Unit-1

Introduction to Computer Network:-

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to process communication and resource sharing among wide range of users.

Uses:

i) Process communication through email, video conferencing, instant messanging etc.
ii) Enable multiple users to share a single hardware device like a printer or scanner.
iii) Enable file sharing across network.
iv) Make information easier to access and maintain among network users.
v) Allows sharing of software or operating programs on remote systems.

Benefits/Advantages:

i) It is highly flexible.
ii) It is an inexpensive system.
iii) It makes file sharing easier.
iv) It boosts storage capacity.
v) It increases cost efficiency.
vi) It allows for more convinent resource sharing.

Disadvantages:

i) It comes with the risk of security issues.
ii) It encourages people to become dependent on computers.
iii) It opens up a doorway for computer viruses and malware.
iv) If a computer network's main server breaks down, the entire system would become useless. Hence, it lacks robustness.
v) It requires an efficient handler.

Scanned by TapScanner

⊛. Network Topologies:-

Network topology refers to the physical or logical layout of a network. It defines the way different nodes are placed and interconnected with eachother. Network topology also describes how the data is transfered between these nodes. Network topology is categorized into five basic models as follows:-

i) Bus topology: All the devices/nodes are connected sequentially to the same transmission line. This is simple, low-cost topology, but its single point of failure presents a risk.

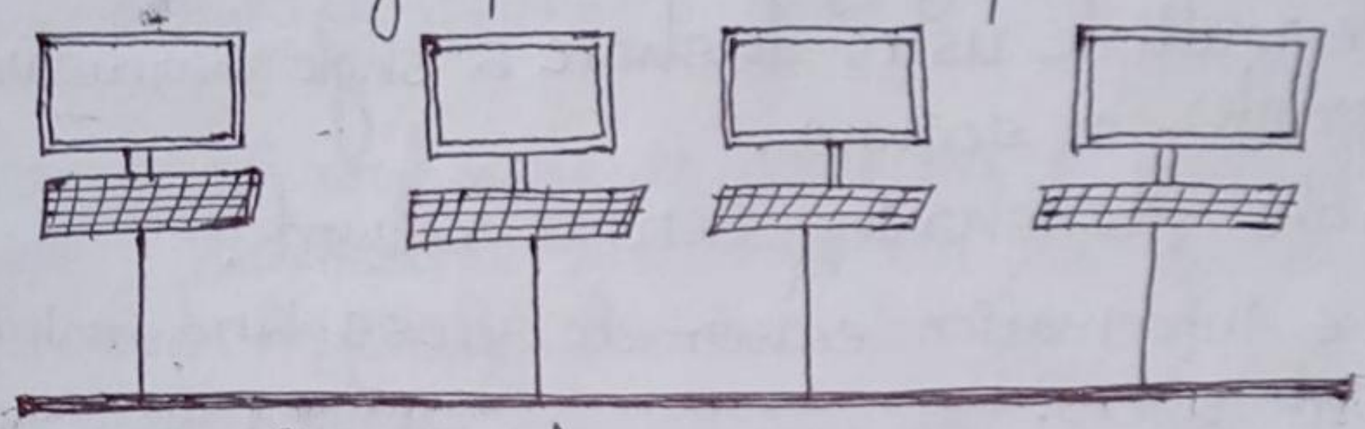


Fig. Bus Topology.

ii) Star Topology: All the nodes in the network are connected to a central device like a switch via cables. Failure of individual node or cable does not necessarily create downtime in the network but the failure of central device can. This topology is the most preferred and popular model.

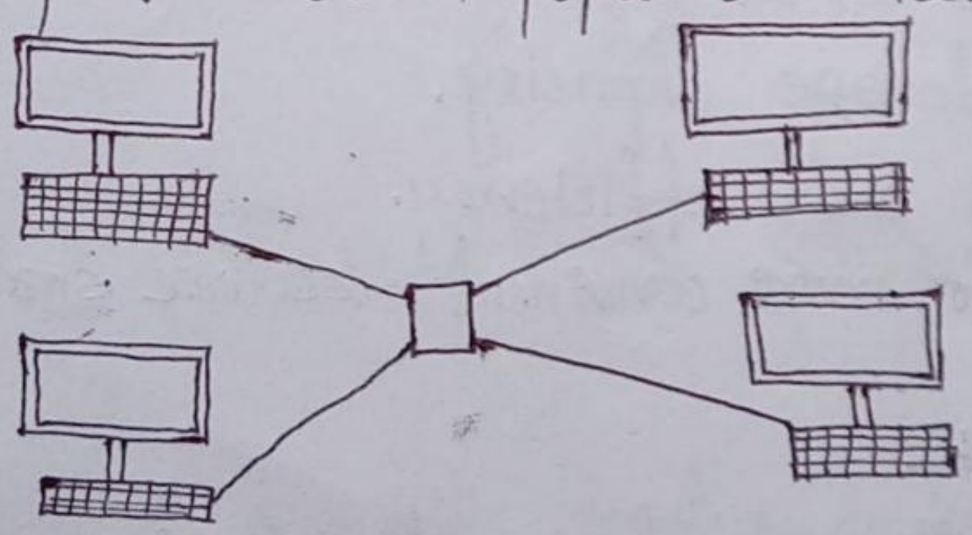


Fig. Star Topology

iii) Ring Topology: All network devices are connected sequentially to same transmission line like bus topology except that the transmission line ends at the starting node, forming a ring. It overcomes many of the limitations of bus topology.

Scanned by TapScanner

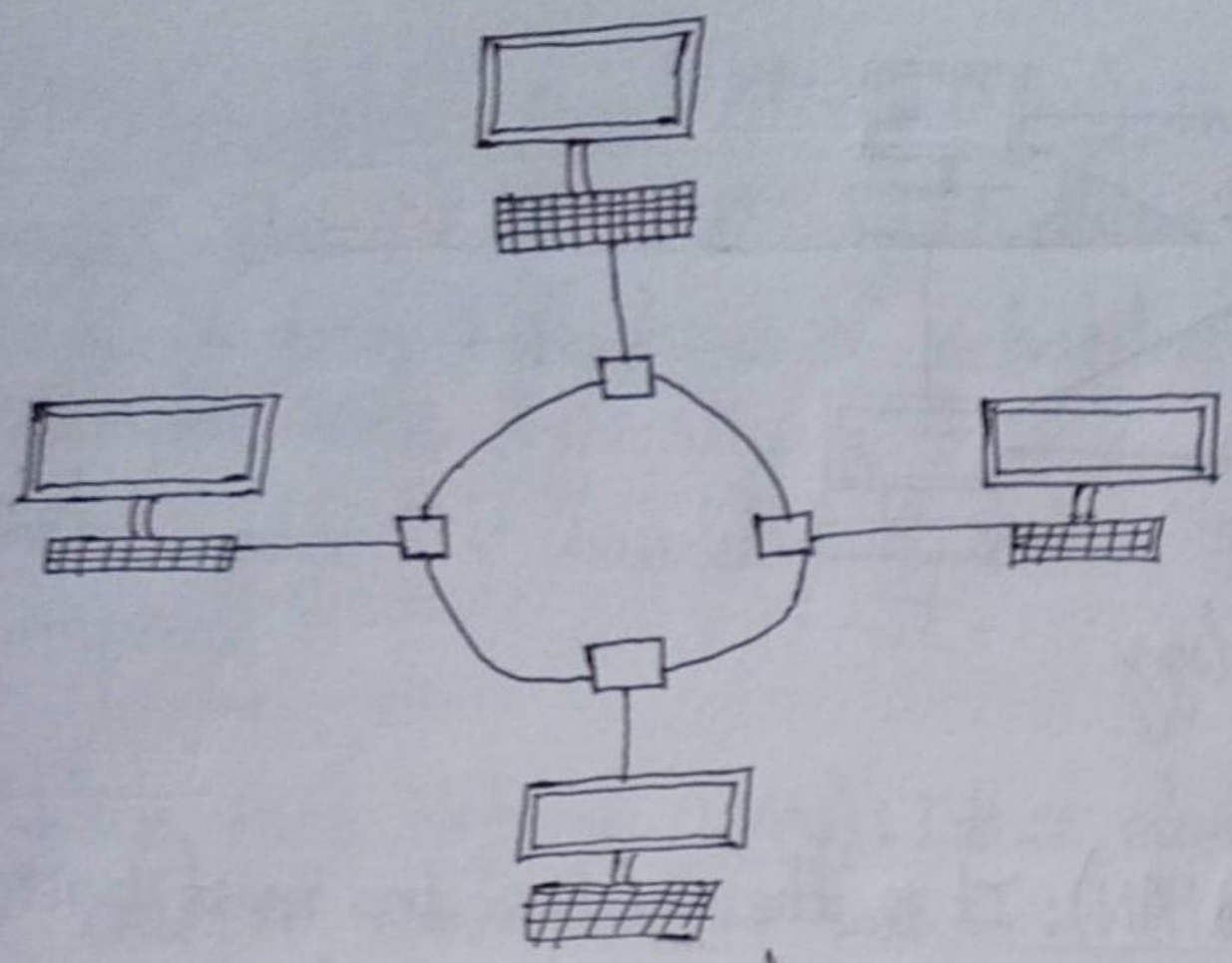


Fig. Ring Topology

iv) Tree Topology: A root node is connected to two or more sub-level nodes, which themselves are connected hierarchically to sub-level nodes. Physically, the tree topology is similar to bus and star topology; the network transmission line may have a bus topology, while low-level nodes connect using star topology.

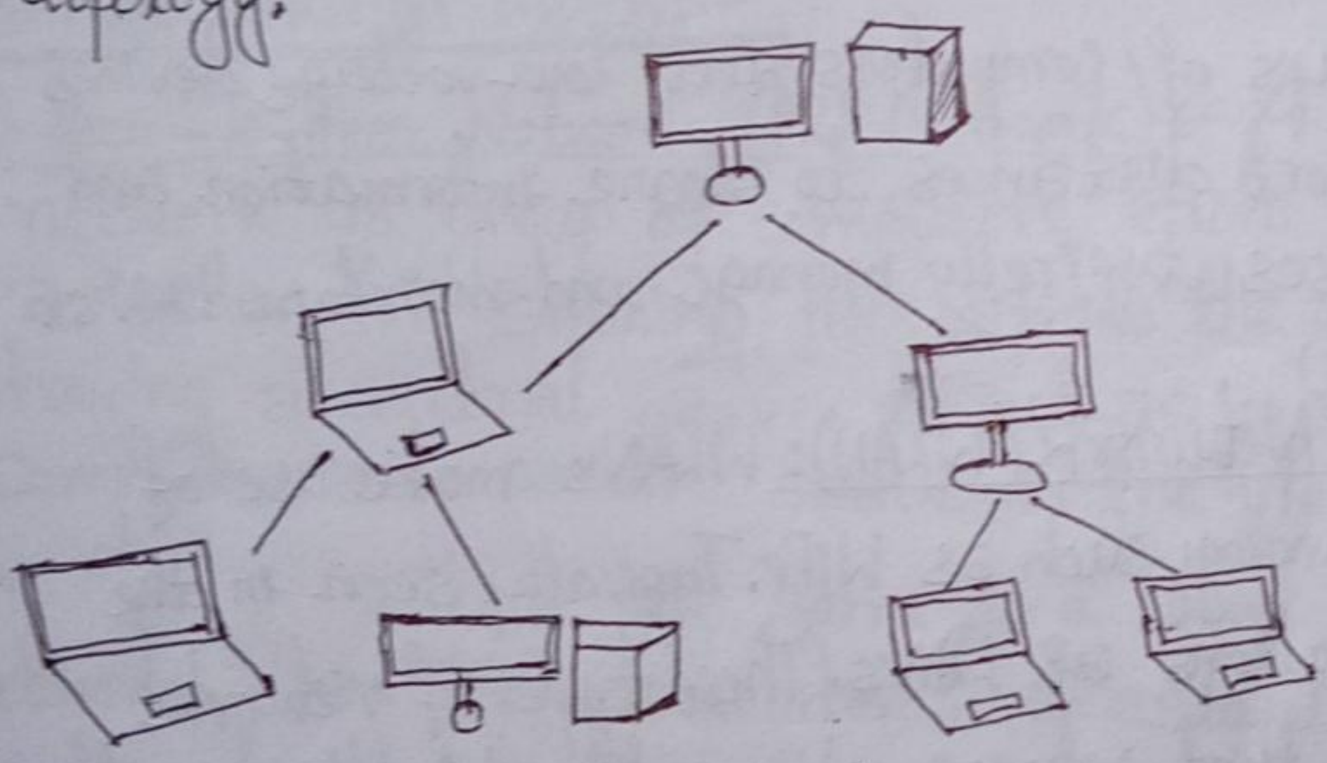


Fig. Tree Topology

v) Mesh Topology: In mesh topology each computer and network device is interconnected with one another. There are two forms of this topology: full-mesh and partially-connected mesh. In full mesh topology, every computer in the network has a connection and number of connections in network can be calculated as $n(n-1)/2$. where, n is number of computers in network. In partially connected mesh topology at least two of the computers in the network have connections to multiple other computers in that network.

Scanned by TapScanner

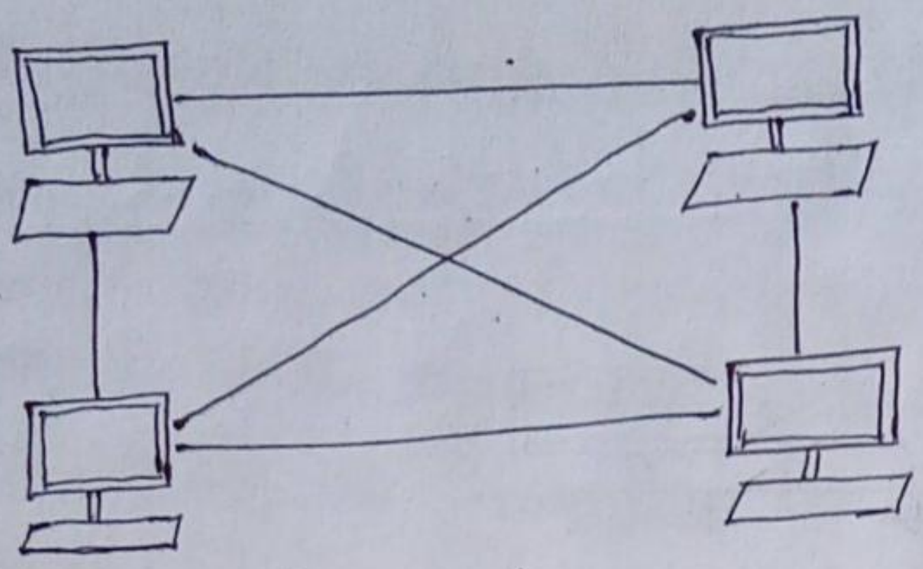


Fig. Mesh Topology

⊛ Network Types:

i) Personal Area Network (PAN): It is the smallest and most basic type of network. A PAN is made up of a wireless modem, one or two, phones, printers, tablets etc, and revolves ~~ab~~ around one person in the building. These types of networks are typically found in small offices or residences and are managed by one person or organization from a single device.

ii) Local Area Network (LAN): It is one of the simplest network. LAN's connect groups of computers and low-voltage devices together across short distances. to share information and resources. Enterprises typically manage and maintain LAN's.

iii) Wireless Local Area Network (WLAN): WLAN's make use of wireless network technology such as WiFi. Typically seen in the same types of applications as LAN's. These types of networks don't require devices that rely on physical cables to connect to the network.

iv) Campus Area Network (CAN): Larger than LAN's but smaller than MAN's. These types of networks are typically seen in universities, large K-12 schools, districts or small business. They can be spread across several buildings that are fairly close to each other so users can share resources.

Scanned by TapScanner

v) Metropolitan Area Network (MAN): These types of networks are larger than LAN's but smaller than WAN's and incorporate elements from both types of networks. MAN's span an entire geographic area typically a town or city. Ownership and maintenance is handeled by either a single person or company.

vi) Wide Area Network (WAN): It is slightly more complex than a LAN. A WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other and one large network to communicate even when they are miles apart. The internet is the most basic example of a WAN connecting all computers together around the world.

⊛ Networking Types:-

i) Peer-To-Peer Network (P2P Network):- A peer-to-peer (P2P) network is group of computers each of which acts as a node for sharing files within the group. Instead of having a central server to act as a shared drive, each computer acts as the server for the files stored upon it.

These are same as a home network or office network. When P2P networks are established over the internet, the size of the network and the files available allow huge amounts of data to be shared. Peer-to-peer networks are usually associated with internet piracy and illegal file sharing.

ii) Multi-point Architectures:- Multipoint architecture means the channel is shared among multiple devices or nodes. In this architecture there is one transmitter and many receivers. In this architecture link is provided all times for sharing the connection among nodes. It does not provide security and privacy because communication channel is shared.

Scanned by TapScanner

Client/Server Architecture: Client/Server architecture is a computing model in which the server hosts, delivers and manages most of the resources and services to be consumed by the client. This type of architecture has one or more client computers connected to a central server over a network or internet connection. This architecture is also known as a networking computing model because all the requests and services are delivered over a network.

Client/Server architecture is a producer/consumer computing architecture where the server acts as the producer and the client as a consumer. A server computer can manage several clients simultaneously, whereas one client can be connected to several servers at a time, each providing a different set of services.

⊛ Network Protocals:-

A network protocal is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design. Network protocals are the reason we can easily communicate with people all over the world, and thus play a critical role in modern digital communications.

Similar to the way that speaking the same language simplifies communication between two people, network protocals make it possible for devices to interact with each other because of predetermined rules built into devices software and hardware. There are thousands of different network protocals, but they all perform one of three primary actions:

→ Communication
→ Network Management
→ Security.

Scanned by TapScanner

Following are the few examples of the most commonly used network protocols:

- Hypertext Transfer Protocal (HTTP): This Internet protocal defines how data is transmitted over the Internet and determines how web servers and browsers should respond to commands. This protocal appears at the beginning of various URLs or web addresses online.
- Secure Socket Shell (SSH): This protocal provides secure access to a computer, even if is on an unsecured network. SSH is particularly useful for network administrators who need to manage different systems remotely.
- Short Message Service (SMS): This communication protocal was created to send and receive text messages over cellular networks.

⇒ In short Protocal is a set of rules that governs communication. The key elements of protocal are syntax, semantics and timing.

Syntax → It refers to the structure and format of the information data.

Semantics → It refers to the meaning of each section of bits. It does an route identify the route to be taken or the final destination of the message.

Timing → It refers to two characteristics: when data should be sent and how fast it should be sent.

⊛. Network Standards:

Network standards define the rules for data communications that are needed for interoperability of networking technologies and processes. Standards help in creating and maintaining open markets and allow different vendors to compete on the basis of the quality of their products while being compatible with existing market products.

Scanned by TapScanner

Types:

1) De facto → These are the standards that are followed without any formal plan or approval by any organization. They have come into existence due to traditions or facts. For example, the HTTP has started as a de facto standard.

2) De jure → These standards are the ones which have been adopted through legislation by any officially recognized standards organization. Most of the communication standards that are used today are de jure standards.

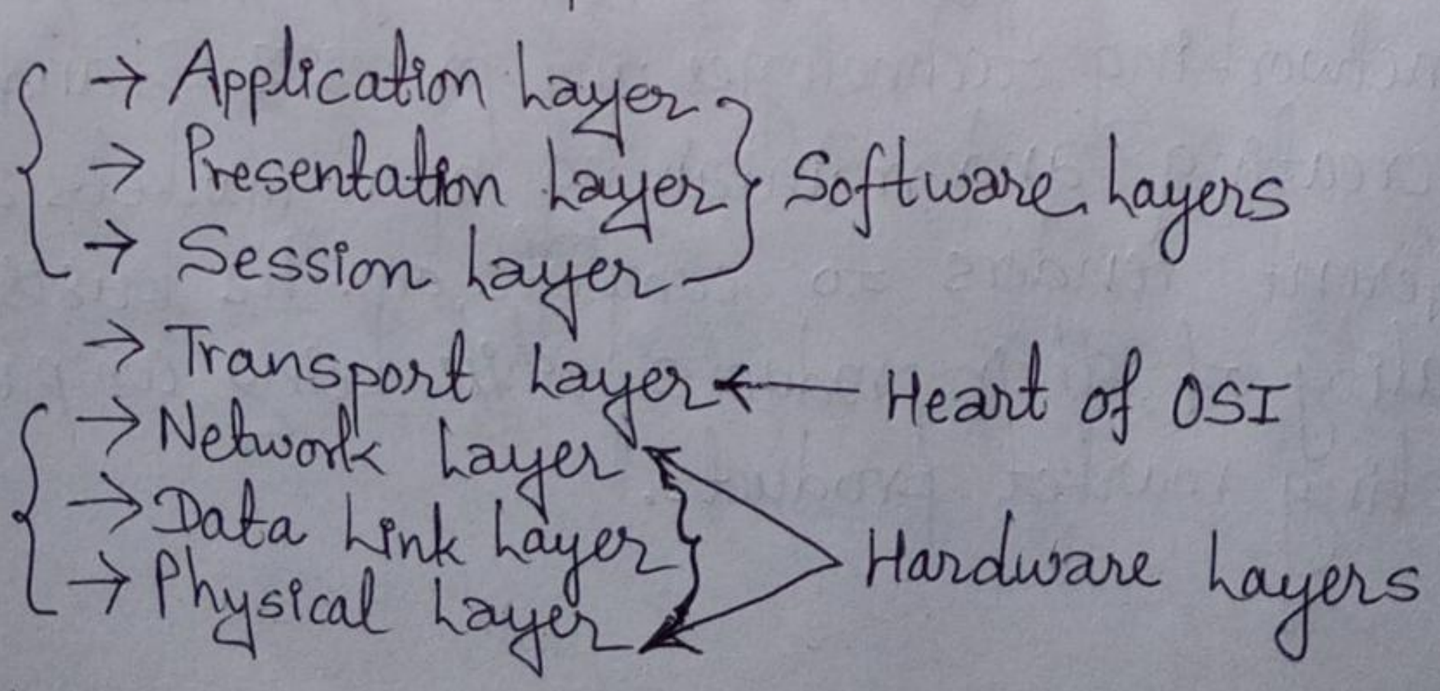
Standards Organizations:

Following are some of the noted standard organizations.

→ International Standards Organization (ISO).
→ International Telecommunication Union (ITU).
→ Instute of Electronics and Electrical Engineers (IEEE).
→ American National Standards Institute (ANSI).
→ Electronic Industries Association (EIA).

⊛ OSI Refrence Model:

OSI stands for Open Systems Interconnection. It has been developed by ISO → 'International Organization of 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.



Scanned by TapScanner

1. Physical Layer (layer 1):- It is the lowest layer of the OSI refrence model. ~~is the physical layer.~~ It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s, and send them to Data Link layer, which will put the frame back together.

Network Layer, Data Link Layer and Physical Layer are also known as lower layers or Hardware layers. Example of Physical layer devices are Hub, Repeater, Modem, Cables etc.

Functions of physical layer:

i) Bit synchronization → Clock (i.e. clock signal) controls both sender and receiver providing synchronization at bit level.

ii) Bit rate control → It defines transmission rate i.e, number of bits sent per second.

iii) Physical topologies → It specifies which network topology is used to arrange nodes/devices.

iv) Transmission mode → It defines the way in which data flows, like simplex, half-duplex and full-duplex.

2. Data Link Layer (Layer 2):- It is responsible for node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. It is divided into two sub layers:

i) Logical Link Control (LLC)
ii) Media Access Control (MAC).

Packet in Data Link Layer is called Frame. Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines. Switch & Bridge are Data Link Layer devices.

Scanned by TapScanner

Functions of data link layer:

i) Framing → It provides a way for a sender to transmit a set of bits that are meaningful to the receiver.

ii) Physical Addressing → After creating frames data link layer adds physical address (MAC address) of sender and receiver in the header of each frame.

iii) Error Control → This layer detects and retransmits damaged or lost files.

iv) Flow Control → The data rate must be constant on both sides else the data may get corrupted.

3. Network layer (layer 3): It works for the transmission of data from one host to the other located in different networks. It also takes care of selection of shortest path to transmit the packet, from the number of routes available. Segment in network layer is refered as packet.

Functions:

i) Routing → The network layer protocals determine which route is suitable from source to destination. This function of network layer is known as routing.

ii) Logical Addressing → The sender & receiver's IP address are placed in the header by network layer to indentify each device.

4. Transport Layer (layer 4): Transport layer provides services to application layer and takes services from network layer. It is responsible for the End to End delivery of the complete message.

- At sender's side → Transport layer receives the formatted data from the upper layers, performs Segmentation and also implements Flow and Error control to ensure proper data transmission.

- At receiver's side → Transport layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reasembling of the segmented data.

Scanned by TapScanner

Data in the transport layer is called as segments. This layer is operated by the Operating System. It is called as Heart of OSI model.

Functions:

i) Segmentation and Reassembly → This layer accepts the message from the (session) layer, breaks into smaller units. The transport layer at the destination station reassembles the message.

ii) Service Point Addressing → This layer includes service point address which makes sure that the message is delivered to the correct process.

5. Session Layer (layer 5):

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

Functions:-

i) Session establishment, maintenance and termination → This layer allows the two processes to establish, use and terminate connection.

ii) Synchronization → This layer has checkpoints considered as synchronization points and help to identify the errors and data loss is avoided.

iii) Dialog Controller → The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

6. Presentation Layer (layer 6):

Presentation Layer is also called Translation layer. The data from application layer is extracted here and manipulated as per the required format to transmit over the network.

Functions:

i) Translation → for example ASCII to EBCDIC

ii) Encryption/Decryption → Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data known as plain text. A key value is used for encrypting as well as decrypting data.

iii) Compression → Reduces no. of bits that need to be transmitted on network.

Scanned by TapScanner

7. Application layer (layer 7):-

This layer is implemented by network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Example:- Applications - Browsers, Skype, Messenger etc.

Application layer is also called Desktop layer.

Functions:

→ Network Virtual Terminal
→ FTAM - File transfer access and management.
→ Mail Services
→ Directory Services.

⊛. TCP/IP Model and its comparision with OSI:

The OSI model was designed to describe functions of communication systems. But TCP/IP model was designed and developed by Department of Defence (DoD) in 1960s and is based on standard protocals. It stands for Transmission Control Protocal/Internet Protocal. It contains following four layers:-

1. Network Access Layer:- This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocals present in this layer allows for the physical transmission of data.

2. Internet layer:- This layer corresponds to the functions of Network layer of OSI Model. It defines the protocals which are responsible for logical transmission of data, over the entire network. The main protocals residing at this layer are:

- IP → IP stands for Internet Protocal and is responsible for delivering packets. It has two versions IPv4 and IPv6.

Scanned by TapScanner

- ICMP → It stands for Internet Control Message Protocal. It is responsible for providing hosts with information about network problems.
- ARP → It stands for Address Resolution Protocal. It's job is to find the hardware address of a host from a known IP address.

3. Host-to-Host Layer: This layer corresponds to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. The two main protocals present in this layer are:-

- Transmission Control Protocal (TCP) → It provides reliable and error-free communication between end systems. It also performs sequencing and segmentation of data. It is very effective protocal but lot of overheads leads to increase it's cost.
- User Datagram Protocal (UDP) → It is good protocal if your application does not require reliable transport as it is very cost-effective. TCP is connection-oriented protocal but UDP is connectionless.

4. Process layer:-

This layer performs functions of Application, Presentation and Session layer. It is responsible for node-to-node communication and controls user-interface specifications. Following are some of the protocals present on this layer:

- HTTP and HTTPS → HTTP stands for Hypertext transfer protocal. It is used by world wide web (www) to manage communication between web browsers and servers. HTTPS stands for HTTP-Secure. It is combination of HTTP with SSL (Secure Socket Layer).
- SSH → SSH stands for Secure Socket layer. It is a terminal emulation software and is more preferred because of its ability to maintain the encrypted connection. It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.

Scanned by TapScanner

• NTP → NTP stands for Network Time Protocal. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions.

TCP/IP Comparision with OSI

TCP/IP	OSI
i) TCP refers to Transmission Control Protocal.	i) OSI refers to Open Systems Interconnection.
ii) TCP/IP has 4 layers.	ii) OSI has 7 layers.
iii) TCP/IP is more reliable.	iii) OSI is less reliable.
iv) TCP/IP does not have very strict boundries.	iv) OSI has strict boundries.
v) TCP/IP follow a horizontal path.	v) OSI follows vertical path.
vi) TCP/IP uses both session and presentation layer in application layer itself.	vi) OSI uses different session and presentation layers.
vii) TCP/IP developed protocals then model.	vii) OSI developed model then protocal.

Scanned by TapScanner

⊛. Connection-less and Connection-Oriented Network Services:-

Both connection-less and connection oriented service are used for the connection establishment between two or more than two devices. These type of services are offered by network layer.

Connection-oriented service is related to the telephone system. It includes the connection establishment and connection termination. In this ~~method~~ service, handshake method is used to establish the connection between sender and receiver. This connection is preferred by long and steady communication.

Connection-less service is related to the postal system. It does not include any connection establishment and connection termination. This service does not give the guarantee of reliability. In this service, packets do not follow same path, to reach destination. Thus connection is preferred by bursty communication.

⊛. Basic Concept of Internet and ISP's:

Internet → Internet is the largest computer network in the world, connecting ~~more~~ billions of computer users. ~~The~~ Internet is ~~used~~ most often used for three main purposes:

→ Communication
→ Buying and selling (e-commerce).
→ Searching for information.

Internet is a self-publishing medium which means that no one is in charge of the content found on it. ~~Ayy~~ Anyone can publish anything on the internet, wheather the information is true or not.

ISPs → An Internet Service Provider (ISP) is a company that provides customers with internet access. ISPs use fiber-optics, satellite, copper wire and other forms to provide internet access to it's customers. To connect to an ISP, we need a modem and an active account. The ISP verifies our account and assigns our modem an IP address. Once, we have IP address we are connected to internet. We can use a router to connect multiple devices to the internet.

Scanned by TapScanner

ISPs act as hubs on the internet since they are often connected directly to the internet backbone. Because of the large amount of traffic ISPs ~~handle~~ require high bandwidth connections to the internet. In order to offer faster speed to customers, ISPs must add more bandwidth to their backbone connection.

⊛ Backbone Networks: Backbone network is a network containing a high capacity connectivity infrastructure to different part of the network.

i) Bus Backbone:- In Bus backbone the topology used for the backbone is bus topology.

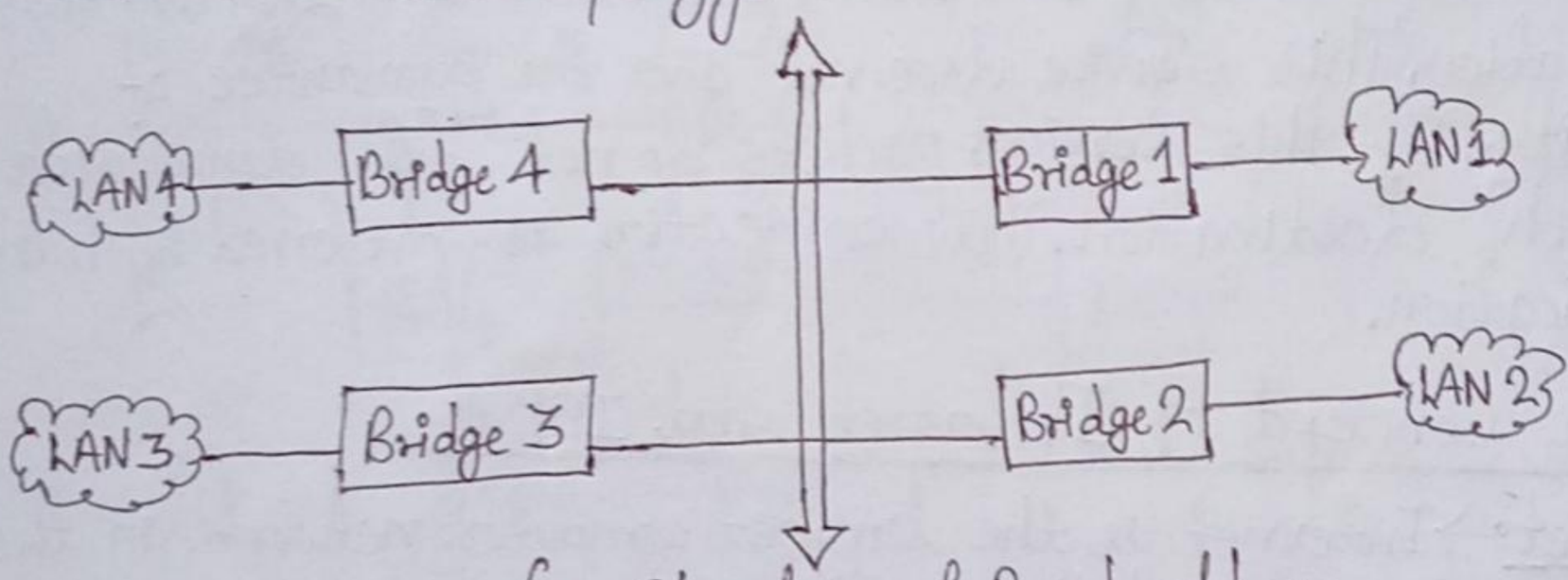


fig. Structure of Bus backbone.

The above Bus Backbone is a bridge based (bridge is the connecting device) backbone with four LANs. This type of backbone are basically used for connecting different buildings in an organization.

ii) Star Backbone:- The topology of this backbone is star topology.

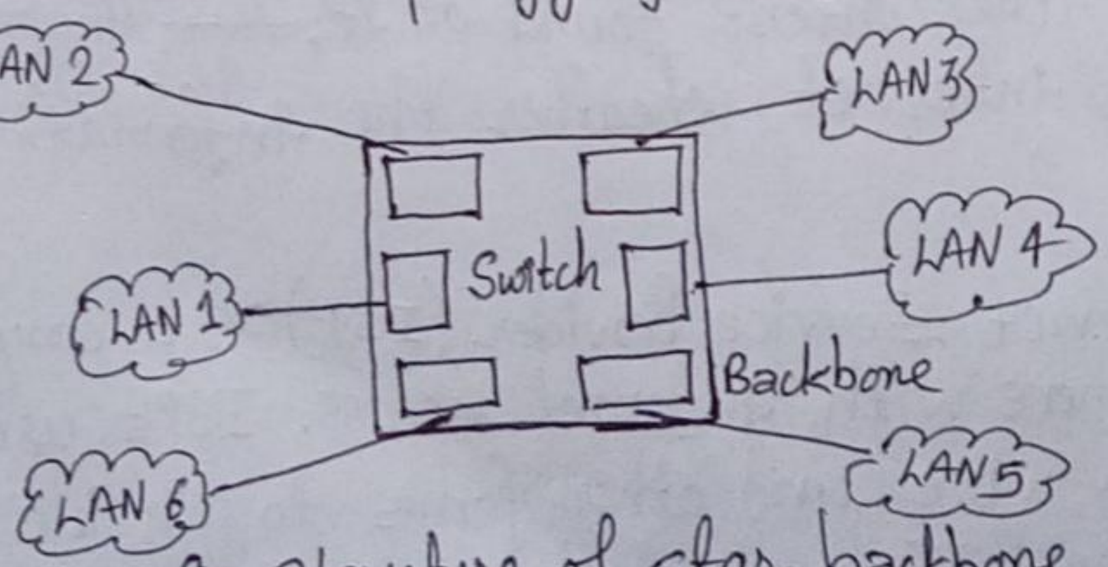


fig. Structure of star backbone

In above figure the switch does the job of backbone and connect the LANs. This type of backbone are basically used as distribution backbone inside a building.

Scanned by TapScanner

⊛ Connecting remote LANs :-

Connecting remote LANs is one of the common application for a backbone network. This type of backbone network is useful when a company has several offices with LANs and needs to connect them. The connection can be done through bridges, sometimes called remote bridges. The bridges act as connecting devices connecting LANs and ~~point-point~~ point-to-point networks such as leased telephone lines or ADSL lines. The following figure shows a backbone connecting remote LANs.

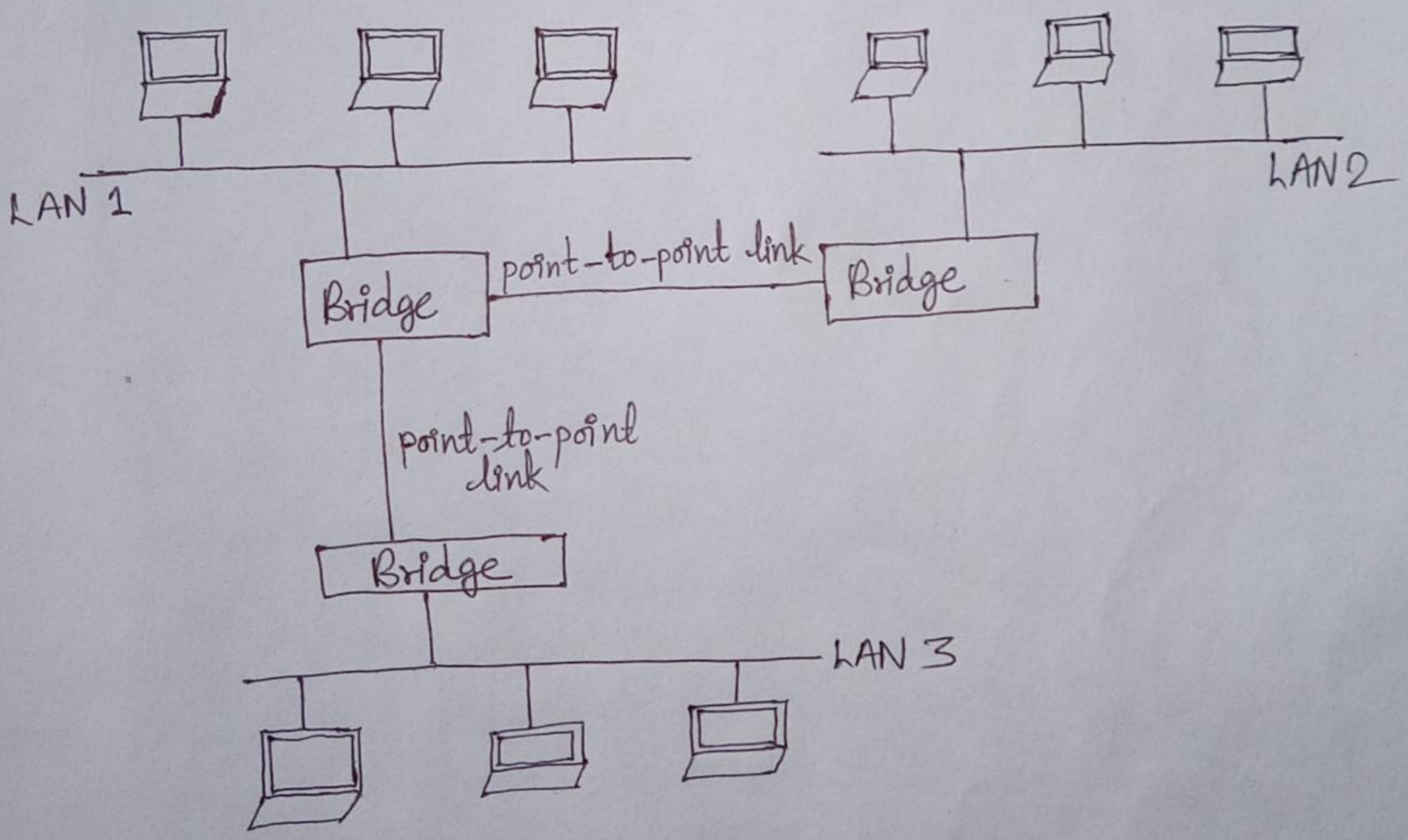


fig. Backbone connecting remote LANs.

Scanned by TapScanner