

UNIT- 2: Introduction to Networking and Topologies

2.1 Overview of Networking:

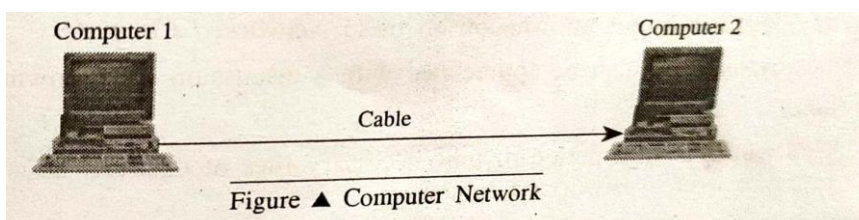
- A **computer network** is an interconnection of various computers to share software, hardware, resources and data through a communication medium between them.

2.2 Need for Networking:

- **Sharing of hardware:** For example, several PCs might be networked together in a wired or wireless local area network (LAN) to share a printer.
- **Sharing of information:** Distributed databases, e-mail, the World Wide Web and so on are examples of this. Here the sharing involves both LANs and wide area networks (WANs).

Needs of networking are:

- **Speed:** Networks provides a very rapid method for sharing and transferring files.
- **File sharing:** a network makes it easy for everyone to access the same file and prevents people from accidentally creating different versions.
- **Printer sharing:** with a network several computers can share the same printer.
- **Communication and collaboration:** A network allows employees to share files, view other peoples work and exchange ideas more efficiently. you can use email and instant messaging tools to communicate quickly and store messages for future use.
- **Remote Access:** users are able to access the same files, data and messages even they are not in the office.
- **Data Backup:** a network makes it easier to back up all of your company's data on an offsite server, a set of tapes, CDs or other backup systems.
- **Data security:** only the authorized users can access data.
- **Cost:** sharing on a network allows for easier upgrading of the programs when compared to buying individually licensed copies
- **2.3 Hardware and Software components:**
 - Network consist of both hardware and software components helps in connecting the computers across small and large locations.



Hardware components:

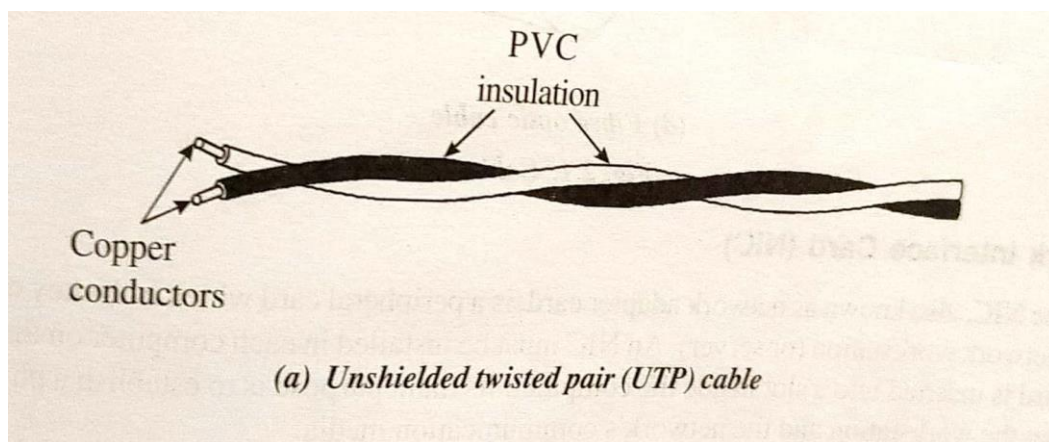
1) Cables.

2) Network Interface Card.

1. Cables.

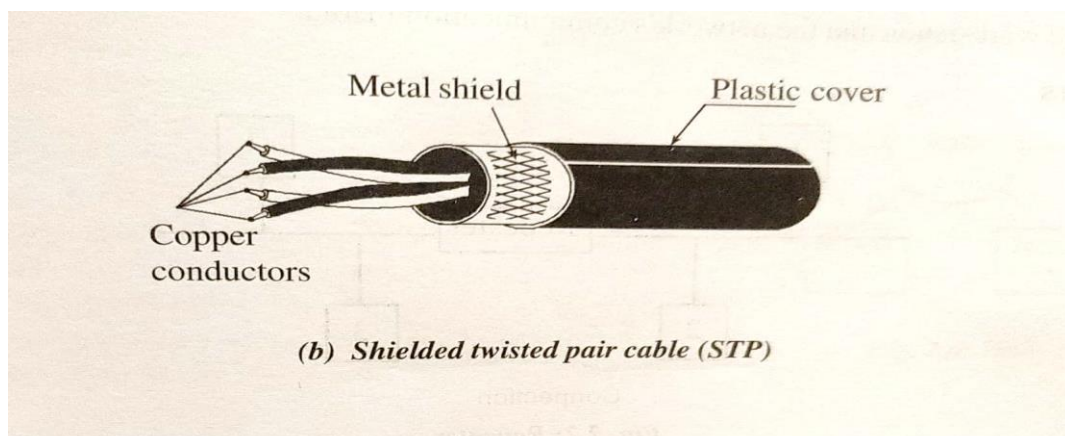
➤ Unshielded twisted pair(UTP) cable:

1. It is the cable used for telephone system.
2. It is used to connect terminals and low speed data equipment to the mainframe.
3. It is frequently pre-installed in buildings.



➤ Shielded twisted pair cable(STP):

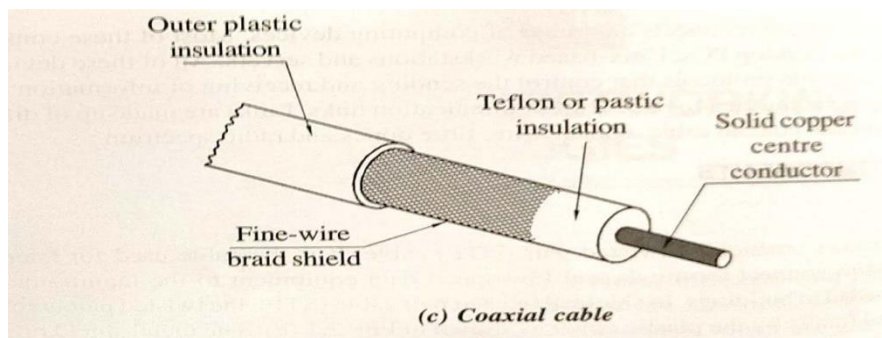
1. First it is covered by metal shield and finally by the plastic cover.
2. The metal shield avoids crosswalks.



➤ Coaxial Cable:

1. It consists of a centre copper conductor surrounded by insulation. And also surrounded by a tube shaped conductor of solid copper or solid aluminium.

2. An outer plastic jacket protects and insulates the wire.



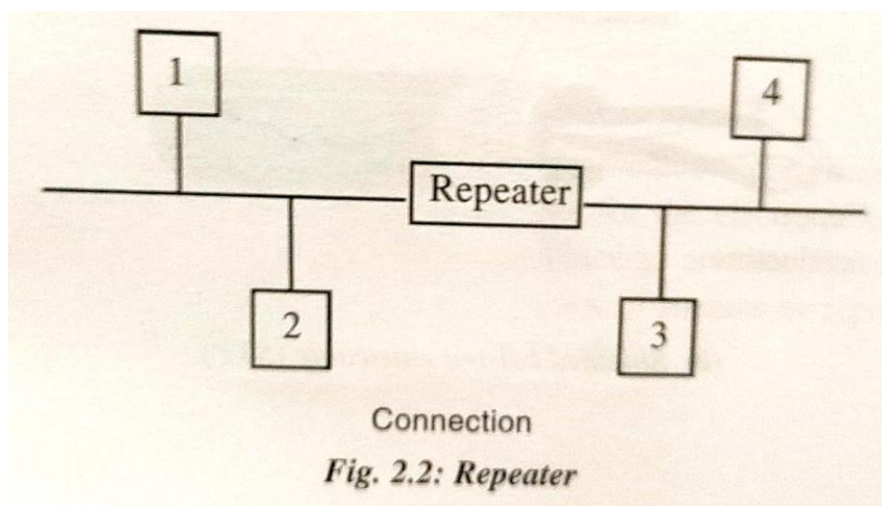
Network Interface Card(NIC)

Its main purpose is to establish a physical link between the workstation and the network's communication media.

➤ Repeaters:

1. It is a device used to **amplify** the incoming signals to be transmitted to the destination computer.
2. Repeaters are required when the **computers are far away from each other**.
3. In such cases signal being transmitted **goes weak**(attenuation or distortion) and does not reach the destination computer successfully.
4. **Advantage of repeater:** Amplifies the incoming signal

(strengthens the signal) and transmits amplified signal to the destination.



➤ Bridges:

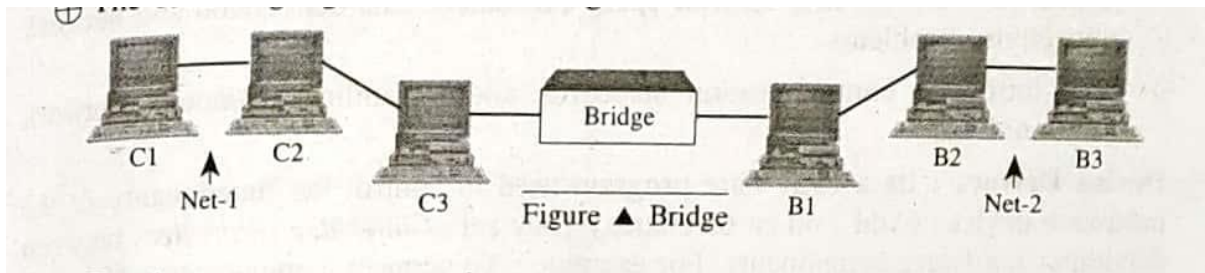
1. A bridge is a device that connects with in a same network.
2. Different types of bridges are,

Local bridge,

Remote bridge,

Transparent bridge etc.

3. Bridges are also used to **divide a large network** into **smaller broad cast domains** that intern **reduce the network traffic** and improve the efficiency of the network.



➤ **Gateways:**

1. A gateway is a device that connects two dissimilar networks.
2. It translates communication protocols and establish link for transmission across different network say LAN , WAN and MAN.

Software Components

The following software components are used in networking:

1. Protocols,
2. Device Drivers.
3. **Protocols:**

“ The protocols are set of rules for successful communication between computers”.

- It helps in solving the problems like data collision, network traffic, transmission error, data transfer speed mismatch etc.

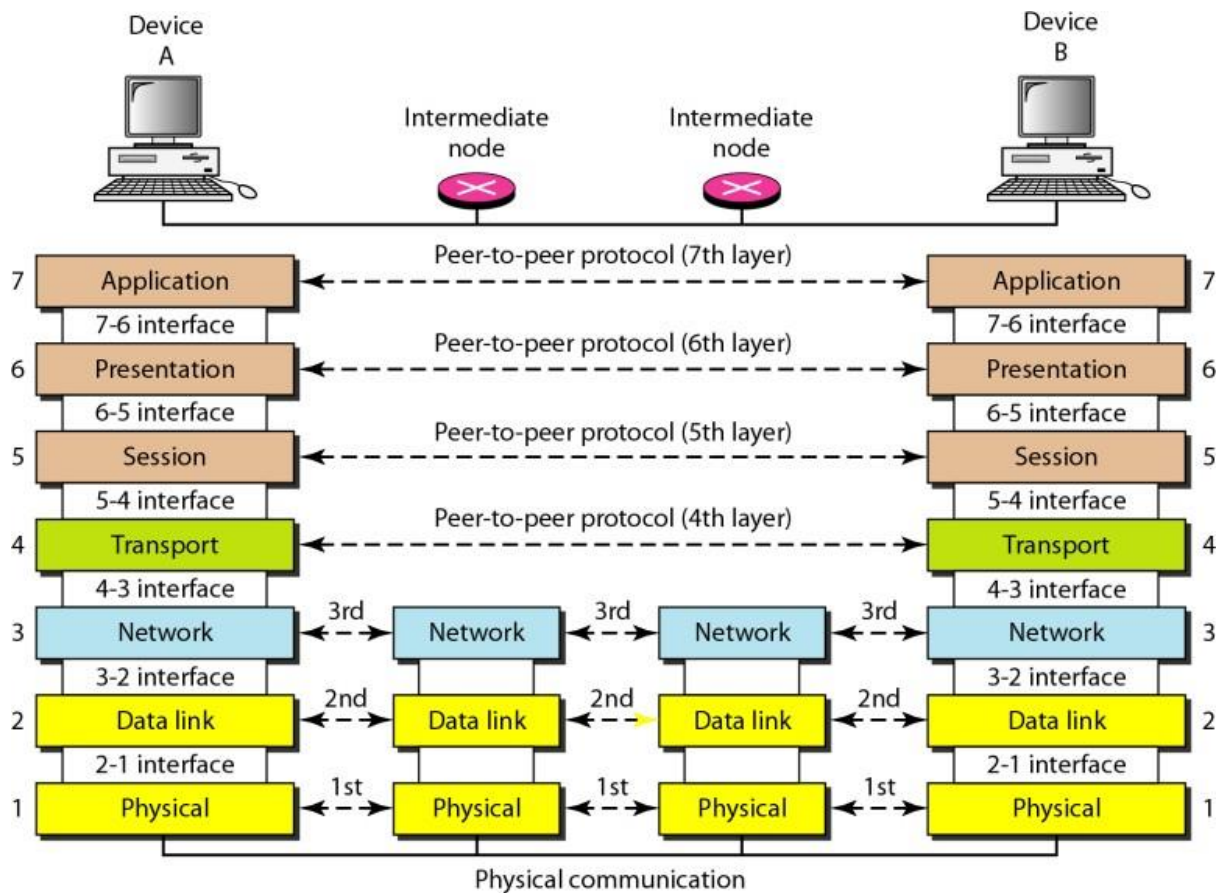
2. **Device Drivers:**

- It's a firm ware program used to control the functionality of the hardware devices.
- They act as interface controllers between dissimilar hardware components.
- Eg: To connect computer to a network. (NIC Card and NIC driver software are used).

2.4: The OSI Model

- OSI is a model which covers all aspects of network communications.

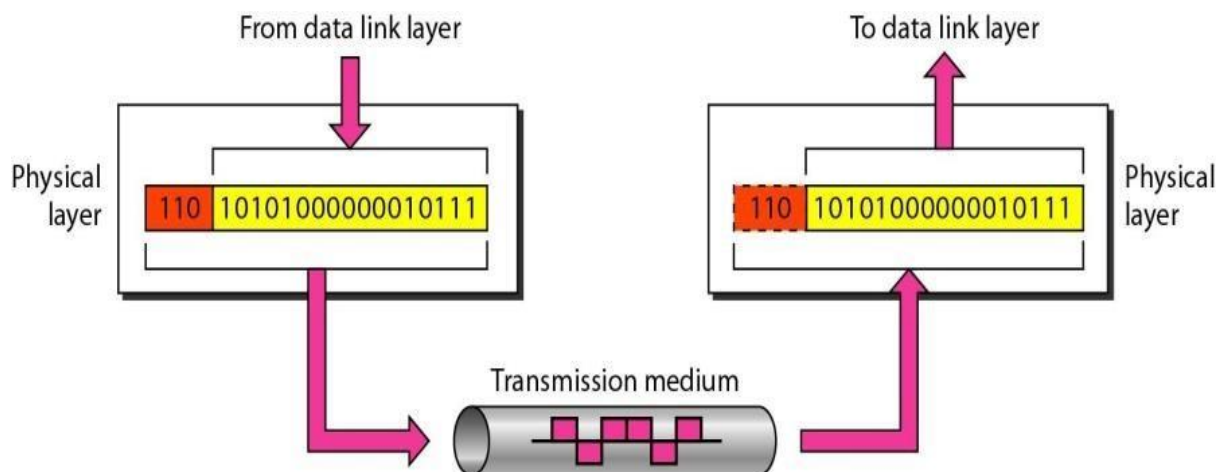
- The OSI Reference Model is developed by International Standards of Organization (ISO).



LAYERS IN THE OSI MODEL:

1. Physical Layer:

“Physical layer is responsible for **movement of individual bits from one node to another node.**”



The physical layer is also concerned with the following:

1. Physical characteristics of interfaces and medium:

- The physical layer defines the characteristics of the interface between the devices and the transmission medium.
- It also defines the type of transmission medium.

2.Representation of bits:

- The physical layer data consists of a **stream of bits** (sequence of 0s or 1s).
- To transmit stream of bits, we must **encode bits into signals** (electrical or light (optical)).

3.Data rate:

- It defines **transmission rate**, i.e., **the number of bits sent each second**.

4.Synchronization of bits:

- The sender and receiver must send and receive the data **at a same time**.

5.Line configuration:

- The physical layer is concerned with the connection of **devices to the media**. i.e. **a point-to-point configuration or a multipoint configuration**.

6.Physical topology:

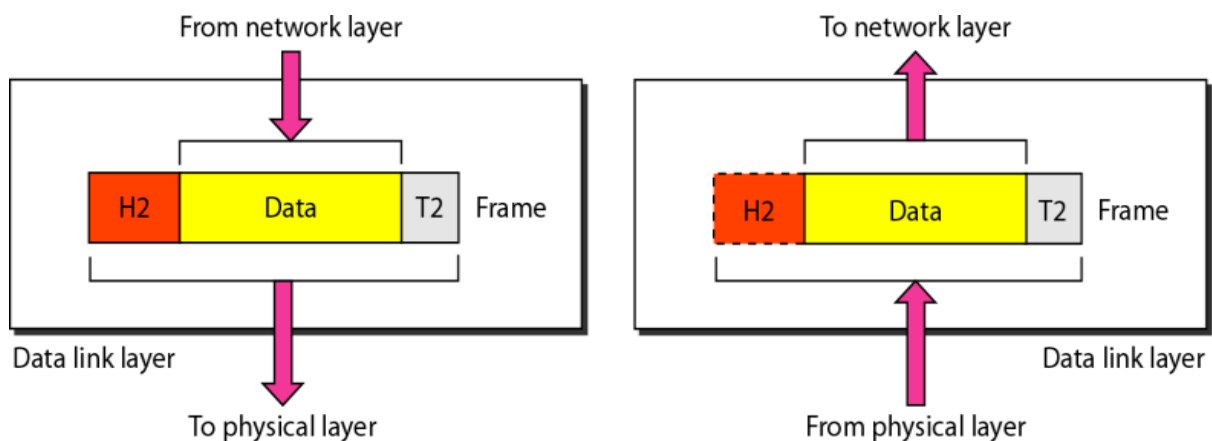
- Devices can be connected by using a **mesh topology**, a **star topology**, a **ring topology**, a **bus topology**, or a **hybrid topology**.

7.Transmission mode:

- The physical layer also defines the mode of transmission between two devices: simplex, half-duplex, or full-duplex.

• 2.Data Link Layer:

- “The data link layer is responsible for **moving frames from one node to the next**.”



Data link Layer

Responsibilities of the data link layer include the following:

1.Framing:

- The data received from network layer is divided into **number of frames**.

2.Physical addressing:

- It adds the **header to the frames**.

3.Flow control:

- It controls the **flow of data**.

4.Error control:

- It controls the error while **transforming the data**. The data transmission should be **error free**.

5.Access control:

- When two or more devices are connected to the **same link**, data link layer protocols are necessary **to determine which device has control over the link at any given time**.

3. Network Layer:

- The network layer is responsible for the delivery of individual packets from the source host to the destination host.
- The network layer ensures that each packet gets from its point of origin to its final destination.
- Figure 2.8 shows the relationship of the network layer to the data link and transport layers.

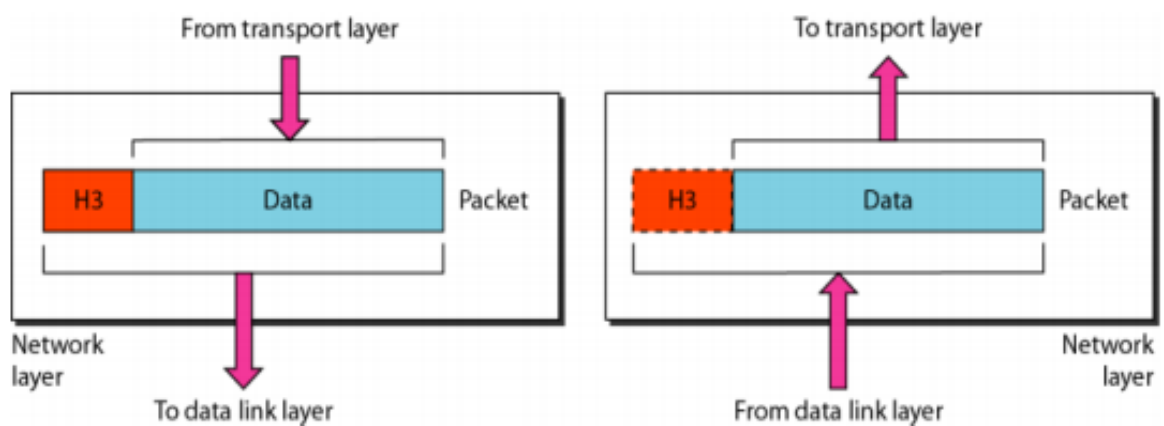


Figure 2.8 Network layer

Other responsibilities of the network layer include the following:

1. Logical addressing:

- The network layer adds a header to the packet coming from the upper layer, includes the logical addresses of the sender and receiver.

2. Routing:

- When independent networks or links are connected to create internetworks or a large network.
- The connecting devices (called routers or switches) route or switch the packets to their final destination.
- One of the functions of the network layer is to provide this mechanism.

4. Transport Layer:

- The transport layer is responsible for the delivery of a message from one process to another.

“ A process is an application program running on a host.”

- The transport layer ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.
- Figure 2.10 shows the relationship of the transport layer to the network and session layers.

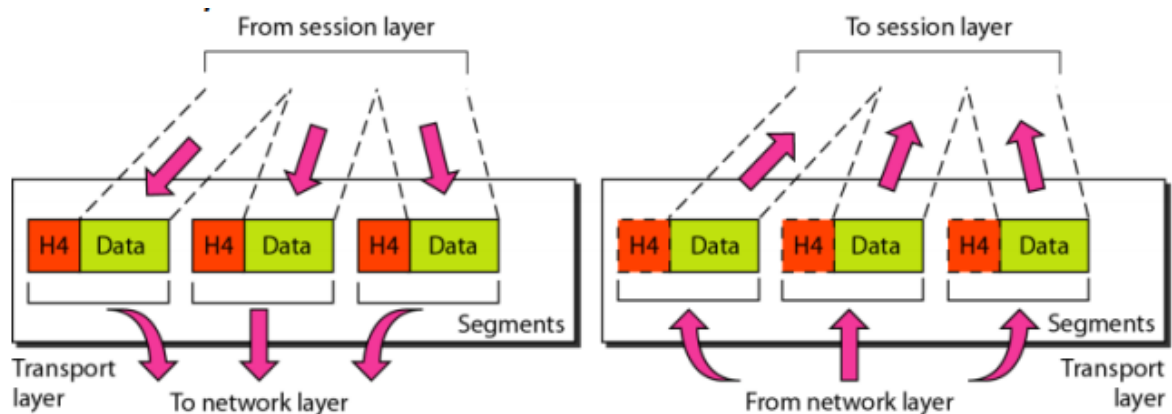


Figure 2.10 Transport layer

Other responsibilities of the transport layer include the following:

1. **Service-point addressing:** The transport layer header must therefore include a type of address called a **service-point address** (or port address).
- The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

2. **Segmentation and reassembly:** A message is divided into transmittable segments, with each segment containing a **sequence number**.
 - These numbers enable the transport layer to **reassemble the message** correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
3. **Connection control:** The transport layer can be either connectionless or connection oriented.
 - A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.
 - A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
4. **Flow control:** Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
5. **Error control:** Like the data link layer, the transport layer is responsible for error control.
 - The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication).
 - Error correction is usually achieved through retransmission.

5. Session Layer: The session layer is responsible for dialog control and synchronization.

- The session layer is the network dialog controller.
- It establishes, maintains, and synchronizes the interaction among communicating systems.

Specific responsibilities of the session layer include the following:

1. **Dialog control:** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex or full-duplex mode.
2. **Synchronization:** The session layer allows a process to add checkpoints, or synchronization points, to a stream of data.
 - **For example,** if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently.

- In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.
- Figure 2.12 illustrates the relationship of the session layer to the transport and presentation layers.

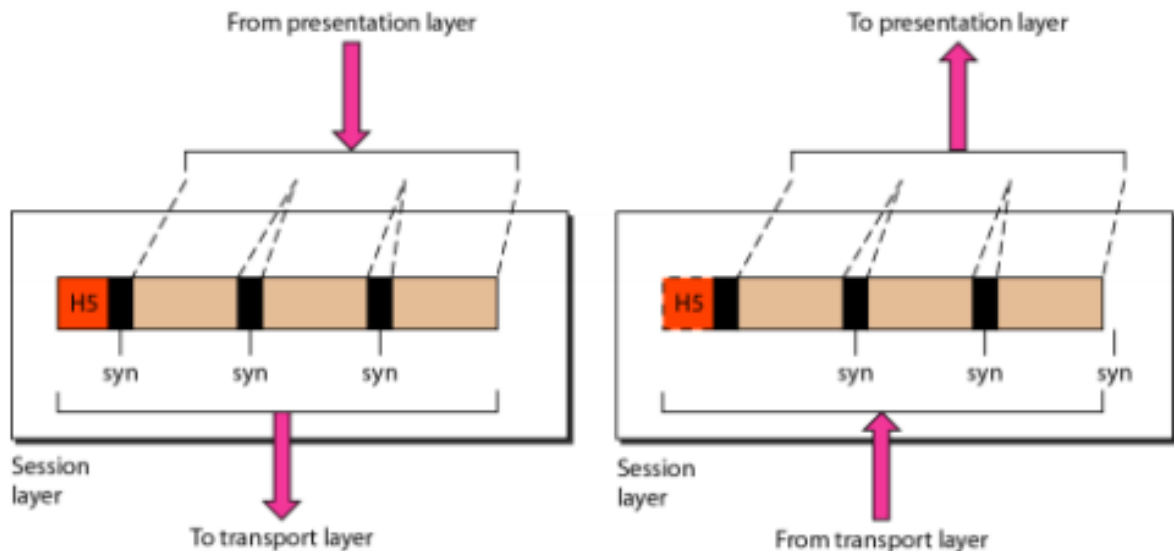


Figure 2.12 Session layer

6. Presentation Layer:

- The presentation layer is responsible for translation, compression, and encryption.
- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.
- Figure 2.13 shows the relationship between the presentation layer and the application and session layers.

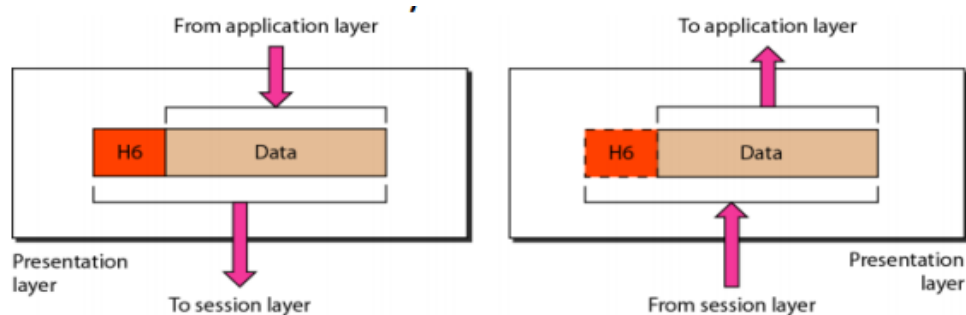


Figure 2.13 Presentation layer

Specific responsibilities of the presentation layer include the following:

1. **Translation:** The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
2. **Encryption:** To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
3. **Compression:** Data compression reduces the number of bits contained in the information.

7. Application Layer:

- The application layer is responsible for providing services to the user.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
- Figure 2.14 shows the relationship of the application layer to the user and the presentation layer.

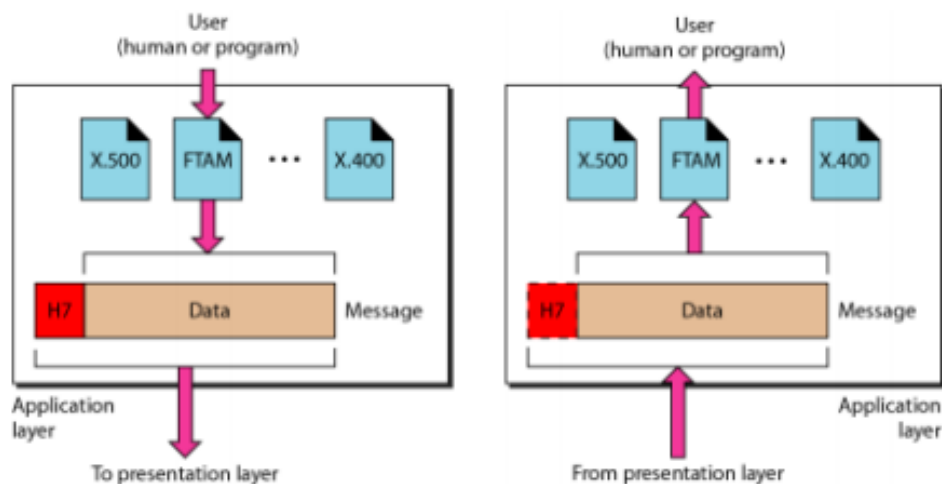


Figure 2.14 Application layer

Specific services provided by the application layer include the following:

1. **Mail services:** This application provides the basis for e-mail forwarding and storage.
2. **Directory services:** This application provides distributed database sources and access for global information about various objects and services.

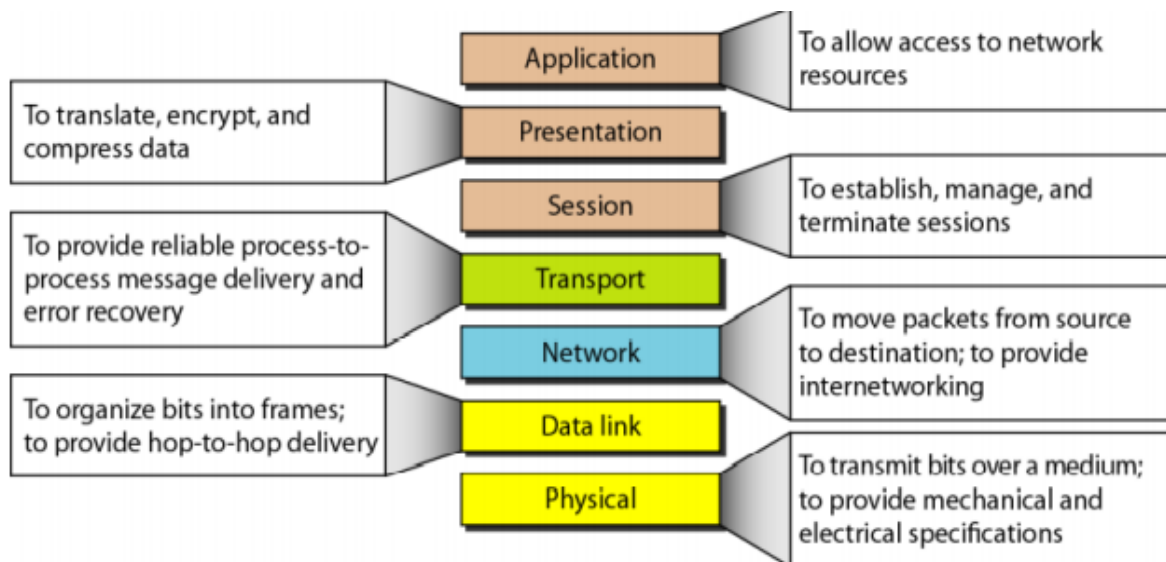


Figure 2.15 Summary of layers

2.6 TCP/IP PROTOCOL SUITE /INTERNET MODEL:

TCP/IP model is used in internet. It is also known as protocol-suits. This model defines internet model, which contain **5 layers**.

They are,

1. Application layer
2. Transport layer
3. Internet layer
4. Host to network layer

1.Host to network layer:

- It has to connect to the network using some protocol, so that host can send the packets to network layer.
- In this layer the protocols are Ethernet and token ring.
- This layer also contains different devices that are attached to network.

2.Internet layer:

- This layer makes the host to insert packets into network by using IP protocols.
- This layer also responsible for routing of packets, congestion control, packet formatting.

3.Transport layer:

- The function of this layer is same as transport layer in OSI reference model.

- The end-to-end protocols used in this layer are **TCP(Transmission control protocol)**, **UDP(User datagram protocol)**.
- **TCP** is reliable and connection oriented protocol. It allows stream of bites to transform from one machine to another without any error.
- It is responsible for flow control.
- **UDP** is unreliable and connectionless protocol and this protocol is used for the application which do not want the sequencing and flow control.

4.Application layer:

- All high-level protocols are defined in this layer to perform different operations.
- The protocols are,
 - **TELNET**(Virtual terminal)
 - **FTP**(File transfer protocol)
 - **SMTP**(Simple mail transfer protocol).

Network Topologies:

There are **five basic topologies** in network, they are,

1. **Bus topology**
2. **Star topology**
3. **Ring topology**
4. **Mesh topology**
5. **Hybrid topology**

1.Bus topology:

- A bus topology is multipoint. One long cable acts as a backbone to link all the devices in a network (see Figure 1.7).
- When one computer sends a message, all computer on the network receive the information, but one with the address that matches the one encoded in the message accepts the information while all others reject the message.
- Speed is slow because only one computer can send a message at a time. A computer must wait until the bus is free before it can transmit.
- Requires a proper termination at both the ends of the cable.
- Bus topology was the one of the first topologies used in the design of early local area networks. Ethernet LANs can use a bus topology, but they are less popular now.

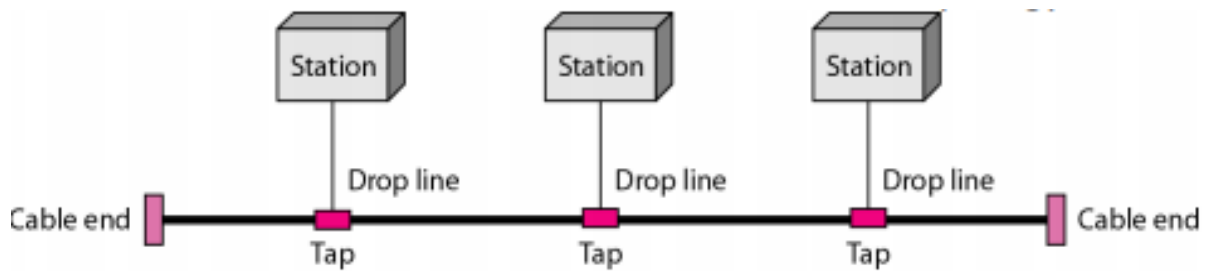


Figure 1.7 A bus topology connecting three stations

Advantages:

1. Easy to understand, install and use for small networks.
2. Cabling cost is less because a bus uses less cabling than mesh or star topologies.
3. Easy to expand by joining 2 cables with connector.

Disadvantages:

1. Difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.
2. Signal reflection at the taps can cause degradation in quality.
3. Adding new devices may therefore require modification or replacement of the backbone.
4. A fault or break in the bus cable stops all transmission.
5. Requires a proper termination at both the ends of the backbone cable.

2. Star topology:

- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another.
- A star topology does not allow direct traffic between devices.
- The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device (see Figure 1.6).

Star Topology

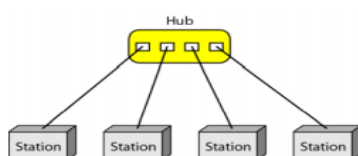


Figure 1.6 A star topology connecting four stations

- The star topology is used in local-area networks (LANs). High-speed LANs often use a star topology with a central hub.
- **Advantages :**
- 1.A star topology is less expensive than a mesh topology.
- 2. Easy to install and reconfigure. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.
- 3. Star topology is robust. If one link fails, only that link is affected. All other links remain active.
- 4. Fault identification and fault isolation is easy.
- **Disadvantage:**
- 1.Disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
- 2. Cabling cost is more.
- 3. The cost of the hub makes the network expensive as compared to bus and ring topology.

3.Ring topology:

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along (see Figure 1.8).

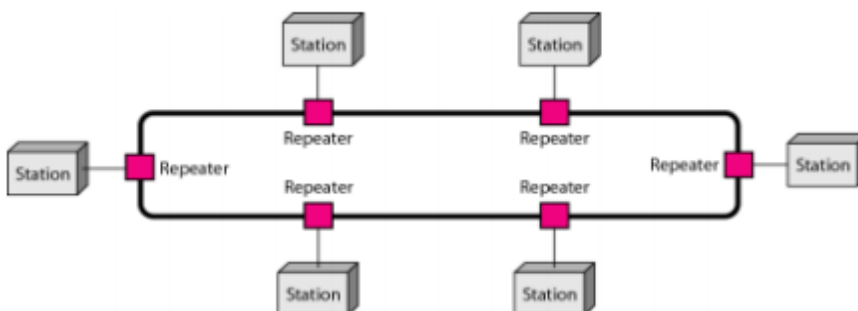


Figure 1.8 A ring topology connecting six stations

Advantages:

1. A ring topology is easy to install and reconfigure.
2. Fault isolation is simplified.
3. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

Disadvantages:

1. Unidirectional traffic can be a disadvantage. Failure in any cable or node on the ring can affect the whole network. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network.
2. It is difficult to troubleshoot the ring.
3. Adding or removing the computers disturbs the network activity.

5. Mesh topology:

- In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.
- In a mesh topology, we need $n(n-1)/2$ duplex-mode links.
- Ex: the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

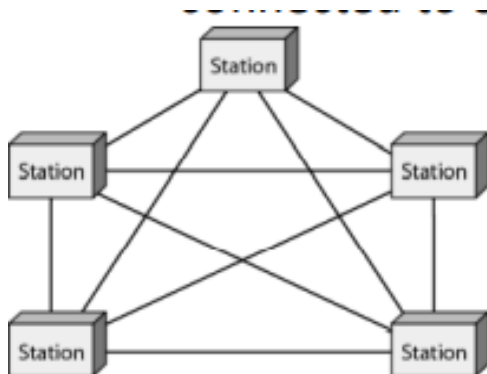


Figure 1.5 A fully connected mesh topology (five devices)

Advantages:

1. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems.

2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
3. There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.
4. Point-to-point links make fault identification and fault isolation easy.

Disadvantages:

1. Disadvantage of a mesh are related to the amount of cabling and the number of I/O ports required.
2. Installation and reconnection are difficult, because every device must be connected to every other device.
3. The bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
4. The hardware required to connect each link (I/O ports and cable) can be expensive.

6. Hybrid topology:

- Hybrid Topology A network can be hybrid.
- For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure 1.9.

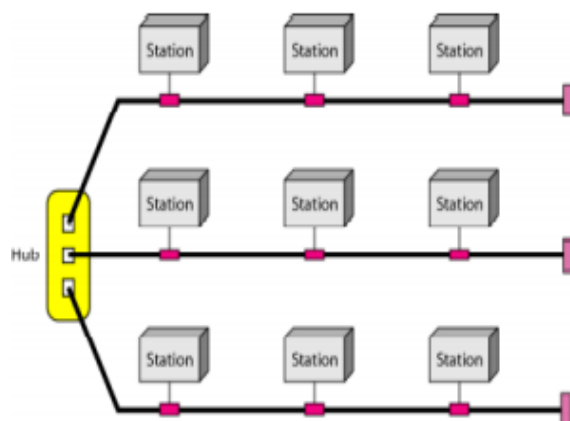


Figure 1.9 A hybrid topology: a star backbone with three bus networks