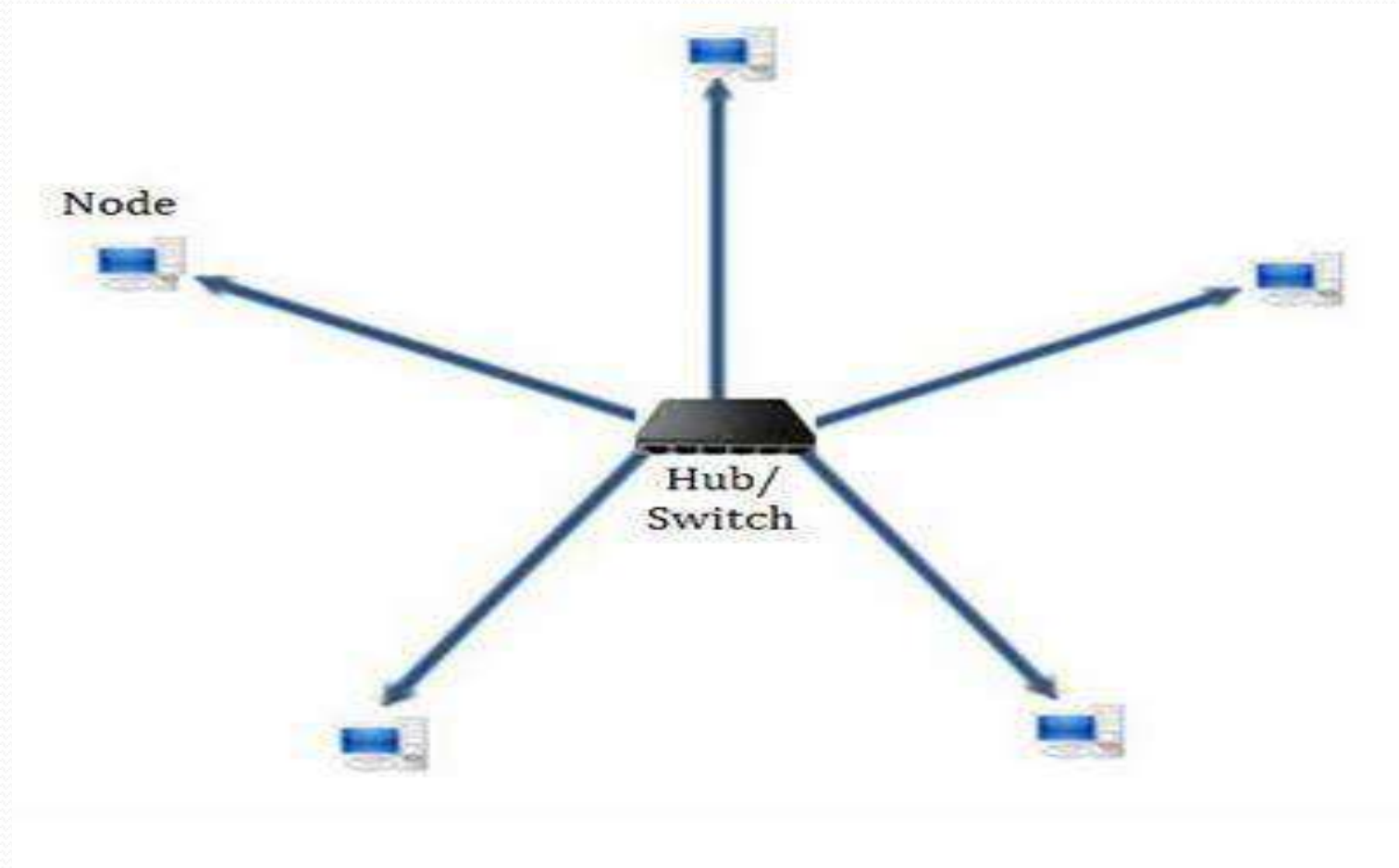
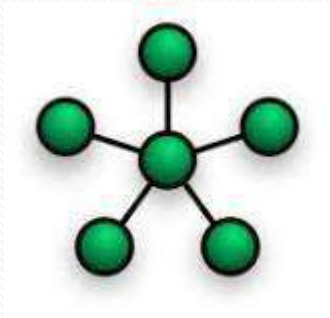
Disadvantages:

- 1) Difficult to administer/troubleshoot
- 2) Limited cable length and number of stations
- 3) A cable break can disable the entire network; no redundancy
- 4) Maintenance costs may be higher in the long run
- 5) Performance degrades as additional computers are added

Star Topology

- The star topology uses a separate cable for each work station as shown in fig.
- The cable connects the work station to a central device typically a Switch/HUB.
- The configuration provides a more reliable network that is easily expended.
- With star there is no central point of failure in the cable .if there is a problem with the cable only the station connected to that cable is a effected .to add more work stations simply connect another Switch/ HUB.
- Each networked device in star topology can access the media independently
- Have become the dominant topology type in contemporary LANs

Star Topology



Advantages and Disadvantages

Advantages:

- 1) Compared to Bus topology it gives far much better performance
- 2) Easy to connect new nodes or devices
- 3) Centralized management. It helps in monitoring the network
- 4) Failure of one node or link doesn't affect the rest of network

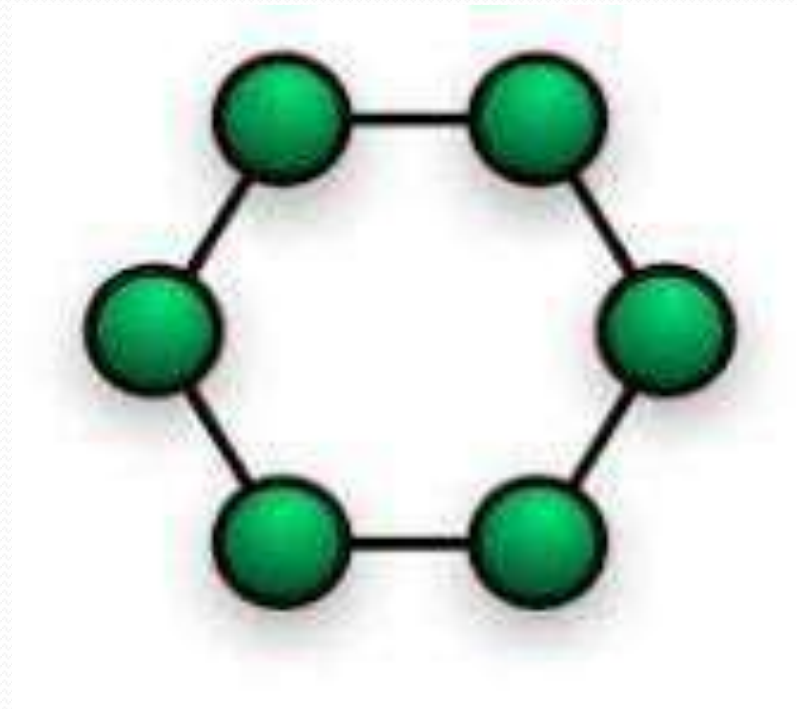
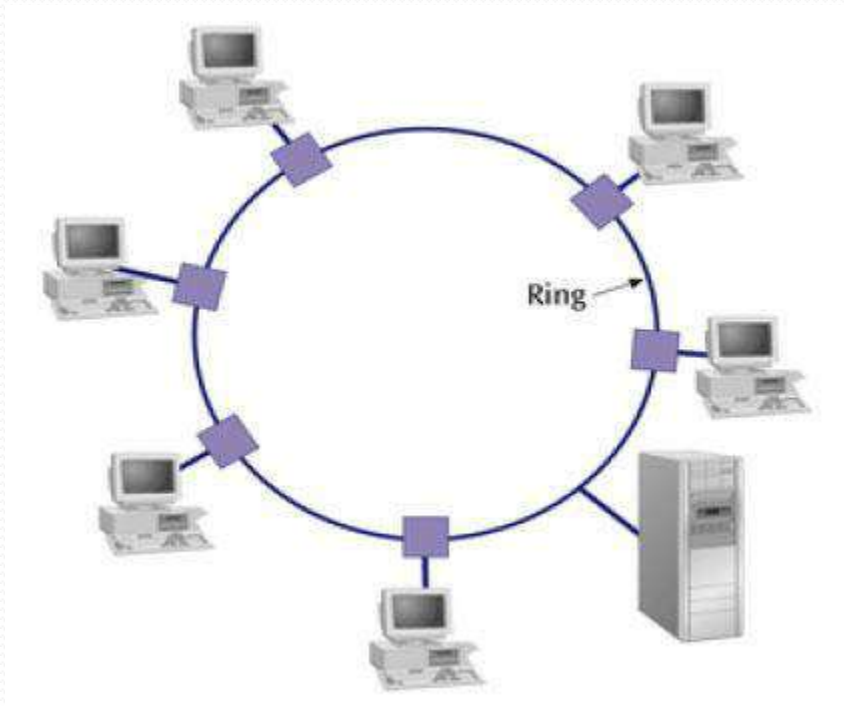
Disadvantages:

- 1) If central device fails whole network goes down
- 2) The use of hub, a router or a switch as central device increases the overall cost of the network
- 3) Performance and as well number of nodes which can be added in such topology is depended on capacity of central device

Ring Topology

- Every computer is connected to the next computer in the ring and each transmits what it receives from the previous computer. The messages flow around the ring in one direction.
- Some ring network do ring token passing. A short message called token (memory area) is passed around a ring until a computer wishes to send information to other computers.
- That computer modifies token, adds an electronic address and data and send it around the ring. Each computer in sequence receives the token and next computer until either the electronic address matches the address of a computer Or the token return to its origin .The receiving computer returns a message to the sender indicating that message has been received.

Ring Topology



Advantages and Disadvantages

Advantages

- 1) This type of network topology is very organized
- 2) Performance is better than that of Bus topology
- 3) No need for network server to control the connectivity between workstations
- 4) Additional components do not affect the performance of network
- 5) Each computer has equal access to resources.

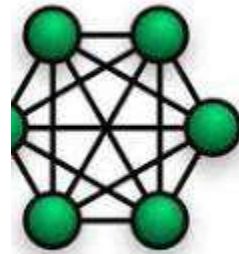
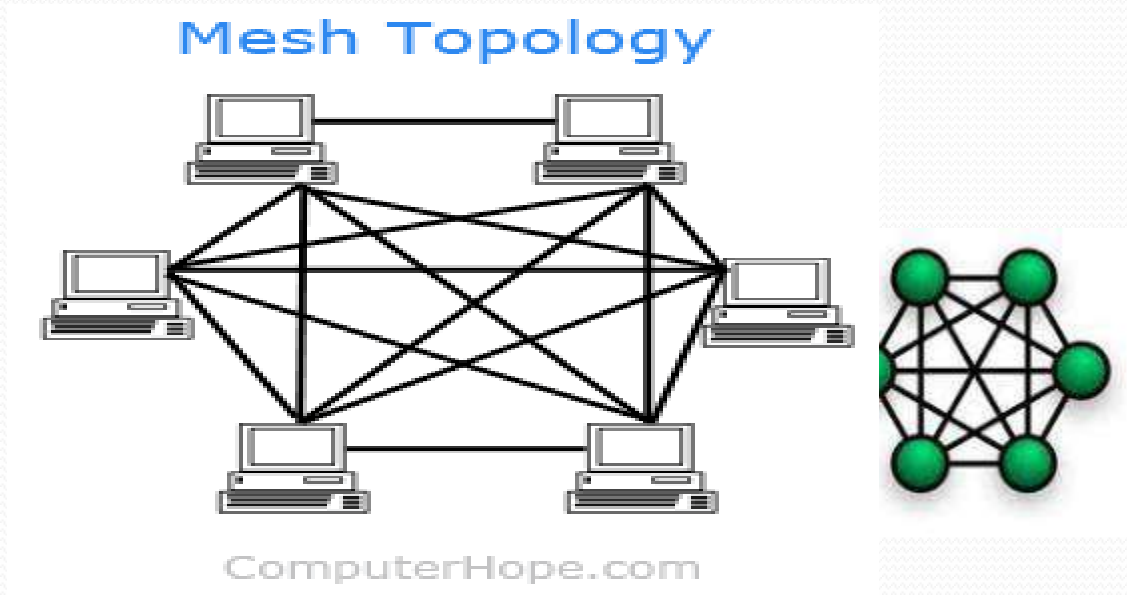
Disadvantages:

- 1) Each packet of data must pass through all the computers between source and destination, slower than star topology
- 2) If one workstation or port goes down, the entire network gets affected
- 3) Network is highly dependent on the wire which connects different components

Mesh Topology

- A mesh network or mesh topology uses separate cable to connect each device to every other device on the network, providing a straight communication path. For sending messages, check the cable connected into two devices. A message is send directly from sender to receiver because each one has individual and separate connection.
- In a *full mesh topology*, every computer in the network has a connection to each of the other computers in that network.
- The number of connections in this network can be calculated using the following formula (n is the number of computers in the network): $n(n-1)/2$

Mesh Topology



Advantages:

- Manages high amounts of traffic, because multiple devices can transmit data simultaneously.
- A failure of one device does not cause a break in the network or transmission of data.
- Adding additional devices does not disrupt data transmission between other devices.

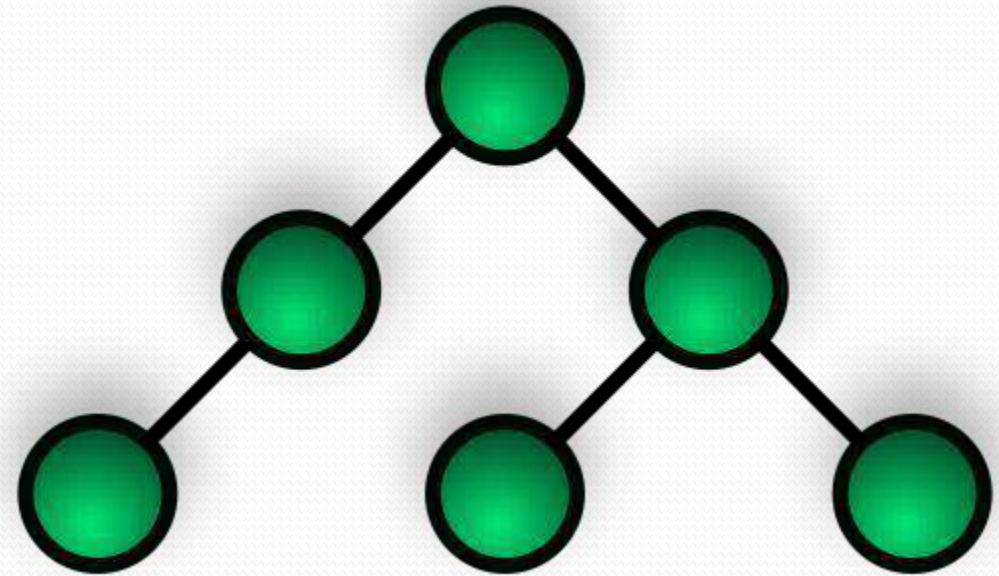
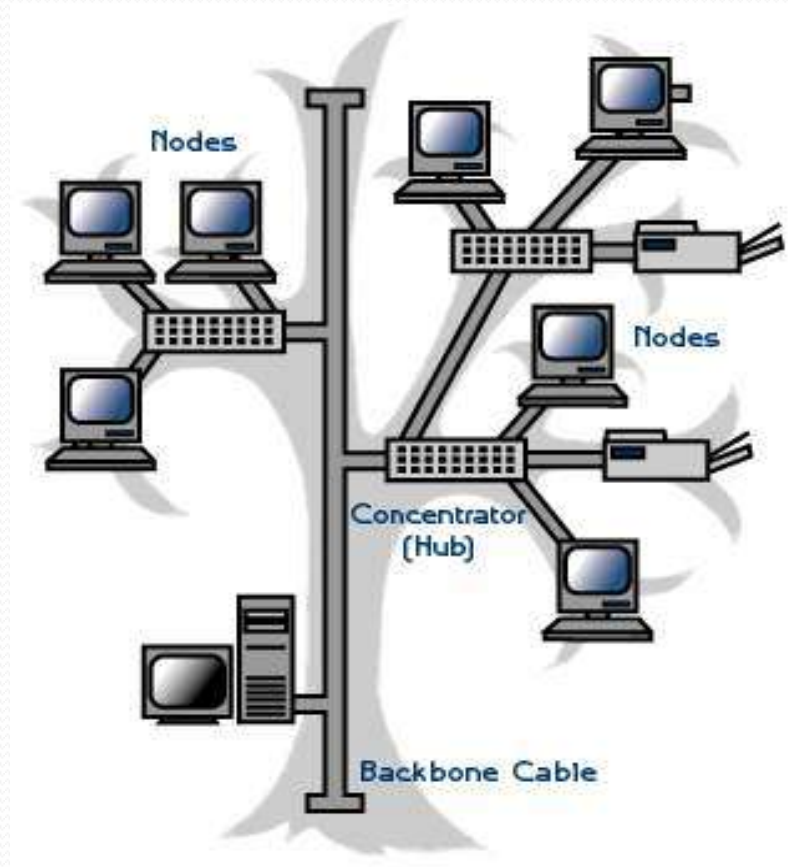
Disadvantages:

- The cost to implement is higher than other network topologies, making it a less desirable option.
- Building and maintaining the topology is difficult and time consuming.
- The chance of redundant connections is high, which adds to the high costs and potential for reduced efficiency.

Tree Topology

- The type of network topology in which a central 'root' node (the top level of the hierarchy) is connected to one or more other nodes that are one level lower in the hierarchy.
- A tree topology combines characteristics of linear bus and star topologies.
- It consists of groups of star-configured workstations connected to a linear bus backbone cable
- Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs.

Tree Topology



Advantages and Disadvantages

Advantages:

- **It is scalable:**Secondary nodes allow more devices to be connected to a central node.
- Point to point connection of devices.
- Having different levels of the network makes it more manageable hence easier fault identification and isolation.

Disadvantages:

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

Overview of Network Types

Depending upon the geographical area covered by a network, it is classified as:

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

LAN

- *A LAN is a network that is used for communicating among computer devices, usually within an office building or home.*
- LAN's enable the sharing of resources such as files or hardware devices that may be needed by multiple users
- Is limited in size, typically spanning a few hundred meters, and no more than a mile
- Is fast, with speeds from 10 Mbps to 10 Gbps
- Requires little wiring, typically a single cable connecting to each device
- Has lower cost compared to MAN's or WAN's.
- **A Local Area Network (LAN) is a computer network covering a small geographic area, like a home, office, or group of buildings**

- LAN's can be either wired or wireless. Twisted pair, coax or fibre optic cable can be used in wired LAN's.
- Every LAN uses a protocol – a set of rules that governs how packets are configured and transmitted.
- Nodes in a LAN are linked together with a certain
- topology. These topologies include:
 - Bus
 - Ring
 - Star
- LANs are capable of very high transmission rates (100s Mb/s to Gb/s).

Advantages

- The basic LAN implementation does not cost too much.
- It is easy to control and manage the entire LAN as it is available in one small region.
- The LAN configuration is very easy due to availability of required protocols in the Operating System (OS) itself.
- The systems or devices connected on LAN communicates at very high speed depending upon LAN type and ethernet cables supported. The common speeds supported are 10 Mbps, 100 Mbps and 1000 Mbps. Gigabit ethernet versions are evolving very fast. Cheaper versions will be available once the technology matures and mass production has been carried out.
- With the help of file servers connected on the LAN, sharing of files and folders among peers will become very easy and efficient
- It is easy to setup security protocols to protect the LAN users from intruders or hackers.
- It is easy to share common resources such as printers and internet line among multiple LAN users.
- LAN users do not require their own harddisk and CD-ROM drives. They can save their work centrally on network file server.
- Application softwares such as MS Office, Anti-Virus, Adobe reader are stored at one system and are shared for all the LAN users.

Disadvantages

- LAN covers small geographical area.
- Security issues are big concern as it is easy to have access to programs and data of peers. Special security measures are needed to stop unauthorized acces
- It is difficult to setup and maintain LAN and requires skilled technicians and network administrators.
- In the server based LAN architecture, if server develops some fault, all the users are affected.
- Appearance of virus in one system can spread very fast to all the LAN users very easily.

Metropolitan Area Network

- A **metropolitan area network (MAN)** is a large computer network that usually spans a city or a large campus.
- A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities.
- A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations.
- A MAN often acts as a high speed network to allow sharing of regional resources.
- A MAN typically covers an area of between 5 and 50 km diameter.
- Examples of MAN: Telephone company network that provides a high speed DSL to customers and cable TV network.
- **A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN).**

Advantages

- It utilizes drawbacks of both LAN and WAN to provide larger and controllable computer network.
- MAN requires fewer resources compare to WAN. This saves the implementation cost
- It helps people interface fast LANs together. This is due to easy implementation of links
- It provides higher security compare to WAN.
- It helps in cost effective sharing of common resources such as printers etc.
- Like LAN and WAN, it also offers centralized management of data and files.

Disadvantages

- It is difficult to manage the network once it becomes large.
- it is difficult to make the system secure from hackers and industrial surveillance.
- Network installation requires skilled technicians and network administrators. This increases overall installation and management costs.
- It requires more cables for connection from one place to the other compare to LAN

Wide Area Network

- WAN covers a large geographic area such as country, continent or even whole of the world.
- A WAN is two or more LANs connected together. The LANs can be many miles apart.
- To cover great distances, WANs may transmit data over leased high-speed phone lines or wireless links such as satellites.
- Multiple LANs can be connected together using devices such as bridges, routers, or gateways, which enable them to share data.
- The world's most popular WAN is the Internet.
- **Wide Area Network (WAN)** is a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries).
- WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations

Advantages

- WAN covers larger geographical area. Hence business offices situated at longer distances can easily communicate.
- Like LAN, it allows sharing of resources and application softwares among distributed workstations or users.
- The software files are shared among all the users. Hence all will have access to latest files. This avoids use of previous versions by them.
- Organizations can form their global integrated network through WAN. Moreover it supports global markets and global businesses.
- The emergence of IoT (Internet of Things) and advanced wireless technologies such as LAN or LAN-Advanced have made it easy for the growth of WAN based devices.

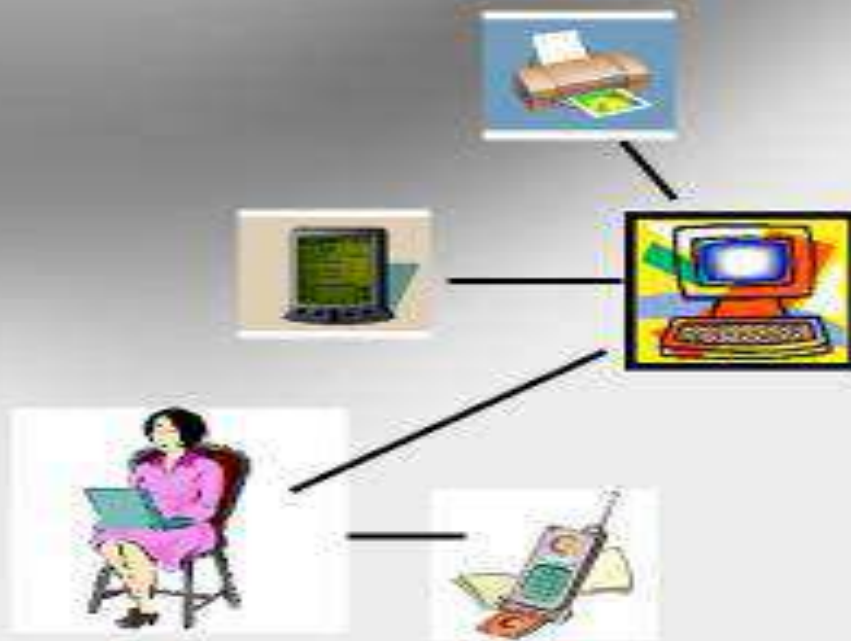
Disadvantages

- Initial investment costs are higher.
- It is difficult to maintain the network. It requires skilled technicians and network administrators.
- There are more errors and issues due to wide coverage and use of different technologies. Often it requires more time to resolve issues due to involvement of multiple wired and wireless technologies.
- It has lower security compare to LAN and MAN due to wider coverage and use of more technologies.
- Security is big concern and requires use of firewall and security softwares/protocols at multiple points across the entire system. This will avoid chances of hacking by intruders.

Personal Area Network

- A **PAN** is a network that is used for communicating among computers and computer devices (including telephones) in close proximity of around a few meters within a room
- It can be used for communicating between the devices themselves, or for connecting to a larger network such as the internet.
- PAN's can be wired or wireless
- A **personal area network (PAN)** is a computer network used for communication among computer devices, including telephones and personal digital assistants, in proximity to an individual's body.
- The devices may or may not belong to the person in question. The reach of a PAN is typically a few meters.

Personal Area Network(PAN)



Campus Area Network

- A campus area network (CAN) is a network of multiple interconnected local area networks (LAN) in a limited geographical area..
- The networking equipments (switches, routers) and transmission media (optical fiber, Twisted pair cabling etc.) are almost entirely owned by the campus , an enterprise, university, government etc.
- A campus area network is larger than a local area network but smaller than a metropolitan area network (MAN) or wide area network (WAN).

- In most cases, CANs own shared network devices and data exchange media.

CAN benefits are as follows:

- Cost-effective
- Wireless, versus cable
- Multidepartmental network access
- Single shared data transfer rate (DTR)

Client Server, Multipoint, P2P Network

Network architecture refers to how computers are organized in a network and how tasks are allocated between these computers

- Two of the most widely used types of network architecture are

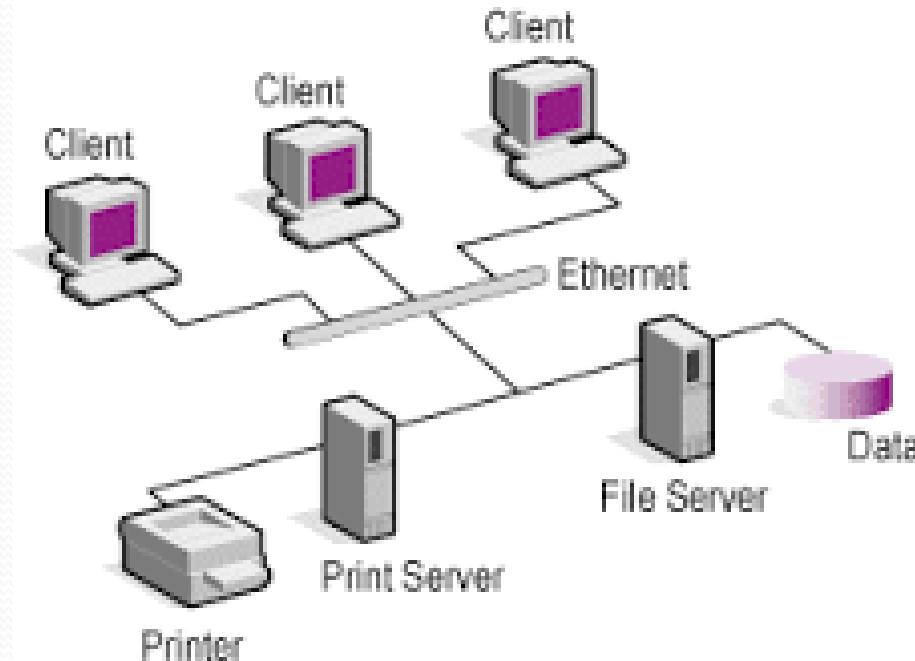
1. Peer-to-Peer(P2P)
2. Client/Server
3. Multipoint and Point to Point

Client Server

- Computing system in which one powerful workstation serves the requests of other systems
- Server :- Provides services to clients
- Client :- Accept services from server
- In client -server model, a small number of computers are designated as centralized *servers* and given the task of providing services to a larger number of user machines called *clients*
- *E.g. e.g., WWW client (browser)/ Web server; email client/mail server*
- **Server** computer is a core component of the network, providing a link to the resources necessary to perform any task.
- A server computer provides a link to the resources necessary to perform any task.
- The link it provides could be to a resource existing on the server itself or a resource on a client computer.
- **Client** computers normally request and receive information over the network *client*. *Client* computers also depends primarily on the central server for processing activities

Client/Server

- Client – name given to a workstation on this type of network
- Server – computer on the network that handles requests for data, emails, file transfers, and other network services from the clients
- Different types of server – File, Printer, Mail, & Web



Advantages

1. Centralization
2. Proper Management
3. Back-up and Recovery possible
4. Upgradation and Scalability in Client-server set-up
5. Accessibility
6. Security

Peer to Peer

- A peer-to-peer network is a network where the computers act as both workstations and servers.
- Great for small, simple, and inexpensive networks.
- In a strict peer-to-peer networking setup, every computer is an equal, a *peer* in the network.
- Each machine can have resources that are shared with any other machine.
- There is no assigned role for any particular device, and each of the devices usually runs similar software. Any device can and will send requests to any other.
- E.g. teleconferencing, groupware, file sharing

Types of Network— Peer-to-Peer

- Each workstation has the same status
- Each workstation has its own applications, programs and storage device
- The user is responsible for storing and backing up the data on the workstation
- If the user moves from one workstation to another their data is no longer easy to access



Advantages and Disadvantages

1. Easy to install and configure
2. All the resources and contents are shared by all the peers
3. P2P is more reliable as central dependency is eliminated
4. No need for full-time System Administrator (No central Admin)
5. Cost comparatively very less

Disadvantages:

- Network security has to be applied to each computer separately.
- Backup has to be performed on each computer separately.
- No centralized server is available to manage and control the access of data.
- Users have to use separate passwords on each computer in the network.

CLIENT SERVER		Peer to Peer
Basic	There is a specific server and specific clients connected to the server.	Clients and server are not distinguished; each node act as client and server.
Service	The client request for service and server respond with the service.	Each node can request for services and can also provide the services.
Focus	Sharing the information.	Connectivity.
Data	The data is stored in a centralized server.	Each peer has its own data.
Server	When several clients request for the services simultaneously, a server can get bottlenecked.	As the services are provided by several servers distributed in the peer-to-peer system, a server in not bottlenecked.
Expense	The client-server are expensive to implement.	Peer-to-peer are less expensive to implement.
Stability	Client-Server is more stable and scalable	Peer-toPeer suffers if the number of peers increases in the system

Point to Point Network

- The point-to-point is a kind of line configuration which describes the method to connect two communication devices in a link. The point-to-point connection is a unicast connection.
- There is a dedicated link between an individual pair of sender and receiver.
- The capacity of the entire channel is reserved only for the transmission of the packet between the sender and receiver.
- If the network is made up of point-to-point connections, then the packet will have to travel through many intermediate devices.
- The link between the multiple intermediate devices may be of different length. So, in point-to-point network finding the smallest distance to reach the receiver is most important.



Main frame

Link

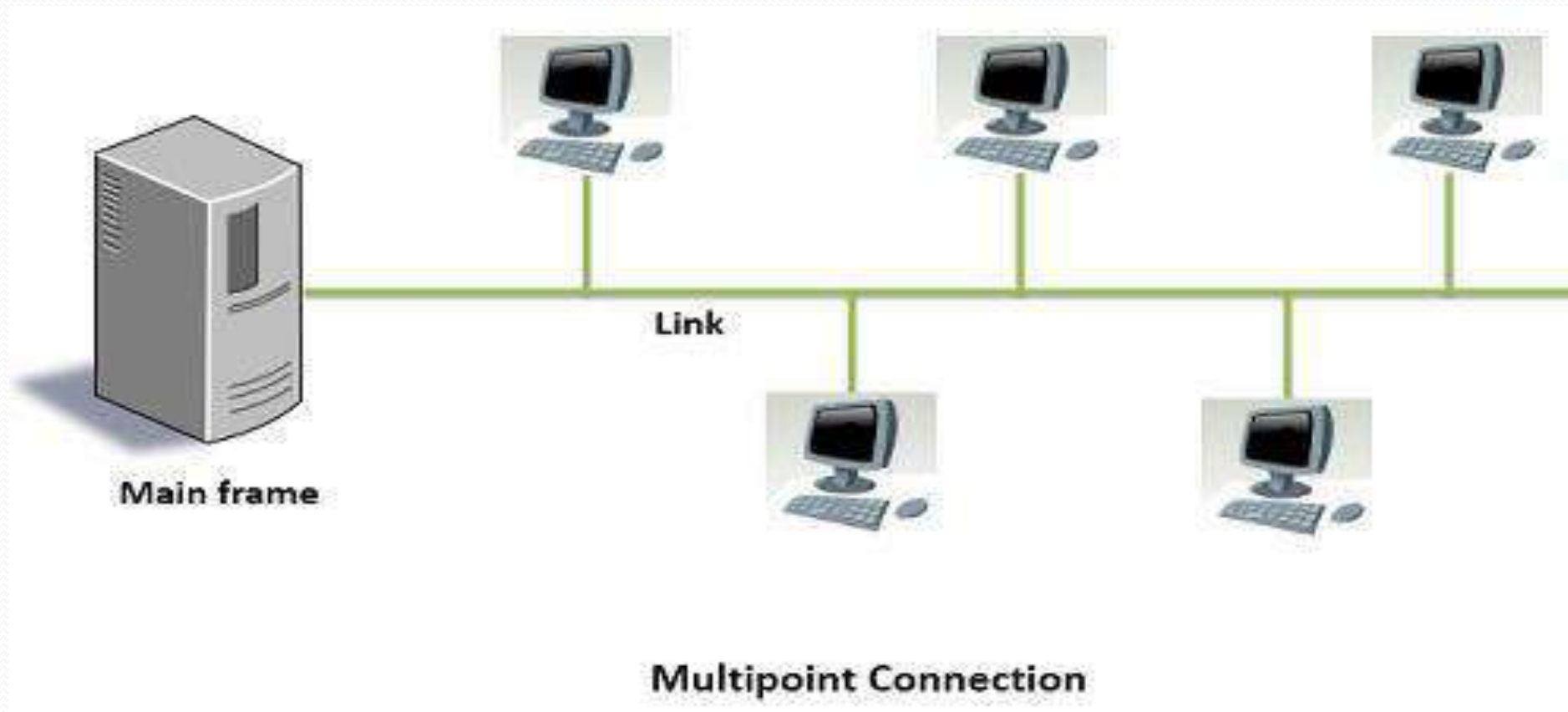


Workstation

Point-to-point Connection

Multipoint Network

- The multipoint connection is a connection established between more than two devices.
- The multipoint connection is also called multidrop line configuration. In multipoint connection, a single link is shared by multiple devices.
- So, it can be said that the channel capacity is shared temporarily by every device connecting to the link. If devices are using the link turn by turn, then it is said to be time shared line configuration.
- The multipoint networks are also called “Broadcast network.” In a broadcast network, the packet transmitted by the sender is received and processed by every device on the link.
- But, by the address field in the packet, the receiver determines whether the packet belongs to it or not, if not, it discards the packet. If packet belongs to the receiver then keeps the packet and respond to the sender accordingly.



BASIS FOR COMPARISON	POINT-TO-POINT	MULTIPOINT
Link	There is dedicated link between two devices.	The link is shared between more than two devices.
Channel Capacity	The channel's entire capacity is reserved for the two connected devices.	The channel's capacity is shared temporarily among the devices connected to the link.
Transmitter and Receiver	There is a single transmitter and a single receiver.	There is a single transmitter and multiple receivers.
Example	Frame relay, T-carrier, X.25, etc.	Frame relay, token ring, Ethernet, ATM, etc.

Difference between P2P and Multipoint

- When there is a single dedicated link only between two devices, it is a point-to-point connection whereas, if a single link is shared by more than two devices then it is said to be a multipoint connection.
- In multipoint connection, the channel capacity is shared temporarily by the devices in connection. On the other hand, in a point-to-point connection, the entire channel capacity is reserved only for the two devices in the connection.
- In point-to-point connection, there can only be a single transmitter and a single receiver. On the other hand, in multipoint connection, there is a single transmitter, and there can be multiple receivers

Protocol

- Protocol is a set of rules that govern all aspect of data communication between computers on a network.
- These rules include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer.
- *A protocol is synonymous with rule. It consists of a set of rules that govern data communications.*
- *It determines what is communicated, how it is communicated and when it is communicated.*
- A **protocol** is the formal definition of external behaviour for communicating entities. It defines:
 - message formats
 - expected actions (message sent, data delivered, abort)
- *The key elements of a protocol are syntax, semantics and timing*

Key elements of Protocol

- **Syntax**
 - Structure or format of the data
 - Indicates how to read the bits - field delineation
- **Semantics**
 - Interprets the meaning of the bits
 - Knows which fields define what action
- **Timing**
 - When data should be sent and what
 - Speed at which data should be sent or speed at which it is being received.

Eg.IP,HTTP,FTP,POP,SMTP,Telnet etc.

Standards

Standards are developed by cooperation among standards creation Committees, forums, and government regulatory agencies.

Standards Creation Committees

- a) International Standards Organization (ISO)
- b) International Telecommunications Union (ITU)
- c) American National Standards Institute (ANSI)
- d) Institute of Electrical and Electronics Engineers (IEEE)
- e) Electronic Industries Association (EIA)
- f) Internet Engineering Task Force (IETF)

International Standards Organization (ISO)

- A multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world
- Dedicated to worldwide agreement on international standards in a variety field.
- Currently includes 82 memberships industrialized nations.
- Aims to facilitate the international exchange of goods and services by providing models for compatibility, improved quality, increased quality, increased productivity and decreased prices.

International Telecommunications Union (ITU)

- Also known as International Telecommunications Union-Telecommunication Standards Sector (ITU-T)
- An international standards organization related to the United Nations that develops standards for telecommunications.
- Two popular standards developed by ITU-T are:
 - i) V series – transmission over phone lines
 - ii) X series – transmission over public digital networks, email and directory services and ISDN.

American National Standards Institute (ANSI)

- A non-profit corporation not affiliated with US government.
- ANSI members include professional societies, industry associations, governmental and regulatory bodies, and consumer groups.
- Discussing the internetwork planning and engineering, ISDN services, signaling, and architecture and optical hierarchy.

Institute of Electrical and Electronics Engineers (IEEE)

- The largest national professional group involved in developing standards for computing, communication, electrical engineering, and electronics.
- Aims to advance theory, creativity and product quality in the fields of electrical engineering, electronics and radio.
- It sponsored an important standard for local area networks called Project 802 (eg. 802.3, 802.4 and 802.5 standards.)

Electronic Industries Association (EIA)

- An association of electronics manufacturers in the US.
- Provide activities include public awareness education and lobbying efforts in addition to standards development.
- Responsible for developing the EIA-232-D and EIA-530 standards.

Internet Engineering Task Force (IETF)

- Concerned with speeding the growth and evolution of Internet communications.
- The standards body for the Internet itself
- Reviews internet software and hardware.

Communication Architecture

- ❑ Strategy for connecting host computers and other communicating equipment.
- ❑ Defines necessary elements for data communication between devices.
- ❑ A communication architecture, therefore, defines a standard for the communicating hosts.
- ❑ A programmer formats data in a manner defined by the communication architecture and passes it on to the communication software.
- ❑ Separating communication functions adds flexibility, for example, we do not need to modify the entire host software to include more communication devices.

Layer Architecture

-
- ❑ Layer architecture simplifies the network design.
 - ❑ It is easy to debug network applications in a layered architecture network.
 - ❑ The network management is easier due to the layered architecture.
 - ❑ Network layers follow a set of rules, called protocol.
 - ❑ The protocol defines the format of the data being exchanged, and the control and timing for the handshake between layers.

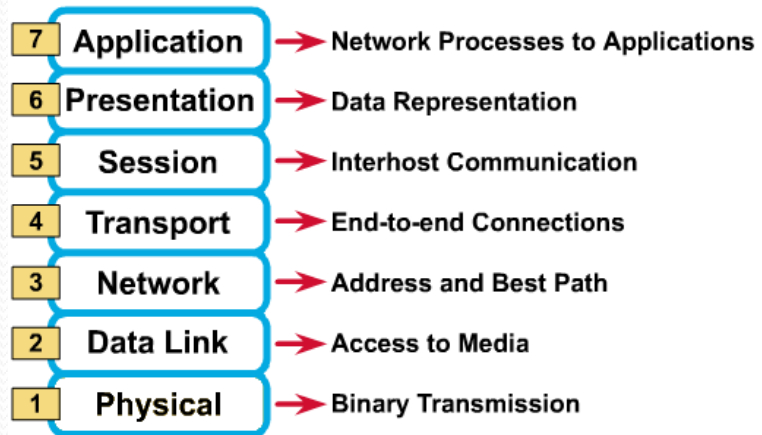
Open Systems Interconnection (OSI) Model

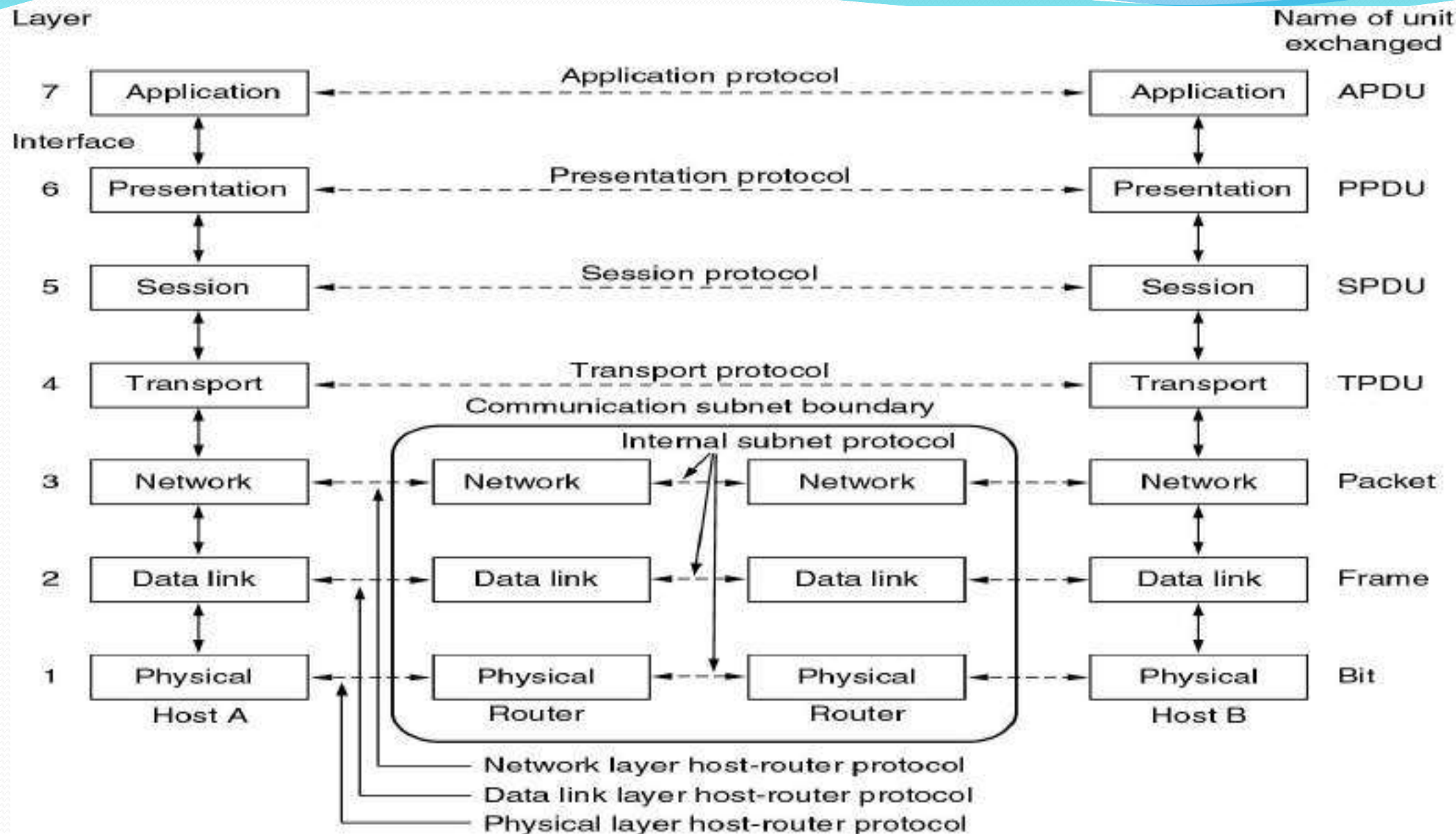
-
- ❑ International standard organization (ISO) established a committee in 1977 to develop an architecture for computer communication.
 - ❑ Open Systems Interconnection (OSI) reference model is the result of this effort.
 - ❑ In 1984, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture.
 - ❑ Term “open” denotes the ability to connect any two systems which conform to the reference model and associated standards.

OSI Reference Model

- The OSI model is now considered the primary Architectural model for inter-computer communications.
- The OSI model describes how information or data makes its way from application programmes (such as spreadsheets) through a network medium (such as wire) to another application programme located on another network.
- The OSI reference model divides the problem of moving information between computers over a network medium into SEVEN smaller and more manageable problems .
- This separation into smaller more manageable functions is known as layering.

OSI Reference Model: 7 Layers





How to remember

- “Please Do Not Throw Salami Pizza Away”
- “All people seem to need data processing.
- All = Application Layer.
- People= Presentation Layer.
- Seem = Session Layer.
- To = Transport Layer.
- Need = Network Layer.
- Data = Data Link Layer.
- Processing = Physical Layer.

OSI: A Layered Network Model

- ❑ The process of breaking up the functions or tasks of networking into layers reduces complexity.
- ❑ Each layer provides a service to the layer above it in the protocol specification.
- ❑ Each layer communicates with the same layer's software or hardware on other computers.
- ❑ The lower 4 layers (transport, network, data link and physical — Layers 4, 3, 2, and 1) are concerned with the flow of data from end to end through the network.
- ❑ The upper three layers of the OSI model (application, presentation and session—Layers 7, 6 and 5) are orientated more toward services to the applications.
- ❑ Data is Encapsulated with the necessary protocol information as it moves down the layers before network transit.

Physical Layer

- ❑ Provides physical interface for transmission of information.
- ❑ Defines rules by which bits are passed from one system to another on a physical communication medium.
- ❑ Covers all - mechanical, electrical, functional and procedural - aspects for physical communication.
- ❑ Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications.

Data Link Layer

- ❑ Data link layer attempts to provide reliable communication over the physical layer interface.
- ❑ Breaks the outgoing data into frames and reassemble the received frames.
- ❑ Create and detect frame boundaries.
- ❑ Handle errors by implementing an acknowledgement and retransmission scheme.
- ❑ Implement flow control.
- ❑ Supports points-to-point as well as broadcast communication.
- ❑ Supports simplex, half-duplex or full-duplex communication.

Network Layer

- ❑ Implements routing of frames (packets) through the network.
- ❑ Defines the most optimum path the packet should take from the source to the destination
- ❑ Defines logical addressing so that any endpoint can be identified.
- ❑ Handles congestion in the network.
- ❑ Facilitates interconnection between heterogeneous networks (Internetworking).
- ❑ The network layer also defines how to fragment a packet into smaller packets to accommodate different media.

Transport Layer

- ❑ Purpose of this layer is to provide a reliable mechanism for the exchange of data between two processes in different computers.
- ❑ Ensures that the data units are delivered error free.
- ❑ Ensures that data units are delivered in sequence.
- ❑ Ensures that there is no loss or duplication of data units.
- ❑ Provides connectionless or connection oriented service.
- ❑ Provides for the connection management.
- ❑ Multiplex multiple connection over a single channel.

Session Layer

- ❑ Session layer provides mechanism for controlling the dialogue between the two end systems. It defines how to start, control and end conversations (called sessions) between applications.
- ❑ This layer requests for a logical connection to be established on an end-user's request.
- ❑ Any necessary log-on or password validation is also handled by this layer.
- ❑ Session layer is also responsible for terminating the connection.
- ❑ This layer provides services like dialogue discipline which can be full duplex or half duplex.
- ❑ Session layer can also provide check-pointing mechanism such that if a failure of some sort occurs between checkpoints, all data can be retransmitted from the last checkpoint.

Presentation Layer

- Presentation layer defines the format in which the data is to be exchanged between the two communicating entities.
- Also handles data compression and data encryption (cryptography).
- Features:
 - Data encryption and decryption
 - Data compression
 - Data formatting
 - Data translation
 - Protocol conversion
 - Verify Data integrity

Application Layer

1. Application layer interacts with application programs and is the highest level of OSI model.
2. Application layer contains management functions to support distributed applications.
3. Examples of application layer are applications such as file transfer, electronic mail, remote login etc.

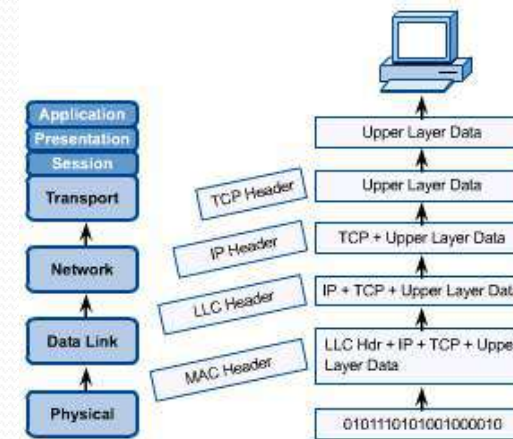
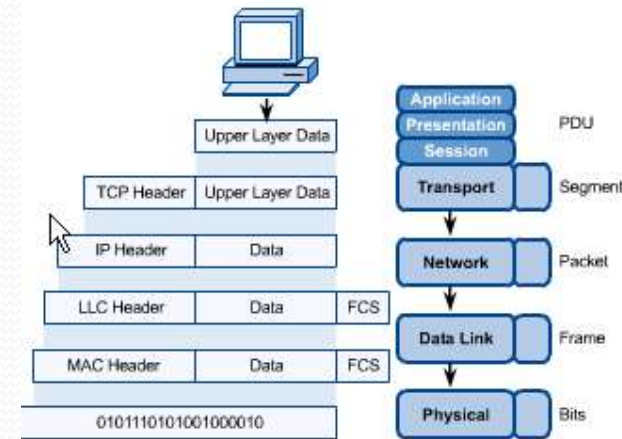


Main Features:

- Provides a user interface that allows users to interact with network services.
- Provides network services to user applications, such as email, file transfer, and remote login.
- Translate between different communication protocols, so that systems using different protocols can communicate with each other.
- Data formatting
- Inter-process communication:.
- Provides services that allow users to share network resources, such as printers and file servers.

OSI in Action

- ❏ A message begins at the top application layer and moves down the OSI layers to the bottom physical layer.
- ❏ As the message descends, each successive OSI model layer adds a header to it.
- ❏ A header is layer-specific information that basically explains what functions the layer carried out.
- ❏ Conversely, at the receiving end, headers are striped from the message as it travels up the corresponding layers.



Data Encapsulation

- Encapsulation is the process of breaking a message into packets, adding control and other information, and transmitting the message through the transmission media.

Five-step data encapsulation process:

- Upper layers prepare the data to be sent through the network.
- The Transport layer breaks the data into pieces called segments, adding sequencing and control information.
- The Network layer converts the segments into packets, adding logical network and device addresses.
- The Data Link layer converts the packets into frames, adding physical device addressing information.
- The Physical layer converts the frames into bits for transmission across the transmission media.

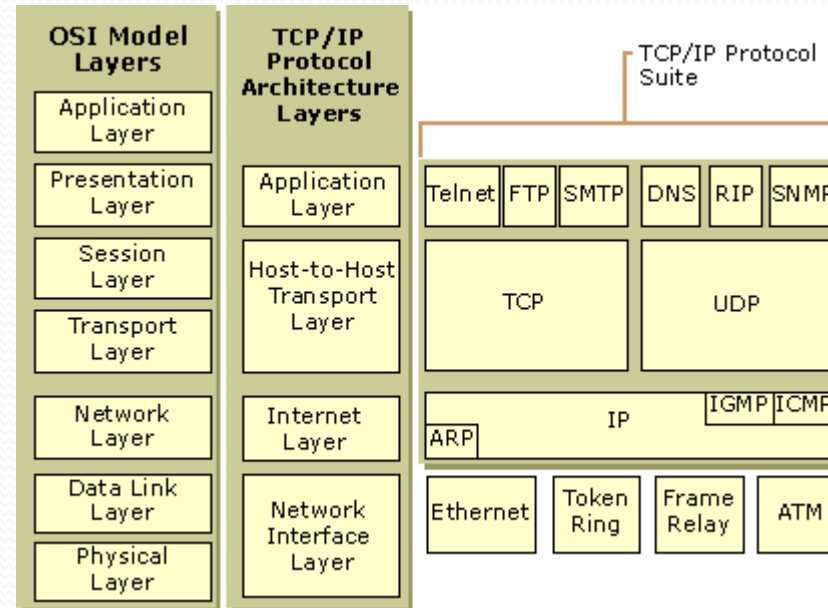
TCP/IP Reference Model

- TCP/IP means Transmission Control Protocol and Internet Protocol.
- The Defense Advanced Research Projects Agency ([DARPA](#)), the research branch of the U.S. Department of Defense, created the TCP/IP model in the 1970s for use in ARPANET, a wide area network that preceded the internet.
- It is the network model used in the current Internet architecture as well.
- **Protocols** are set of rules which govern every possible communication over a network.
- These protocols describe the movement of data between the source and destination or the internet.
- They also offer simple naming and addressing schemes.

TCP/IP Reference Model

Application	Application	FTP, Telnet, SMTP, HTTP..
Presentation		
Session		
Transport	Host-to-Host	TCP, UDP
Network	Internet	IP, ICMP, IGMP
Data Link	Network Access	Ethernet, Token-Ring ...
Physical		

TCP/IP Reference Model



Network Interface Layer

- **Physical addressing:** The Network Interface layer adds a physical address to the data packet, allowing it to be sent over the physical network.
- **Framing:** The Network Interface layer divides the data packet into smaller units called frames, which are transmitted over the network.
- **Error detection and correction:** The Network Interface layer includes error detection and correction mechanisms to ensure that the data transmitted over the network is accurate.
- **Flow control:** The Network Interface layer includes flow control mechanisms to manage the transmission of data between devices.
- **Access control:** The Network Interface layer provides access control to the physical network, allowing devices to share the network resources.
- **Media access management:** The Network Interface layer manages the access to the physical media, such as a shared Ethernet cable, to avoid collisions between data packets.
- **Protocols**
- Ethernet - for wired networks
- Wi-Fi (802.11) - for wireless networks
- Point-to-Point Protocol (PPP) - for point-to-point connections
- Serial Line Internet Protocol (SLIP) - for serial connections

Internet Layer

- The Internet layer is responsible for logical transmission of data packets over the internet. It can be compared to the network layer of the OSI model.
- The main functions of the internet layer are:
- It transmits data packets to the link layer.
- It routes each of the data packets independently from the source to the destination, using the optimal route.
- It reassembles the out-of-order packets when they reach the destination.
- It handles the error in transmission of data packets and fragmentation of data packets.
- The protocols used in this layer are:
- **Internet Protocol, IP:** It is a connectionless and unreliable protocol that provides a best effort delivery service. It transports data packets called datagrams that travel over different routes across multiple nodes.
- **Address Resolution Protocol, ARP:** This protocol maps the logical address or the Internet address of a host to its physical address, as printed in the network interface card.
- **Internet Control Message Protocol, ICMP:** It monitors sending the queries as well as the error messages.
- **Internet Group Message Protocol, IGMP:** It allows the transmission of a message to a group of recipients simultaneously.

Transport Layer

- The transport layer is responsible for error-free, end-to-end delivery of data from the source host to the destination host. It corresponds to the transport layer of the OSI model.
- The functions of the transport layer are:
- It facilitates the communicating hosts to carry on a conversation.
- It provides an interface for the users to the underlying network.
- It can provide for a reliable connection. It can also carry out error checking, flow control, and verification.
- The protocols used in this layer are:
- *Transmission Control Protocol, TCP*: a connection-oriented protocol that provides reliable, ordered, and error-checked delivery of data, with mechanisms for flow control and congestion control.
- *User Datagram Protocol, UDP*: It is a message-oriented protocol that provides a simple unreliable, connectionless, unacknowledged service. It is suitable for applications that do not require TCP's sequencing, error control or flow control. It is used for transmitting a small amount of data where the speed of delivery is more important than the accuracy of delivery.

Application Layer

- It provides the interface between the applications we use to communicate and the underlying network over which our messages are transmitted.
- Application layer protocols are used to exchange data between programs running on the source and destination hosts.
- There are many Application layer protocols and new protocols are always being developed.
- The functions of the application layer are:
 - It facilitates the user to use the services of the network.
 - It is used to develop network-based applications.
 - It provides user services like user login, naming network devices, formatting messages, and e-mails, transfer of files etc.
 - It is also concerned with error handling and recovery of the message as a whole.

- This layer uses a number of protocols, the main among which are as follows:
- *Hyper Text Transfer Protocol, HTTP*: It is the underlying protocol for world wide web. It defines how hypermedia messages are formatted and transmitted.
- *File Transfer Protocol, FTP*: It is a client-server based protocol for transfer of files between client and server over the network.
- *Simple Mail Transfer Protocol, SMTP*: It lays down the rules and semantics for sending and receiving electronic mails (e-mails).
- *Domain Name System, DNS*: It is a naming system for devices in networks. It provides services for translating domain names to IP addresses.
- *TELNET*: It provides bi-directional text-oriented services for remote login to the hosts over the network.
- *Simple Network Management Protocol, SNMP*: It is for managing, monitoring the network and for organizing information about the networked devices.

Comparison of OSI and TCP/IP Models

- Both of them use a layered architecture to explain data communication process in computer networks.
- Each layer performs well-defined functions in both models.
- Similar types of protocols are used in both models.
- OSI and TCP/IP reference models are open in nature.
- Both models give a good explanation on how various types of network hardware and software interact during a data communication process.
- Data hiding principle is well maintained on each layer in the two models. The core level functional details of each layer are not revealed to other layers.
- Transport layer defines end-end data communication process and error-correction techniques in both the models.
- OSI and TCP/IP reference models process data in the form of packets to perform routing.

Difference between OSI and TCP/IP

OSI MODEL	TCP/IP MODEL
1. 7 layers present in the architecture.	Only 4 layers are present.
2. Not practically implemented yet.	Practical Model.
3. Layering aspects, functions of each layer and division of responsibilities are specifically presented by this model.	Division of responsibilities on each layer is not so specific.
4. The concept of services, interfaces and protocols are well explained.	No clear distinction between the three
5. Model was devised first and protocols were latter fitted to appropriate layers.	The protocols came first and model was just explanation of protocols based on 4 layers.
6. Widely used as a standard reference model in the design of computer networks.	Not considered as a design standard due to the failure in distinguishing services, interfaces and protocols.
7. Connectionless and connection oriented services are there in Network layer but only connection oriented services in Transport layer.	Connectionless and connection oriented services in transport layer but only connectionless service in Network layer.
8. This is a protocol independent model.	This is a protocol specific model.

Internet

What's the Internet: "nuts and bolts" view

- ❑ millions of connected computing devices: *hosts, end-systems*
 - pc's workstations, servers
 - PDA's phones, toastersrunning *network apps*
- ❑ *communication links*
 - fiber, copper, radio, satellite
- ❑ *routers*: forward packets (chunks) of data thru network



What's the Internet: "nuts and bolts" view

- *protocols*: control sending, receiving of msgs
 - e.g., TCP, IP, HTTP, FTP, PPP
- *Internet*: "network of networks"
 - loosely hierarchical
 - public Internet versus private intranet




Internet and ISPs

- The public Internet is a world-wide computer network, that is, a network that interconnects millions of computing devices throughout the world.
- The Internet is a global, interconnected computer network in which every computer connected to it can exchange data with any other connected computer.
- The Internet is the physical connection of millions of networks.
- Most of these computing devices are traditional desktop PCs, Unix-based workstations, and so called servers that store and transmit information such as Web (WWW) pages and e-mail messages.
- Increasingly, nontraditional computing devices such as Web TVs, mobile computers, pagers, and toasters are being connected to the Internet.
- In the Internet jargon, all of these devices are called hosts or end systems.
- The Internet applications with which many of us are familiar, such as the Web and e-mail, are network application programs that run on such end systems.

- **End systems**, as well as most other "pieces" of the Internet, run protocols that control the sending and receiving of information within the Internet.
- **TCP (the Transmission Control Protocol) and IP (the Internet Protocol)** are two of the most important protocols in the Internet. The Internet's principal protocols are collectively known as TCP/IP.
- **End systems** are connected together by communication links. Links are made up of different types of physical media, including coaxial cable, copper wire, fiber optics, and radio spectrum.
- Different links can transmit data at different rates. The link transmission rate is often called the link bandwidth and is typically measured in bits/second

- Usually, end systems **are** not directly attached to each other via a single communication link. Instead, they are indirectly connected to each other intermediate switching devices known as **routers**.
- The topology of the Internet, that is, the structure of the interconnection among the various pieces of the Internet, is loosely hierarchical.
- Roughly speaking, from bottom-to-top, the hierarchy consists of end systems connected to local Internet service providers (**ISPs**) **through access networks**.
- **An access network** may be a so called local area network within a company or university, a dial telephone line with a modem, or a high-speed cable-based or phone-based access network.
- **Local ISPs** are in turn connected **to regional ISPs**, which are in turn connected to national and **international ISPs**. The national and international ISPs are connected together at the highest tier in the hierarchy.

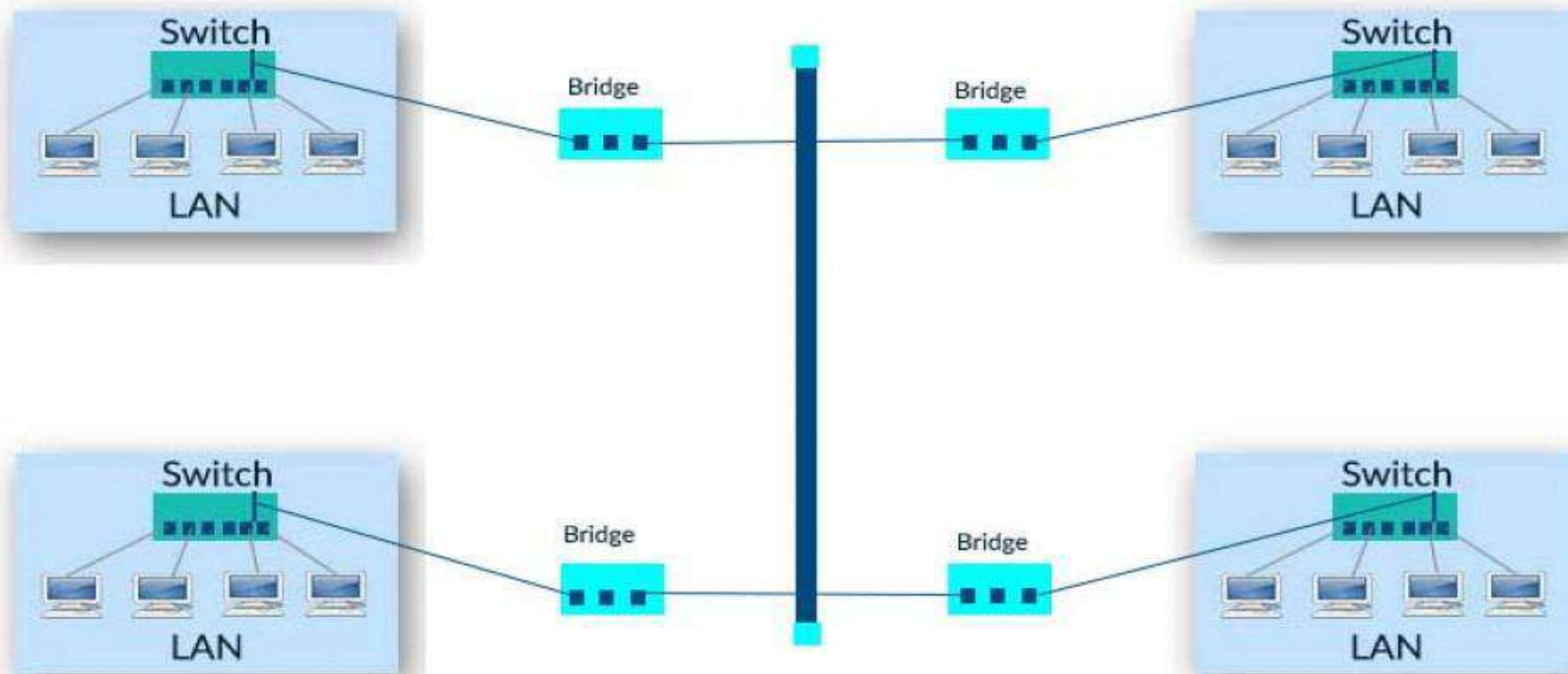
- 
- An Internet service provider (ISP) is a company that provides customers with Internet access. Data may be transmitted using several technologies, including dial-up, DSL, cable modem, wireless or dedicated high-speed interconnects.
 - Other services, such as telephone and television services, may be provided as well. The services and service combinations may be unique to each ISP.
 -

Backbone Network

- Core network and backbone network typically refer to the high capacity communication facilities that connect primary nodes. Core/backbone network provides path for the exchange of information between different sub-networks.
- Edge network provides information exchange between the access network and the core network.
- The devices and facilities in the edge networks are switches, routers, routing switches and a variety of MAN/WAN devices, which are often called edge devices.
- Edge network provide entry points into carrier/service provider core/backbone networks.

Bus Backbone(Distributed Backbone)

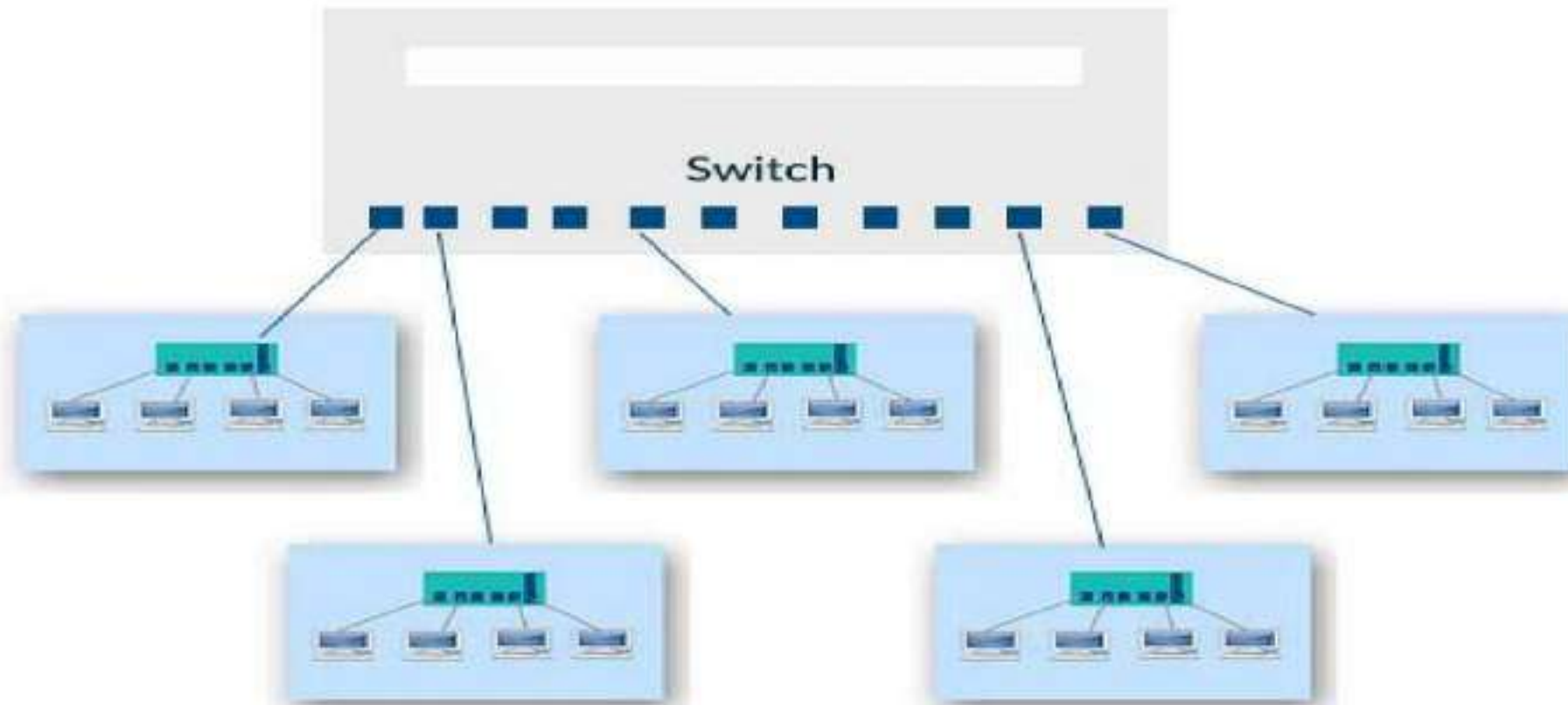
- The Bus backbone handles bus topology as well as all its protocols that are adaptable with bus topology like 10Base2 or 10Base5.
- To connect the different subnetwork at the different floors. All the LAN is connected together to the different floor of the building.
- They also form backbone which is star topology, thus the multiple LAN are connected through a bus Backbone to exchange the data and share the resources .
- Thus the backbone is connected through each other and the backbone which are made for each user are used to flow the information



Bus Backbone Network Interconnecting different LAN's

Star Backbone

- Star backbone uses wiring hubs, switches to generate a backbone to connect different LAN's or subnetwork.
- The one switch is used to interconnect the different LAN's. So it also referred as a switched backbone.
- In star backbone, the particular LAN of each floor are interconnected with the star backbone.
- In the star backbone switch perform as a backbone. It is installed at one unify location in the building that location may be a computer centre or data centre.
- Separate cable runs from the switch to each floor of the LAN's. Each of the LAN is implemented in star topology hubs can be equipped in a closet at each floor or hubs or switches can be installed in the same place where the backbone switch is equipped.



Star Backbone

Internet Backbone and ISPs

- An Internet backbone refers to one of the principal data routes between large, strategically interconnected networks and core routers on the Internet.
- An Internet backbone is a very high-speed data transmission line that provides networking facilities to relatively small but high-speed Internet service providers all around the world.
- Internet backbones are the largest data connections on the Internet. They require high-speed bandwidth connections and high-performance servers/routers.
- Backbone networks are primarily owned by commercial, educational, government and military entities because they provide a consistent way for Internet service providers (ISPs) to keep and maintain online information in a secure manner.

- Some of the largest companies running different parts of the Internet backbone include UUNET, AT&T, GTE Corp. and Sprint Nextel Corp. Their routers are connected with high-speed links and support different range options like T₁, T₃, OC₁, OC₃ or OC₄₈.

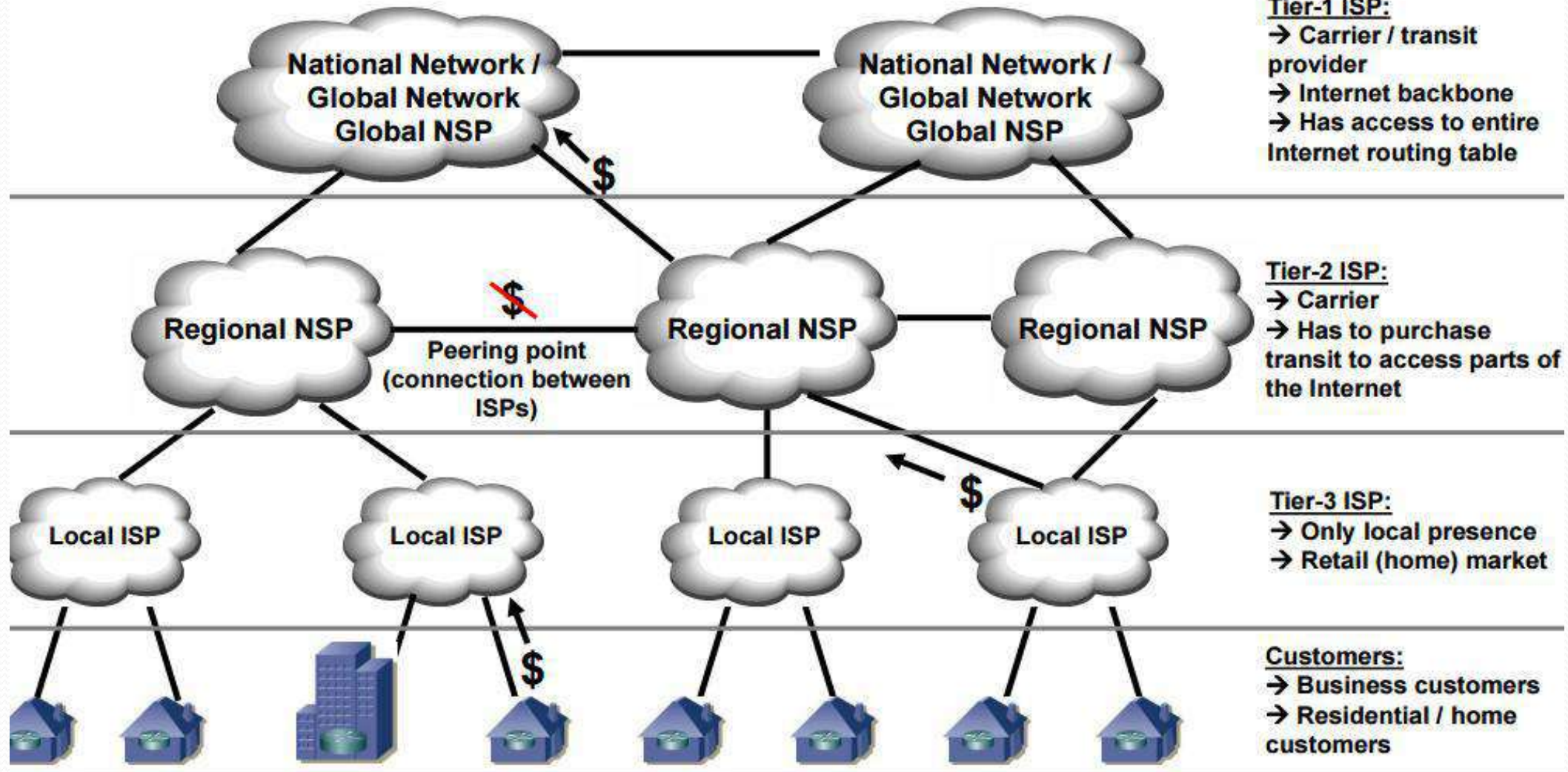
A few key features of an Internet backbone include:

- ISPs are either connected directly to their contingency backbones or to some larger ISP that is connected to its backbone.
- The smaller networks are interlinked to support the multiversatile backup that is required to keep the Internet services intact in case of failure. This is done through transit agreements and peering processes.
- The transit agreement is a monetary contract between several larger and smaller ISPs. It is initiated to share traffic loads or to handle data traffic in case of a partial failure of some networks. In peering, several ISPs also share features and traffic burden.
- The first Internet backbone was named NSFNET. It was funded by the U.S. government and introduced by the National Science Foundation (NSF) in 1987. It was a T₁ line that consisted of approximately 170 smaller networks operated at 1.544 Mbps. The backbone was a combination of fiber-optic trunk lines, each of which had several fiber-optic cables wired together to increase capacity.

3. Internet Carriers / Providers (1/3)

→ Three classes of ISPs fulfill different roles in the Internet:

ISP: Internet Service Provider
NSP: Network Service Provider
\$: Payments for service
Ⓢ: No payments



History of Internet

- The Internet grew from ARPANET the first computer network designed for the Advanced Research Projects Agency (ARPA) of the U.S Department of Defense
- ARPA sponsored research on interconnecting geographically remote computers to allow communication and sharing of data and resources
- The goal was to create a communications network that could exist even if a part of it was incapacitated.
- One of the early developments that proved significant to the success of ARPANET (which later on becomes the Internet) were “packet switching” and “TCP/IP.

- Packet switching involves digital systems that transmit data in small packets that use the best current path to their destination
- TCP/IP is the core Internet protocol that allows computers to communicate with each other
- Realizing the value of interconnected computers the academic community started with its own research network
- The NSFNet, created and named for the National Science Foundation, linked academic networks that connected universities and research organizations around North America.
- Networks from Europe and other countries were connected to NSFNet making it the backbone of the Internet

- ARPANET was decommissioned and the management of the Internet was passed on to the NSFNET(NSFNET was a network for research computing deployed in the mid-1980s that in time also became the first backbone infrastructure for the commercial public Internet.)
- Restriction on commercial use was lifted
- The emergence of World Wide Web, and Mosaic brought an unprecedented growth to the Internet
- NSFNET reverts back to a research project, leaving the Internet in commercial hands and its management to independent organizations

Application of Internet

- E-mail
- Searchable Data (Web Sites)
- E-Commerce
- News Groups
- Internet Telephony (VoIP)
- Video Conferencing
- Chat Groups
- Instant Messengers
- Internet Radio

Network/Internet Services

- The Internet allows distributed applications running on its end systems to exchange data with each other.
- These applications include remote login, file transfer, electronic mail, audio and video streaming, real-time audio and video conferencing, distributed games, the World Wide Web, and much, much more.
- The Network/Internet provides two services to its distributed applications:
- a connection oriented service and
- a connectionless service.
- connection oriented service guarantees that data transmitted from a sender to a receiver will eventually be delivered to the receiver in order and in its entirety.
- Connectionless service does not make any guarantees about eventual delivery.

Connection-Oriented Service

Connection-oriented services must first establish a connection between the two end-points (sending/receiving) before passing any data traffic between them. An example of a connection-oriented service is Frame Relay, where a VC (virtual connection) is required between both end-points before data traffic can be exchanged. Connection-oriented service involves three phases:

- **Connection establishment**
- **Data transfer**
- **Connection termination**
- During connection establishment, the end-points can reserve resources and negotiate traffic parameters for the connection; for example, to ensure Quality of Service (QoS).
- Connection oriented service is more reliable than connectionless service. We can send the message in connection oriented service if there is an error at the receivers end. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

Connectionless Services

- **Connectionless services** can send data without requiring an established connection. Connection-oriented services provide some level of delivery guarantee, whereas connectionless services do not. An example of a connectionless service is any IP service, such as the Internet. No established connection is made between a web browsing user and the home page being viewed.
- In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

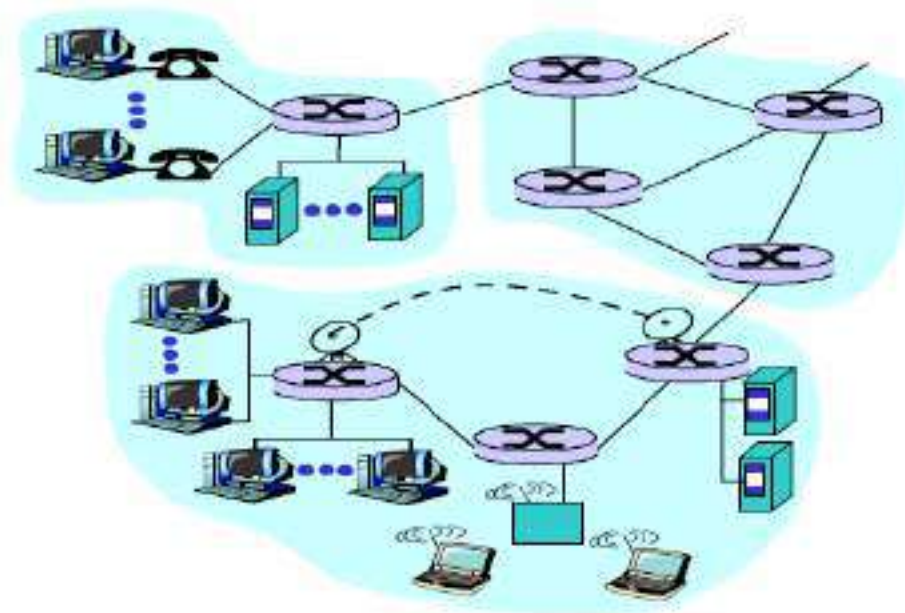
Comparision

- In connection oriented service authentication is needed, while connectionless service does not need any authentication.
- Connection oriented protocol makes a connection and checks whether message is received or not and sends again if an error occurs, while connectionless service protocol does not guarantees a message delivery.
- Connection oriented service is more reliable than connectionless service.
- Connection oriented service interface is stream based and connectionless is message based.

Network Structure

A closer look at network structure:

- **network edge:**
applications and hosts
- **network core:**
 - routers
 - network of networks
- **access networks, physical media:**
communication links



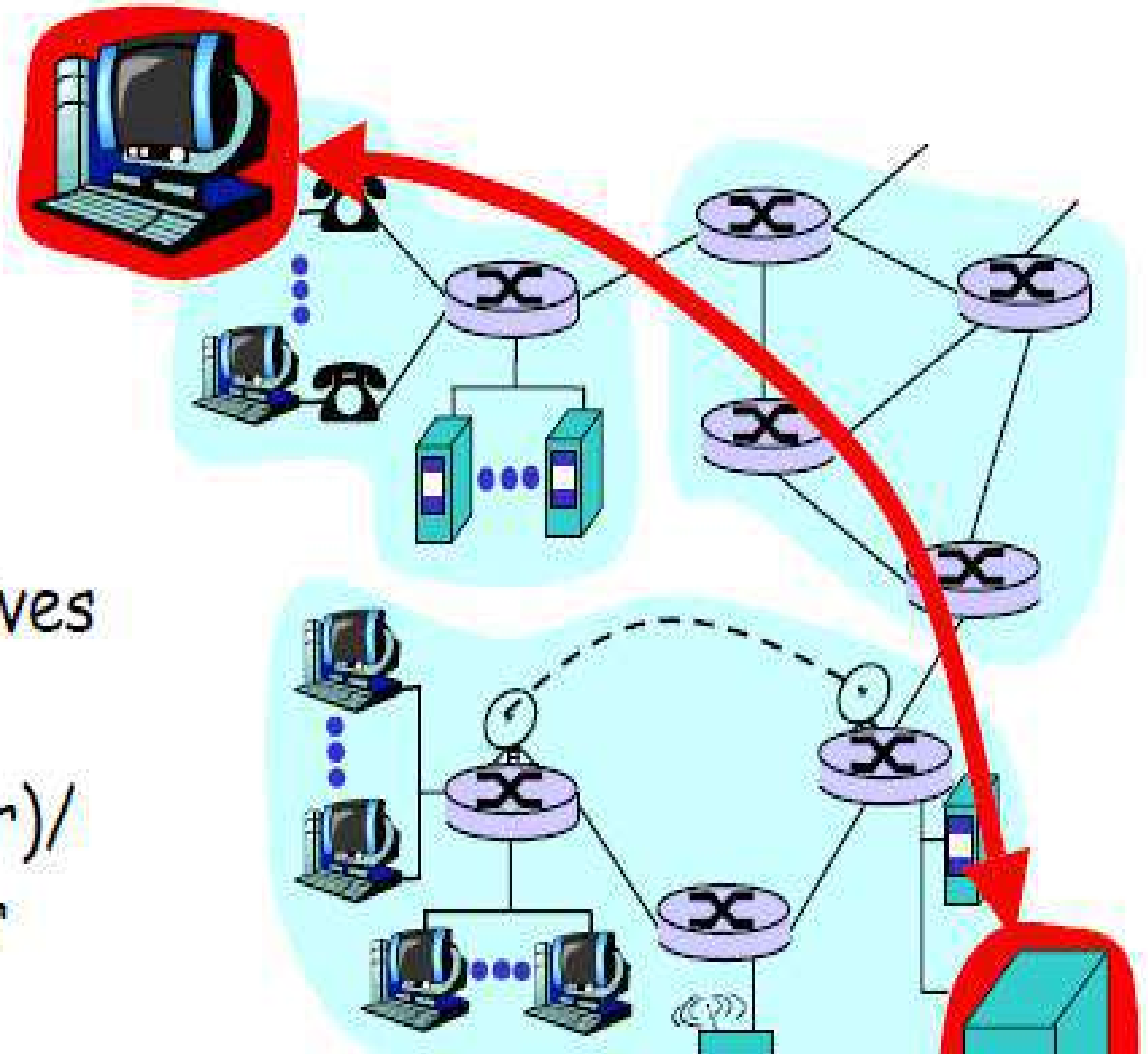
□ end systems (hosts):

- run application programs
- e.g., WWW, email
- at "edge of network"

□ client/server model

- client host requests, receives service from server
- e.g., WWW client (browser)/server; email client/server

□ peer-to-peer model:



- The computers that we use on a daily basis are often referred to as hosts or **end systems**.
- They are referred to **as hosts** because they host (run) application-level programs such as a Web browser or server program, or an email program.
- They are also referred to as **end systems** because they sit at the edge of the network.
- Hosts are sometimes further divided into two categories: **clients and servers**.
- Informally, clients often tend to be desktop PCs or workstations, whereas servers are more powerful machines.