2.1 Introduction to OSI model with all layers

OSI Model

- OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model:

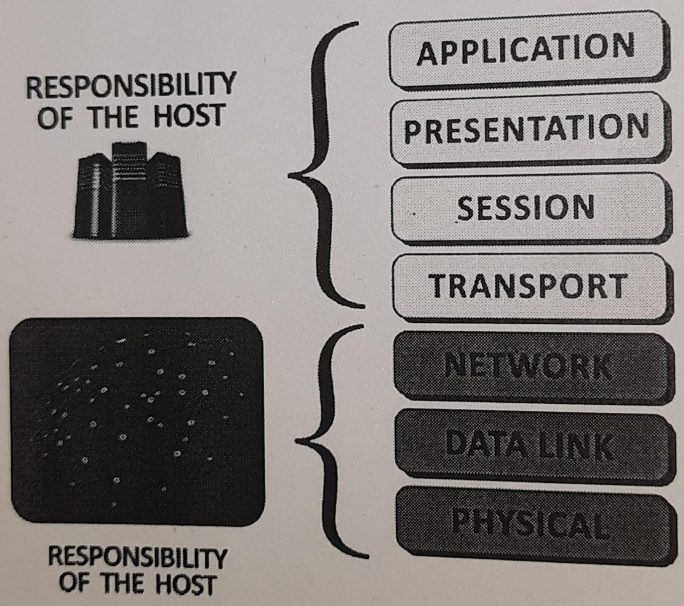


Figure 2.1

- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

Functions of the OSI Layers

There are the seven OSI layers. Each layer has different functions. Lists of seven layers are given below:

1) Physical Layer
2) Data-Link Layer
3) Network Layer
4) Transport Layer
5) Session Layer
5) Session Layer
6) Presentation Layer
7) Application Layer

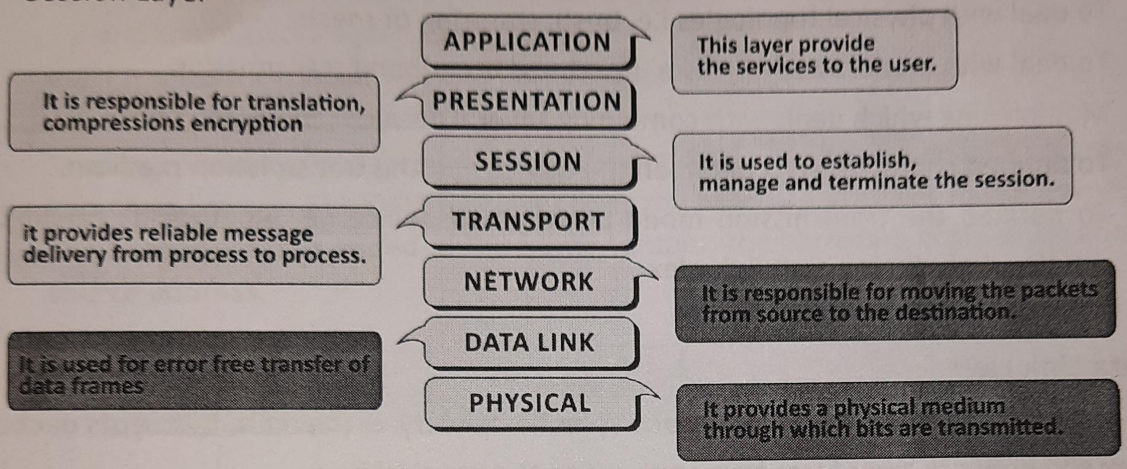


Figure 2.2

Physical layer :-

1. The physical layer responsible for sending bits from one computer to another .
2. The physical layer is not concerned with the meaning of the bits but it deals with physical connection to the network and with transmission and reception of signals.
3. The physical level is used to defined physical and electrical such as what will represent a 1 or a 0 how many pins network will have, how data will be synchronized and when the network adapter may or may not transmit the data.
4. The position of the physical layer with respect to transmission medium and the data link layer

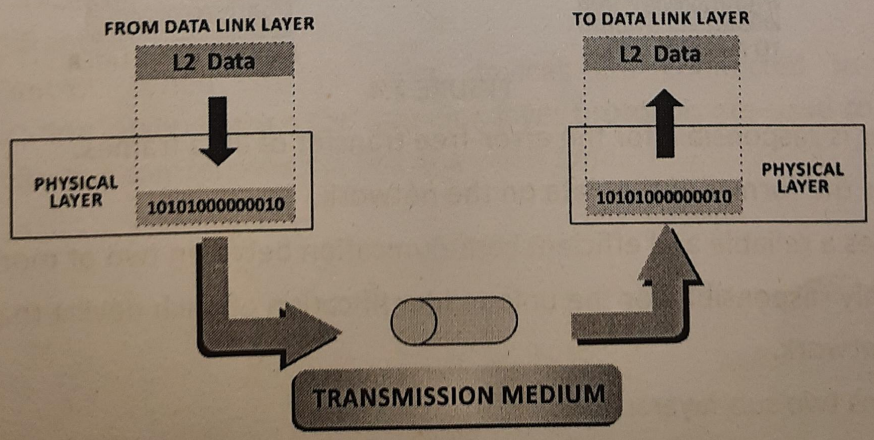


FIGURE 2.3

Following are the function of the physical layer:-

1. To defined the typed of encoding i.e. how 0`s and 1`s are changed to signals.
2. To defined the transmission rate i.e. the number of bits transmitted per second.
3. To deal with the synchronization of the transmitter and receiver.
4. To deal with network connection types, including multipoint and point to point connection.
5. To deal with physical topologies i.e. bush, star, ring or mesh.
6. To deal with media bandwidth i.e. baseband broadband transmission .
7. Multiplexing which deals with combining several data channels into one.
8. To defined characteristics between the device and the transmission medium.
9. To defined the transmission mode between to device i.e. whether it should be simplex, half duplex or full duplex.

Data Link Layer :-

It is responsible for reliable node to node delivery of the data. It accepts packets from the network layer form frames give it to the physical layer.

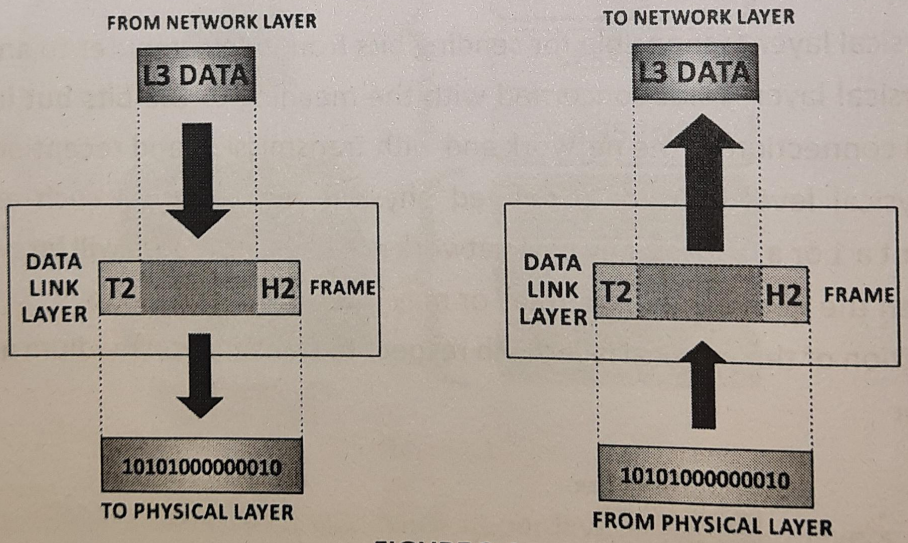


FIGURE 2.4

- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:

Logical Link Control Layer

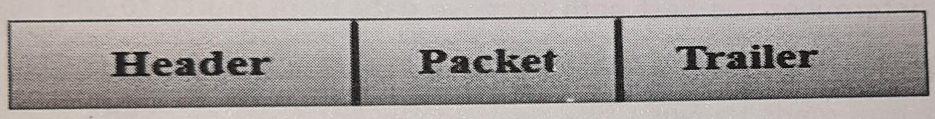
- It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
- It identifies the address of the network layer protocol from the header.
- It also provides flow control.

Media Access Control Layer

- A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
- It is used for transferring the packets over the network.

Functions of the Data-link layer

- Framing: The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.



- Physical Addressing: The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- Flow Control: Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- Error Control: Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- Access Control: When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

Network Layer

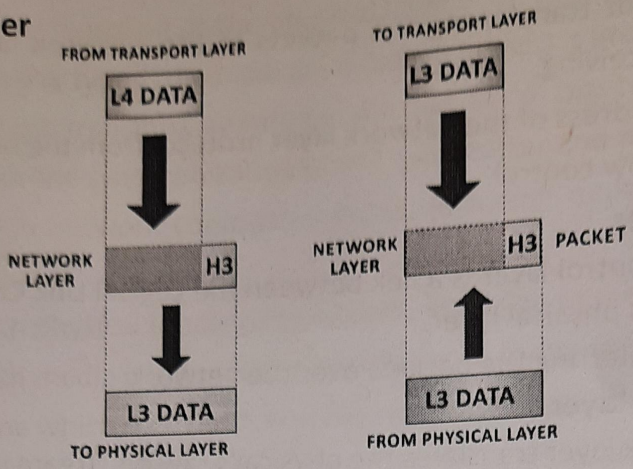


FIGURE 2.5

- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

Transport Layer:

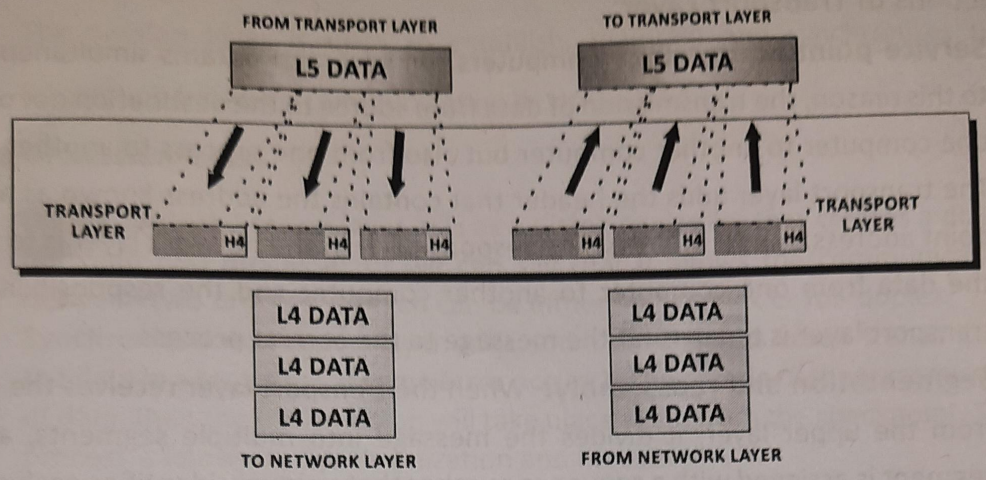


FIGURE 2.6

- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.

- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

- **Transmission Control Protocol**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.
  - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

Session Layer:

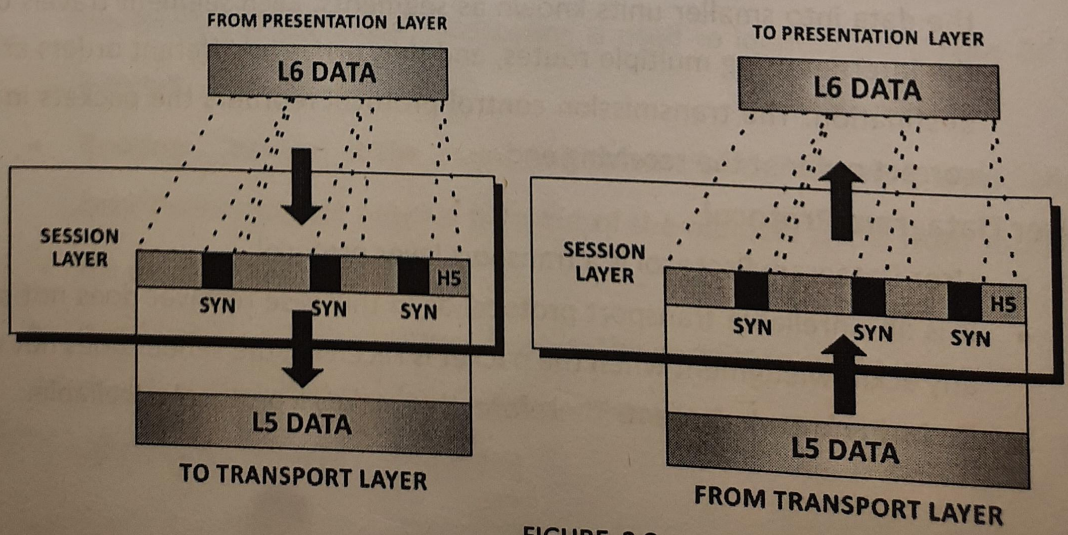


FIGURE 2.8

- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

Presentation Layer

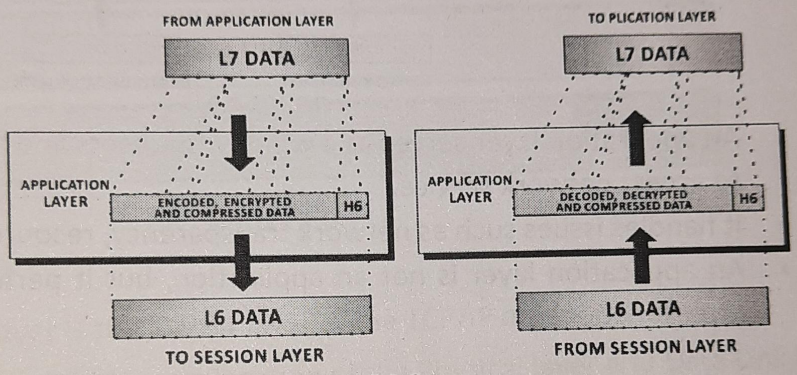


FIGURE 2.8

- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

- Translation: The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.

- Encryption: Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- Compression: Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

Application Layer

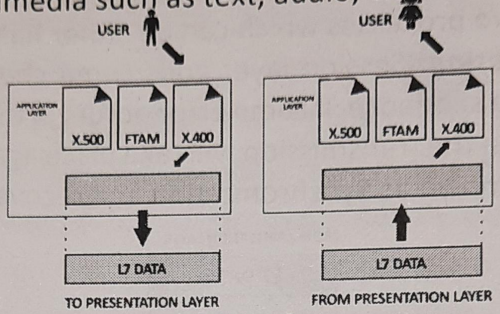


FIGURE 2.9

- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

Functions of Application layer:

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- **Directory services:** An application provides the distributed database sources and is used to provide that global information about various objects.

CP/IP model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:

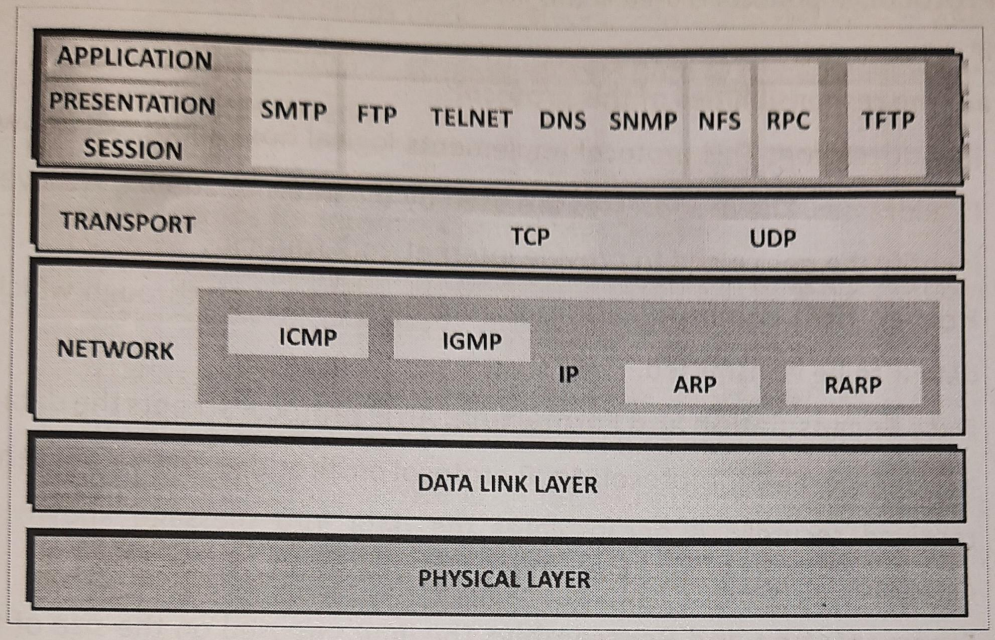


FIGURE 2.10

Network Access Layer

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

Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

- ARP stands for Address Resolution Protocol.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- The two terms are mainly associated with the ARP Protocol:
  - ARP request: When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.

- ARP reply: Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

- ICMP stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- An ICMP protocol mainly uses two terms:
  - ICMP Test: ICMP Test is used to test whether the destination is reachable or not.
  - ICMP Reply: ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and** Transmission

Control protocol.

- **User Datagram Protocol (UDP)**
  - It provides connectionless service and end-to-end delivery of transmission.

- It is an unreliable protocol as it discovers the errors but not specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
- **UDP consists of the following fields:** Source port address: The source port address is the address of the application program that has created the message.
- **Destination port address:** The destination port address is the address of the application program that receives the message.
- **Total length:** It defines the total number of bytes of the user datagram in bytes.
- **Checksum:** The checksum is a 16-bit field used in error detection.

- UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.

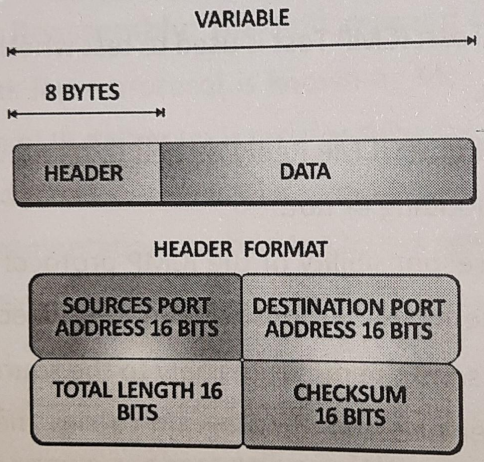


FIGURE 2.11

Transmission Control Protocol (TCP)

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using HTTP protocol to interact with the network where HTTP protocol is an application layer protocol.

Following are the main protocols used in the application layer:

- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

2.2 Differences between OSI Model & TCP/IP model

OSI(Open System Interconnection)	TCP/IP (Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol

10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers

2.3 Data Communication Model, Digital and Analog data and signals (Chapter-1)

bit rate, baud, bandwidth, Nyquist bit rate

Bit rate

Bit rate is defined as the transmission of number of bits per second.

Bit rate is also defined as per second travel number of bits.

Bit rate emphasized on computer efficiency.

The formula of **Bit Rate** is: = baud rate x the number of bit per baud

Bit rate is not used to decide the requirement of bandwidth for transmission of signal.

Baud Rate

Baud rate is defined as the number of signal units per second.

Baud rate is also defined as per second number of changes in signal.

While baud rate emphasized on data transmission.

The formula of Baud Rate is: = bit rate / the number of bit While baud rate is used to decide the requirement of bandwidth for transmission of signal.

Bandwidth

In computer networking, the term bandwidth is refers to as the measure of the capacity of a medium to transmit 'data. A medium that has a high capacity, has high bandwidth, whereas a medium that has limited capacity has low bandwidth. Bandwidth can be best- understood by comparing it to its hose. If half-inch garden hose can carry water from a trickle up two gallons per minute, that hose can be said to have a bandwidth gallons per minute. A four-inch fire hose, however, might have a bandwidth that exceeds 100 gallons per minute.

3.1 INTRODUCTION TO GUIDED TRANSMISSION MEDIA-TWISTED PAIR, COAXIAL CABLE, OPTICAL FIBER

INTRODUCTION TO GUIDED TRANSMISSION MEDIA

Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.

The main functionality of the transmission media is to carry the information in the form of bits through LAN(Local Area Network).

Each type of transmission media has special characteristics that make it suitable for specific type of service. Each media type should be discussed keeping the following factors in the mind:

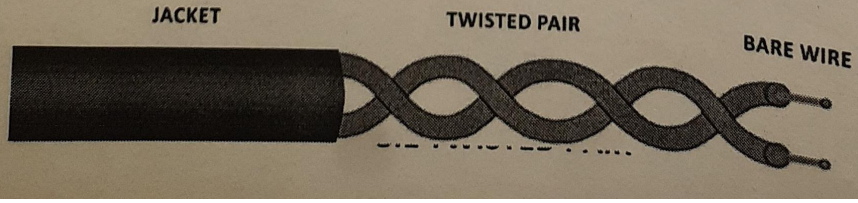
- Cost
- Capacity (bandwidth)
- Ease of installation
- Attenuation
- Immunity from electromagnetic interference (EMI)

TWISTED PAIR

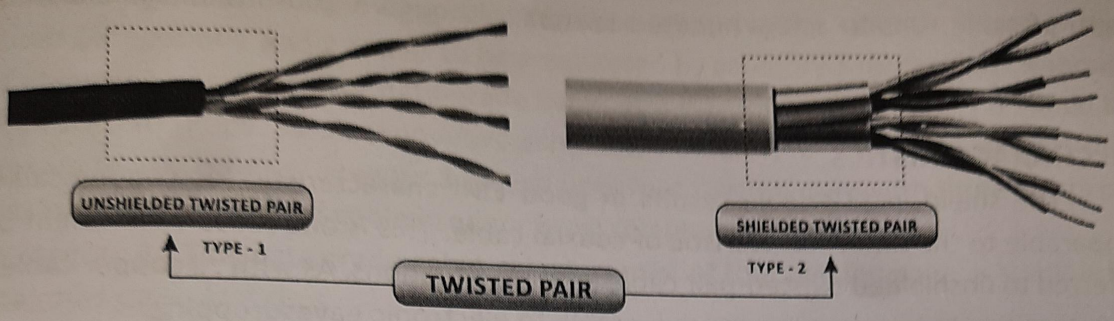
Although the bandwidth characteristics of magnetic tapes are excellent, the delay characteristics are poor. Transmission time is measured in minutes or hours, not milliseconds. For many applications an online connection is needed. The oldest and still most common transmission medium is twisted pair, which employs copper cable. One more reason for popularity of twisted pair is low cost. This type of cable is inexpensive to install and offers the lowest cost per foot of-any cable type.

A basic twisted pair cable consists of two strands of copper wire twisted together, as shown below. This twisting reduces the sensitivity of the cable to EMI and also reduces the tendency of the cable to radiate radio frequency noise that interferes with nearby cables and electronic components. This is because the radiated signals from the twisted wires tens to cancel each other out. Antennas, which are purposely designed to radiate radio frequency signals, consist of parallel, not twisted wires)

Twisting also controls the tendency of the wires in the pair to cause EMI each other. Whenever two wires are in close proximity, the signals in each wire tend to produce noise, called crosstalk, in the other. Twisting the wires in the pair reduces crosstalk in much the same way that twisting reduces the tendency of the wires to radiate EMI.



Two types of twisted-pair cable are used in LANs :



3.2 TWISTED SHIELDED AND UNSHIELDED CABLE

- Shielded twisted Pair
- Unshielded Twisted Pair

SHIELDED TWISTED-PAIR (STP) CABLE:

Shielded twisted-pair cabling consists of one or more twisted pairs of cables enclosed in a foil wrap and woven copper shielding as shown above. Diagram shows IBM type 1 cabling, the first cable type used with IBM token Ring. Early LAN designers used shielded twisted-pair cable because shield further reduces the tendency of the cable to radiate EMI and thus reduces the cable's sensitivity to outside interference.

Co-axial and STP cable used shields for the same purpose. The shield is connected to the ground is a portion of the electronic device to which the cable is connected. A ground is a portion of the device that serves as an electrical reference point. Usually it literally connected to a metal stake driven into the ground. A property grounded shield prevents signals from getting in to or of the cable.

In IBM Type 1 cable include twisted pairs of wire within a single shield Various types of STP cable exist. Some shield each pair individually, and others shield several pairs. The engineers who design a network's cabling system choose the exact configuration. IBM design, and each several twisted pair cable types to use with their Token ring network design, and each cable type is appropriate for a given kind of installation.

STP cables cost more than thin coaxial or unshielded twisted pair cable. STP is less costly, than thick coax or fiber-optic cable.

CAPACITY:

STP cable has a theoretical capacity of 500 Mbps, although few implementations exceed 153 Mbps with 100 meters cable runs. The most common data rate for STP cable is 16 Mbps, which is the top data rate for token Ring networks.

ATTENUATION:

All varieties of twisted-pair cable have attenuation characteristics that limit the length pf cable runs to a few hundred teeters, although a 100-flfteter limit is most common.

EMI CHARACTERISTICS

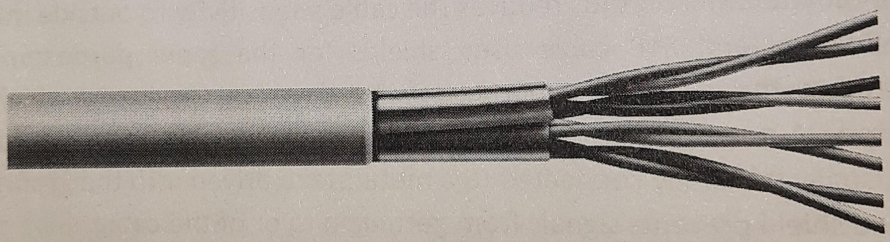
The shield in STP cable results in good EMI characteristic for copper cable, comparable to the EMI characteristic of coaxial cable. This is one reason STP might be preferred to unshielded twisted-pair cable in some situations. As with all copper cables. STP is sensitive to interference and vulnerable to electronic eavesdropping.

ADVANTAGES:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparatively faster

DISADVANTAGES:

- Comparatively difficult to install and manufacture
- More expensive
- Bulky



3.3 SHIELDED TWISTED-PAIR (UTP) CABLE

UNSHIELDED TWISTED-PAIR (UTP) CABLE

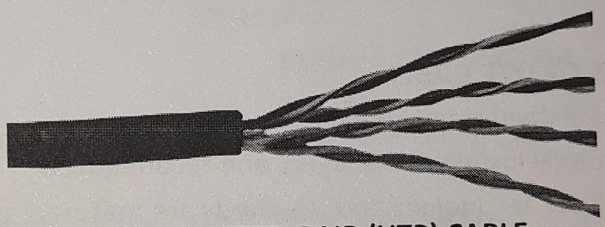
Unshielded Twisted-pair cable does not incorporate a braided shield into its structure; however, the characteristics of UTP are similar in many ways to STP, differing primarily in attenuation and EMI. As shown in figure, several Twisted-pairs can be bundled in a single cable. These pairs typically are colour-coded to distinguish them. Telephone systems commonly use UTP cabling. Network engineers can sometime use existing UTP telephone cabling (if it is new enough and of high-enough quality to support network communications) for network cabling.

UTP cable is a latecomer to high-performance LANs because engineers only recently solved the problems of managing radiated noise and susceptibility to EMI. However, a clear trend toward UTP is in operation, and all new copper based cabling schemes are based on UTP.

UTP cable is available in the following five grades, or categories :

- Categories 1 and 2 - These voice-grade cables are suitable only for voice and for low rates (below 4 mbps). Category 1 was once the standard voice-grade cable for telephone systems. The growing need for data-ready cabling systems, however, has caused Categories 1 and 2 cables to be supplanted by category 3 for new installation.
- Category 3 - As the tower data-grade cable, this type of cable generally is suited for data rates 10 mbps. Some innovative schemes, however, let the cable support data rates up to 100 mbps. Category 3, which uses four twisted pairs with three twists per foot, is now the standard cable used for most telephone installations.
- Category 4 - This data grade cable, which consist of four twisted pairs, is suitable for data rates up to 16 Mbps.
- Category 5 - this data grade cable, which also consist of four twisted pairs, is suitable for data range up to 100 mbps. Most new cabling systems; for 100 Mbps data rates designed around Category 5 cable.

DTP cable offers an excellent balance of cost and performance characteristics, a discussed in the following sections.



3.4 UNSHIELDED TWISTED-PAIR (UTP) CABLE

COST

UTP cable is the least costly of any cable type, although properly installed Category 5 tends to be fairly expensive. In some cases existing cable in buildings can be used for LANs, although you should verify the category of the cable and know the length of the cable in the walls. Distance limits for voice cabling are much less stringent than for data-grade cabling.

INSTALLATION

UTP cable is easy to install. Some specialized equipment might be required, but the equipment is low in cost and can be mastered with a bit of practice. Properly designed UTP cabling systems easily can be reconfigured to meet changing requirements. As noted earlier, however, Category 5 cable has stricter installation requirements than lower categories of UTP. Special training is recommended for dealing with Category 5 UTP.

CAPACITY

The data- rates possible with UTP have increase from 1 Mbps; pat 4 and 16 Mbps, to the point where 100 Mbps data rate are now common,

ATTENUATION

UTP cable share similar attenuation characteristics with other copper cables. UTP cable runs are limited to a few hundred meters, with 100 meters as the most frequent limit.

EMI CHARACTERISTICS

Because DTP cable lacks a, shield, it is more sensitive to EMI than coaxial or STP cables. The latest technology makes it possible to use UTP in the vast majority of situation, provided that reasonable care is taken to avoid electrically noisy devices such as motors and fluorescent lights. Nevertheless, UTP might not be suitable for noisy environments such as factories. Cross talk between nearby unshielded pairs limits the maximum length of cable runs.

Connectors for UTP

The most common connector use with UTP cables is the RJ-45 connector. These connectors are easy to install on cables and are also extremely easy to connect and disconnect.

ADVANTAGES OF UTP CABLE

- Relatively inexpensive
- Easily installed, managed, and reconfigured
- Basic technology and standards are matured and stable

DISADVANTAGES OF UTP CABLE

- Only categories 5,6,7 UTP cables are capable of high-speed (> 100 Mbps) data transmission.
- Relatively high rate of attenuation
- Sensitive to EMI

COAXIAL CABLES

Coaxial cables were the first cable types used in LANs. Coaxial cable gets its name because two conductors share a common axis. The cable is most frequently referred as coax. It has better shielding than twisted pair, so it can span longer distances at higher speed two kinds of co-axial cable are widely used.

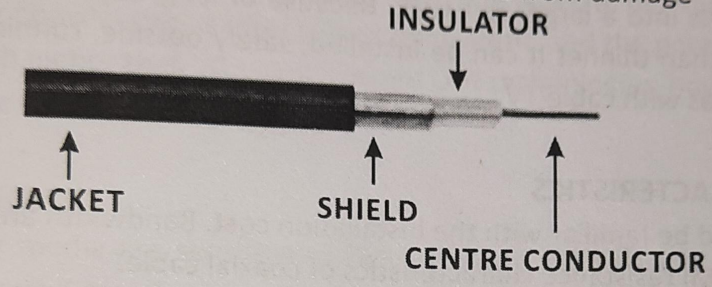
1. 50-ohm cable (Base band coaxial cables / Thinnet) is commonly used for digital transmission.

2. 75-ohm cable (Broad band coaxial cables / thicknet) is commonly used for analog transmission.

This distinction is based on historical, rather than technical, factors (e.g.- early dipole antennas had an impedance of 300 ohms, as it was easy to built 4:1 impedance matching transformers)

THE COMPONENTS OF THE CO-AXIAL CABLE ARE AS FOLLOWS:

- A central conductor, although usually solid copper wire, this sometimes is also made of standard wire.
- An outer conductor forms a tube surrounding the central conductor. This conductor can consist of braided wires, metallic foil or both. The outer conductor, frequency called the shield, servers as a ground and also protects the inner conductor from EMI.
- An insulation layer keeps the outer conductor spaced evenly from the inner conductor.
- A plastic encasement (jacket) protects the cable from damage



3.4 THE COMPONENTS OF THE CO-AXIAL CABLE

The construction and shielding of the co-axial cable give it a good combination of high bandwidth and excellent noise immunity. The possible bandwidth depends on the cable length.

TYPES OF CO-AXIAL CABLES

BASEBAND CO-AXIAL CABLES (THINNET)

This is light and flexible cabling-medium that is inexpensive and easy to install. Following table illustrate some thinnet classifications. Note that thinnet falls under the RG-58 family, which has 50 ohm impedance. Thinnet is approximately .25 inches (6 mm) in thickness.

CABLE	DESCRIPTION	IMPEDANCE
RG-59/U	Solid copper centre	50 ohm
RG-58A/U	Wire stand centre	50 ohm
RG-58C/U	Military version of RG-58 A/ U	50 ohm

Thinnet cable can reliably transmit a signal for 185 meters (about 610 feet). Although it's called 10Base2 to give the impression that it can run 200 meters, this is erroneous. It should really be called 10Base 1.85.

BROADBAND CO-AXIAL CABLES (THICKNET)

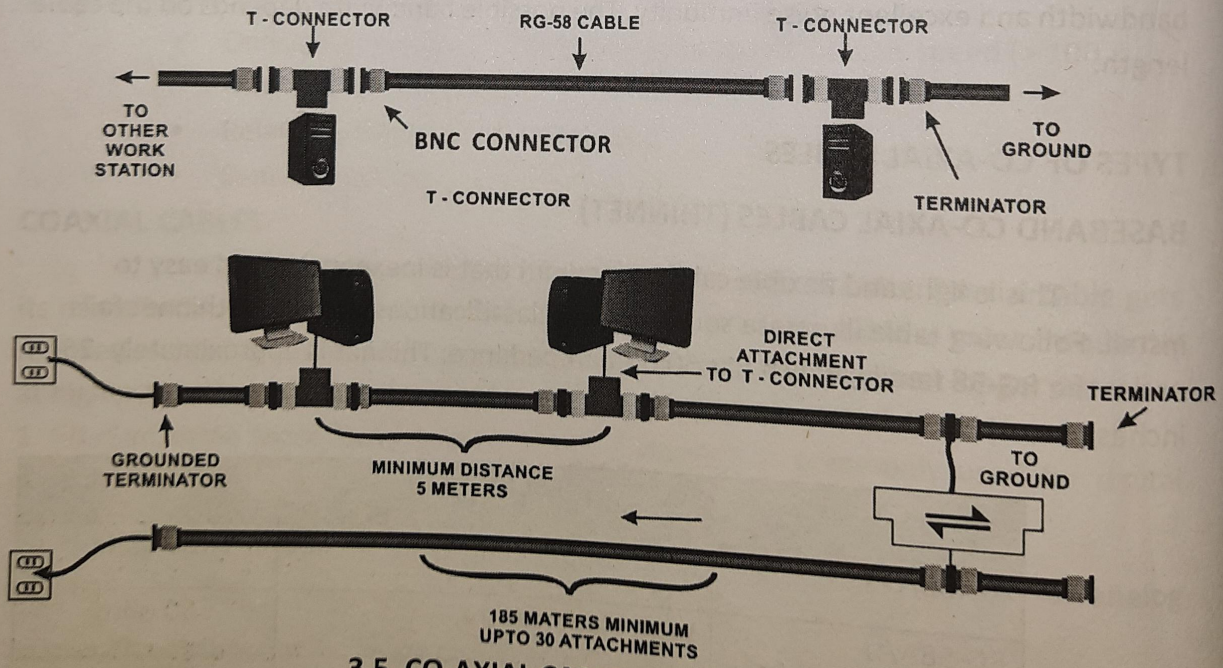
Thicknet is thicker in diameter that thinnet (approximate 0.5 inches). Because it is thicker and doesn't bend as readily as Thinnet. Thicknet cable is harder to work with. A thicker center core, however, means that Thicknet can carry more signals for a greater distance than Thinnet. Thicknet can transmit a signal approximately 500 meters (1650 feet). Thicknet cable is sometimes called Standard Ethernet (although other cabling types are also useful for Ethernet) Thicknet can be used to connect two or more small thinnet LANs into a larger network. Because of its greater size, Thicknet is also more expensive than thinnet It can be installed, safely outside, running from building to building, such as with cable TV.

CO-AXIAL CHARACTERISTICS

You should be familiar with the installation cost. Bandwidth and EMI cost, bandwidth and EMI resistance characteristics of coaxial cable.

INSTALLATION

Co-axial cable typically is installed in two configurations: daisy chain (from device to device-Ethernet) and star (ARC net)



3.5 CO-AXIAL CABLE INTALLATION

The Ethernet cabling shown in the figure is an example of Thinnet, which uses RG-58 cable. Devices are connected to the cable by means of T. connectors. Cables are used to provide connections between T-Connectors. One characteristic of this type of

cabling is that a special connector, called terminator, must terminate the ends of cable run. The terminator contains a resistor that is-matched to the characteristics of the cable. The resister prevents signals that reach the end of the cable from bouncing back and causing interference.

Co-axial cable is reasonably easy to install because it is robust and difficult to damage. In addition, connectors can be installed with inexpensive tools and a bit of practice. The device -to-device cabling approach can be difficult to reconfigure, however, when new devices cannot installed near an existing cabling path.

The co-axial cable used for Thinnet fall at the low end of the cost spectrum, whereas Thicknet is among the more costly options.

BANDWIDTH

LANs that employ coaxial cable typically have a bandwidth between 8.5 mbps and 10 Mbps. Thicker co-axial cables offer higher bandwidth, and the potential bandwidth of co-axial is much higher than 10 Mbps. Current LAN technologies, however don't take advantage of take of this potential.

EMI CHARACTERISTIC

All copper media are sensitive to EMI, although the shield in coax makes the cable fairly resistant, Coaxial cables, however, do radiate a portion of their signal, and electronic eavesdropping equipment can detect this radiated signal.

CONNECTORS FOR COAXIAL CABLES

Two types of connectors are commonly used with coaxial cable. The most common is the BNC corrector mainly used for thinnet cabling. In contrast Thicknet uses N-Connectors, which Screw instead of using a twist lock.

ADVANTAGES OF COAXIAL CABLE:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

DISADVANTAGES OF COAXIAL CABLE:

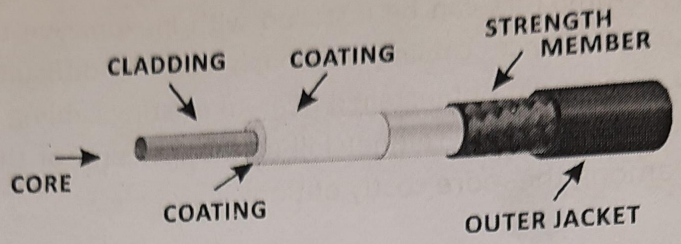
- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

FIBER-OPTIC CABLE

In almost every way, fiber-optic cable is the ideal cable for data transmission. Not only does this type of cable accommodate extremely high bandwidth's, but it also presents no problems with EMI and supports durable cables an cable runs as long as several kilometers. The two disadvantages of fiber-optic, however, are cost difficulty of installation.

The center conductor of a fiber-optic cable is a fiber that consists of highly refined glass or plastic designed to transmit light signals with little loss. A glass core supports a

longer cabling distance, but a plastic core is typically easier to work with. The fiber is coated with a cladding that reflected signals back into the fiber to reduce signal loss. A plastic sheath protects the fiber.



3.6 FIBER-OPTIC CABLE

Optical fibers are much smaller and more lightweight than copper wires. Therefore, large fiber optic cables carry more conductors than similar sized copper cables. There are two types of optical fibers.

1. Multimode fiber 2. Single mode fiber

The following table shows the comparison between single mode and multimode fibers.

SR. NO	SINGLE MODE FIBER	MULTIMODE FIBER
1	High capacity Lesser	capacity than single mode
2	More costlier	Cheaper than single mode
3	Light pulses are generated by injection Laser diode (ILDs)	Light pulses are generated by light emitted diodes (LEDs)
4	Can sustain a transmission rate of 100 Mbps at distance of 20 KM	Pan sustain a transmission rate of 100 Mbps at distance of 2 KM
5	Has been, optimized to allow one light path	Has been optimized to multiple one light path

A fiber-optic network cable consists of two strands separately enclosed in plastics sheaths- one strand sends and the other receives.

Two types of cable configuration are available:

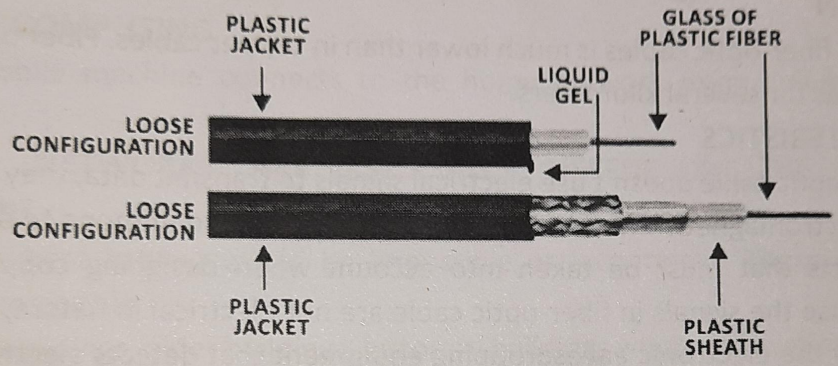
- **LOOSE CONFIGURATION**

Loose configuration incorporates a space between the fiber sheath and the outer plastic encasement; this space is filled with gel or other material.

- **TIGHT CONFIGURATION**

Tight configuration contains strength wires between the conductor and the outer plastic encasement.

In both cases, plastic encasement must supply the strength of the cable, while the get layer or strength wires protect the delicate fiber from mechanical damage.



3.8 LOOSE & TIGHT CONFIGURATION

Fiber optic cable doesn't transmit electrical signals. Instead, the data signals must be converted into light signals. Light sources include lasers and light-emitting diodes (LEDs). LEDs are inexpensive but produce a fairly poor quality of light suitable for less-stringent application. The end of the cable that receives the light signal must convert the signal back to an electrical form. Several types of solid-state components can perform this service.

One of the significant difficulties of installing fiber-optic cable arises when two cables must be joined. The small cores of the two cables (some are as small as 8.3 microns) must be lined up with extreme precision to prevent excessive signal loss.

As with all cable types, fiber-optic cable has their share of advantages and disadvantages.

COST

The cost of the cable and connector has fallen significantly in recent years. However, the electronic devices required are significantly more expensive than comparable devices for copper cable. Fiber-optic cable is also the most expensive cable type to install.

INSTALLATION

Greater skill is required to install fiber-optic cable than to install most copper cables. However, improved tools and techniques have reduced the training required. Still, fiber-optic cable requires greater care, because the cable must be treated fairly

gently during installation. Every cable has a minimum bend radius, for example, and fibers are damaged if the cables are bent too sharply. It is also important not to stretch the cable during installation.

CAPACITY

Fiber-optic cable can support high data fates (as high as 200,000 Mbps), even with long cable runs. Although UTP runs cable are limited to less than 100 meters with TOO Mbps data rates, fiber optic cable can transmit 100 Mbps signals for several kilometers.

ATTENUATION

Attenuation in fiber-optic cables is much lower than in copper cables. Fiber optic cables can carry signals for several kilometers.

EMI CHARACTERISTICS

Because fiber-optic cable doesn't use electrical signals to transmit data, they are totally immune to electromagnetic interference. These cables are also immune to a variety of electrical effects that must be taken into account when designing copper cabling systems. Because the signals in fiber-optic cable are not electrical in nature, they can't be detected by the electronic eavesdropping equipment that detects electromagnetic radiation. Therefore, fiber-optic cable is the perfect choice for high-security networks.

ADVANTAGES OF FIBER OPTIC CABLE

- Supports very high bandwidth- from 100 Mbps to >2Gbps
- Very low alteration
- Immune to EMI or eavesdropping

.DISADVANTAGES OF FIBER OPTIC CABLE

- Very expensive cables
- More complex to install
- High precision required for connections

3.2 WIRELESS TRANSMISSION-RADIO WAVES, MICROWAVES, INFRARED WAVES, SATELLITE COMMUNICATION.

WIRELESS TRANSMISSION

Our age has given rise to in formation junkies: people who need to be online all the time. For these mobile users, twisted pair, coax, and fiber optics are of no use. They need to get their hits of data for their laptop, notebook or palm top. Without being depending on the terrestrial communication infrastructure, for these users wireless communication is the answer. In this section we will look at wireless communication in general, as it has many other important applications besides providing connectivity to users who want to read their e-mail in airplanes. Technology is expanding rapidly and will continue to expand into the near future, offering more and better options for wireless networks.

FOLLOWING ARE THE DISADVANTAGES OF USING SATELLITE COMMUNICATION –

- Launching of satellites into orbits is a costly process.
- Propagation delay of satellite systems is more than that of conventional terrestrial systems.
- Difficult to provide repairing activities if any problem occurs in a satellite system.
- Free space loss is more
- There can be congestion of frequencies.

3.3 NETWORKING DEVICES (REPEATER, HUB, SWITCH, ROUTER, BRIDGE, MODEM)

NETWORKING DEVICES

The interfaces and devises that are used to connect computing devices and transmission media are called connectivity hardware or network connectivity devices.

Network connectivity hardware connects individual devices and transmission media are called connectivity hardware or network connectivity devices".

Network connectivity hardware connects individual devices to a single network, for example a PC or printer would use network connectivity devices to connect to UTP or some other that we are going to study in particular section of your book.

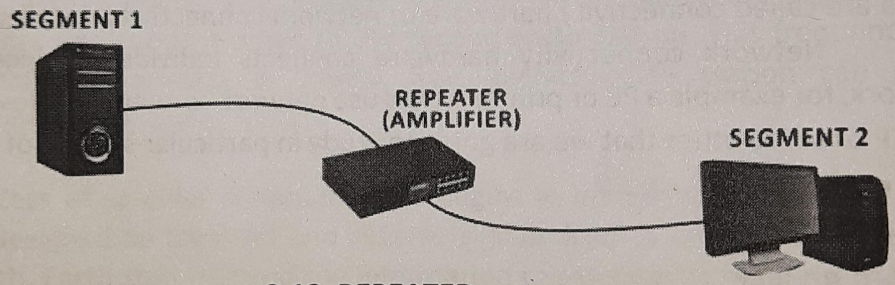
- Repeaters
- Hubs
- Bridges
- Switches
- Routers
- Modem

REPEATERS

- The repeater also called a regenerator.
- It is an electromagnetic device that simply regenerates a signal.
- A repeater is a simplest low level device.
- It works at physical layer of OSI reference mode
- They are often used if a few network stations are located far from the rest of the network.
- A repeater installed on a link, receive the signal before it becomes too week of or corrupted, regenerates the origin at big pattern and put the refreshed copy back on to the link.
- A repeater allows us to extended only physical length of network.
- The repeater does not change the functionality of the networks in anyway.

HOW IT WORKS?

- A repeater just forward bits from one network to another, making two networks logically like one network.
- They are passive in nature, do not look at or alter the content of the packet flowing across the wire. That is, repeater are dumb, they just copy bits blindly without understanding what they are doing.
- Signals travels across physical wire. After traveling some distance, they become weak or get corrupted.
- A repeater receive corrupted and weak signal and regenerate it.
- For ex, if station A sends a frame to station b, all station will receive the frame just as they would without repeater.
- The repeater does not have the intelligence to keep the frame from passing to the right side when actual station on the left side.
- The difference is that with repeater station C and D receive a truer copy of the frame.

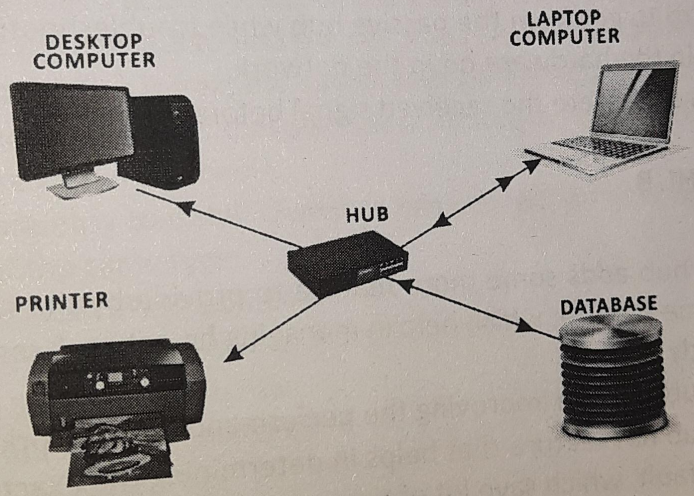


3.12 REPEATER

ADVANTAGES AND DISADVANTAGES OF REPEATERS

ADVANTAGES	DISADVANTAGES
Allow you to extend the network over large distances	Have no knowledge of addressing or data types.
Do not affect the speed of network	Can't ease network congestion problems
Can connect network segments of different media.	Limit the number of repeaters that can be used.

- It is physical layer device. It is the simplest network device so, it has low cost.
- It serves central connection point fro several network devices. Hub is nothing more than a multiport repeater.
- A hub repeats what it receives one port to all other ports. They do not alter or look at the contents of the packet traveling across the wire.
- Hub joins two or more twisted pair cables. It provide from 8 to 24 twisted pair connection depending on the manufacturer and the model of the hub.
- A hub is a medium used to collect signals from the input lines and redistribute them in various available wiring around a topology.
- Hub is basically act as a signal splitters, it accept signal through it input port and outputs it to the outputs ports.
- Some hubs help in regenerating the weak signals before, sending them to the intended output lines. Generally hubs are used more commonly, where star topology used



3.13 HUB WORKING

CLASSIFICATION OF HUB

- There are many types of hub with various features or specifications, which provide the type of functionality you need in building networks.
- There are 3 main types of Hub.
  1. Active Hub
  2. Passive Hub
  3. Intelligence Hub

1. ACTIVE HUB

- Active hub is a type of hub that takes active participation in data communication within the network
- Active hub come with carious features such as receiving the signal from the input port and storing it for sometimes before forwarding it.
- Some hub comes with a feature that helps in transmitting data that has high priority before the data that has lower priority before the data that has lower priority.
- Some hubs help in synchronizing data communication by retransmitting the packet.
- Active hubs come with a feature that rectifying the feature before forwarding it in the LAN or in a network.

2. PASSIVE HUB

- Passive hub does not provide any additional feature accept working just as n interface between the topology
- These types of hubs do not help in rectifying on enhancing the which they pass on the network.
- It is very hard to get from the passive hub while troubleshooting in case if there is any fault in the hardware on in the network.
- It does not regenerate the received signal before forwarding.

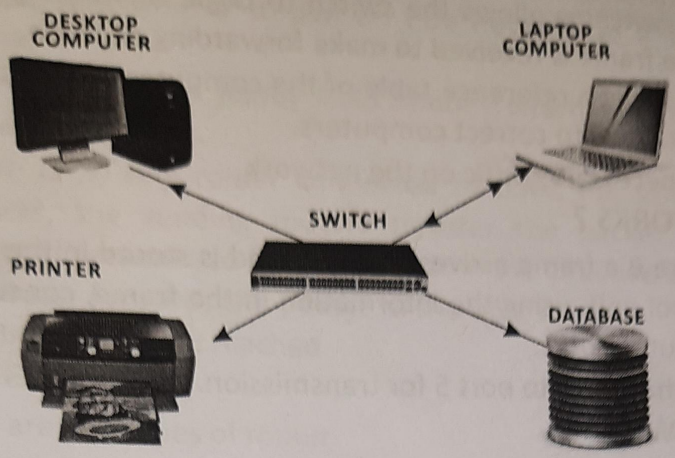
3. INTELLIGENCE HUB

- Intelligence hub adds some more feature to provide by the active hub. It also provides some feature, which help in managing he network resource effectively and efficiently.
- Intelligent hub helps in improving the performance of network and LAN.
- Intelligent hub has feature that helps in determining the exact cause and exact place of the fault, which save lot of time and energy.
- It helps in controlling and minimizing data traffic in the network.
- Intelligent hub also helps in managing the data communication within the network by recognized the slower device automatically and helps them to transmit the data with their own speed.

HOW IT WORKS ?

- When a hub received data from one of the connected devices. It passes data to all other ports without checking for the destination device except the port through which it receives the data.

SWITCHES



3.14 SWITCH WORKING

- A switch is a device that provides bridging functionality with greater efficiency. A switch may act as a multiport bridge to connect devices or segment in LAN.
- The switch normally has a buffer for each network or link to which it is connected.
- When it receives a packet, it stored the packet in the buffer of the receiving link and checks the address to find the out going link (Destination station)
- If the out going link is free, the switch sends the frame to that particular link.
- Switches are smart hubs that send data directly to the destination rather than everywhere within a network.
- Switches are easy to install. Switches can connect different network types or a network of the same types.
- A switch is available in 8,16,24 and 48 ports.
- It operates in data link layer of the OSI reference model.
- There are 2 types of switches
  1. Store and forward switches
  2. Cut through switches

1. STORE AND FORWARD SWITCHES

- Examine the entire packet. Each in coming packet in buffered that examine.
- Filters out any bad packets if it detect.
- Good packets are forwarded to the correct segment
- It detects more errors than cut through variety

2. CUT THROUGH SWITCHES

- Only the first few bytes of the packets are read to obtain the source and destination address.
- The packets are than passed through the destination segment without checking the rest of the packet errors.
- Invalid packet can still be passed on to other segment.

- This kind of switching allows the switch to begin forwarding the frame when enough of the frame is received to make forwarding decision.
- Switches construct a reference table of the computers connected to them and then send data only to correct computers.
- This limits unnecessary traffic on the network

HOW SWITCHES WORKS ?

- In above figure B a frame arrives at port 2 and is stored in the buffer. The CPU and the control unit, using the information in the frame, consult the switching table to the output port.
- The frame is than send to port 5 for transmission.

ADVANTAGES OF SWITCHES

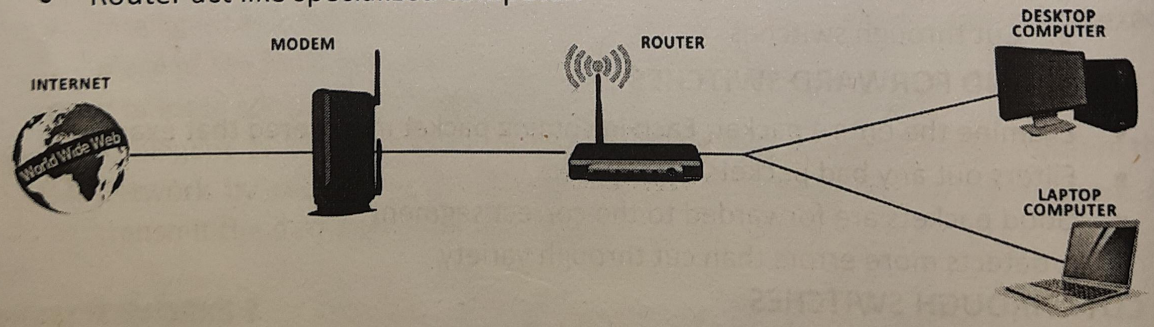
- Isolate traffic
- Separate collision domains
- Reducing collision

DISADVANTAGES OF SWITCHES

- Currently its price is 3 to 5 times more than price of the hub.
- Packet processing time is longer than in a hub.
- Monitoring the network is more complicated.

ROUTER

- Repeaters and bridges are simple hardware devices which are capable of executing specific task.
- Routers are more sophisticated.
- Router checks the destination address of the received packet.
- Depending on the destination, router selects the best route the packet from its routing table.
- Router operates at network layer of OSI reference model.
- It forwards packets based on the network id.
- Router act like specialized computer.



3.15 ROUTER WORKS

HOW ROUTER WORKS?

- Router maintain routing table.
- Routing table contains information of network id to know how to get to that network.
- Router makes the decision based on the routing table.

- Above figure shows a possible internetwork of five networks.
- A packet sent from a station on one network to a station on another network.
- It first goes to the jointly held router, which switches it over to the destination network.
- It there is no one router connected to both, the sending and receiving networks, the sending routers transfer the packet across one of its connected networks to the next router in the direction of the destination.
- That router forwards the packet to the next router on the path and so on, until the destination reached.

TYPES OF ROUTER

- There are two types of router
  a. Static Router
  b. Dynamic Router

a. STATIC ROUTER

- It enables the network administrator to enter the route information manually in th following routing table
- This process is very time consuming.

b. DYNAMIC ROUTER

- It updates the routing table automatically according to the changes in network topology and information received from other router.

ADVANTAGES OF ROUTER

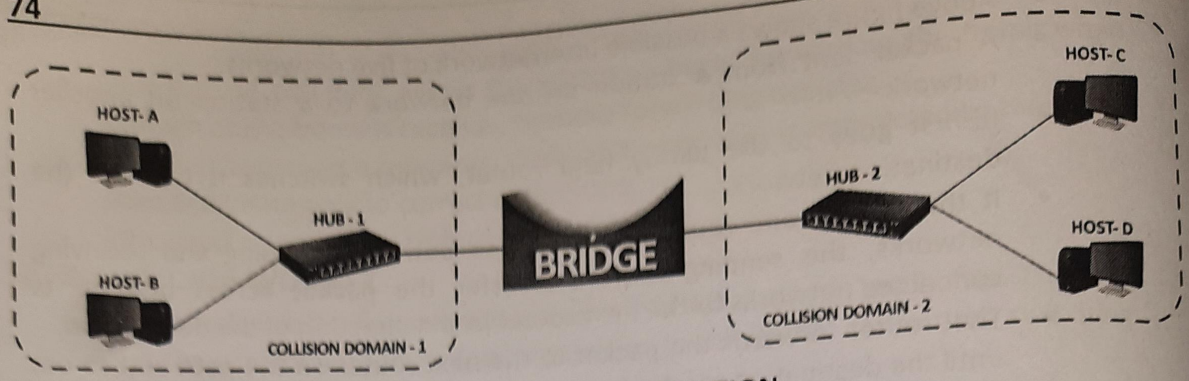
- Transfer data to the destination node by selecting the best path.
- Connect different type of networks.
- Share information with other router in the network.
- Contains routing table that keep track of the routes to the network.

DISADVANTAGES OF ROUTER

- More expensive than bridges and routers
- Operates slowly than bridges and repeaters

BRIDGE

- Bridge operates at the data link layer of the OSI reference model.
- A bridge is sometimes combining with router in a product called Brouter.
- The main idea of using a bridge is to divide a big network into smaller sub network called segment.
- It logically separates a single network in to two segments of the network to which the destination station attached. It will not pass to the other segment.
- Bridges can connect dissimilar network type, For ex, token ring and Ethernet.
- It the bridges operate at the lower layer,the bridge can connect only similar network types. For ex, token ring and Ethernet to Ethernet.



3.16 BRINGE OPERATION

HOW BRIDGES WORK?

1. **How it reduce the traffic?**

- If you have a group of workstation that constantly exchange data on the same network segment. As a group of workstation that do not use the network much, the busy group will slow down the performance of the network for the other users.
- If you put the bridge to separate two groups, only traffic destined for a workstation on the other side of the bridge will pass to that side only. All the other traffic stays local.
- A bride access the physical addresses of all the stations connected to it. When a frame enters a bridge, the bridge not only regenerates the signal but also checks the address of the destination and forward the new copy only to the segment to which the address Belongs.
- As a bridge encounter packet, it reads the address contained in the frame and compares that address with a table station on both segment. When it find the match, it discovers to which segment the station belongs and relays the packet only to that segment.
- For ex, two segments join by a bridge in above figure a packet from station A address to station D arrives at the bridge. The station D therefore a packet Is blocked from crossing in to the lower segment. If a packet from station A address to the station G, the bridge allow the packet to cross and relates it entire lower segment.

TYPES OF BRIDGE

- There are several types of bridge:

1. Simple bridge
2. Multiport bridge
3. Transport bridge
4. Source Routing bridge

1. SIMPLE BRIDGE

- Simple bridges are least expensive type of bridge.
- A simple bridge links two segments and contains a table that least the addresses of all the station included in each of them.
- In this type of bridge addresses must be entered manually

2.MULTIPORT BRIDGE

- A multiport bridge can because to connect more then two LANs.
- Each bridge holding the physical addresses of stations reachable through the corresponding port.

3.TRANSPORT BRIDGE

- A bridge is called transport Bridge if it is invisible to other devices on the network.
- When transport is first install, it's table is empty.
- Transport bridge only blocks or forwards frame, If address is not found in the forwarding table, the frame is flooded to all the ports of the bridge.

4.SOURCE ROUTING BRIDGE

- it is found in a token ring environment
- Source routing bridge provides an alternative to transport bridge.

ADVANTAGES OF BRIDGE

- In case the number of attached workstations and network segment.
- By sub dividing the LAN into smaller segment, overall reliability ios increased and the network becomes easier to maintain.
- Help to localize network traffic by only forwarding data on to other segment as required.

DISADVANTAGES OF BRIDGE

- Bridges may overload during periods of high traffic.
- In complex networks data may be sent over redundant path and the shortest path is not always taken.

MODEM (MODULATOR/ DEMODULATOR)

Modem converts your computer digital signal to an analog transmission signal to use with telephone tines or microwave transceivers. Modem is necessary because telephone lines and microwave media uses electromagnetic waves, but your computer uses electric pulses. Modems are also useful when the signal from the transceiver is hot powerful enough to travel a required, distance without significant loss of data, modems can be used to amplify signals.