HR.

1 Introduction to Computer Networks and Internet

Syllabus

Understanding of network and Internet, The network edge, The network core, Understanding of delay, loss and throughput in the packet-switching network, Protocols layers and their service model, History of the computer network.

Contents

1.1 Internet

- Internet is known through its applications : The World Wide Web, email, streaming audio and video, chat rooms, and music (file) sharing.
- The Internet is a type of world-wide **computer network**. Internet is a network that interconnects millions of computing devices throughout the world.
- The Internet is a "network of networks" that consists of numerous academic, business, and government networks, which together carry various information and services, such as e-mail, web access, file transfer and many other.
- The Internet provides a much lower cost alternative to PSTN for support of multimedia applications.

communication done
file sharing/ to two device then
called. Rate

1.1.1 Protocol and Standards

- A protocol is a set of rules that governs data communications. Protocol defines the method of communication, how to communicate, when to communicate etc.

  Important elements of protocol are

  1. Syntax 2. Semantics 3. Timing

1. Syntax

- Syntax means format of data or the structure how it is presented e.g. first eight bits are for sender address, next eight bits for receiver address and rest of the bits for message data.

2. Semantics

- Semantics is the meaning of each section of bits e.g. the address bit means the route of transmission or final destination of the message.

3. Timing

- Timing means, at what time data can be sent and how fast data can be sent.

Standards

- Standards provide guidelines to the manufacturers, venders, government agencies and service provider. It ensures the interconnectivity and compatibility of the device.
- Standards help in maintaining market competitiveness and guarantees interoperability.
- Data communication standards are of two categories

a) De facto : De facto means by facts or by convention. The standards that are not approved by any organization but are widely used are De facto standards. These are established by manufacturers.

b) **De jure** : De jure means by law or by regulation. These are the standards that are recognized officially by an organization.

1.2 Types of Network

GTU : Dec.-11

1.2.1 Local Area Network (LAN)

1 km to 10 km range

- The IEEE 802 LAN is a popularly used shared medium peer-to-peer communications network that broadcasts information for all stations to receive.
- The LAN enables stations to communicate directly using a common physical medium on a point-to-point basis without any intermediate switching node being required.
- A LAN is a system composed of computer hardware and transmission media and software.
- LANs are privately owned networks within a single building or campus of upto few km in range. It generally use only one type of transmission media.
- Depends upon application and cost, various topology used in LAN. (e.g. star, bus, ring).
- The basic idea of a LAN is to provide easy access to Data Terminal Equipment (DTEs) within the office. These DTEs are not only computers but other devices, such as printer, plotters and electronic files and databases.
- Fig. 1.2.1 shows the local area networks.

School, collage,

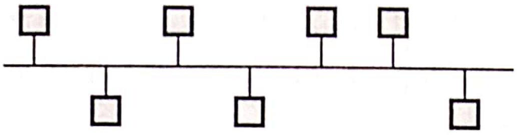


Fig. 1.2.1 LAN

- LAN can provide users
  1) Flexibility
  2) Speed
  3) Reliability
  4) Adaptability
  5) Security
  6) Transparent interface
  7) Access to the other LAN and WAN
  8) Hardware and software sharing
  9) Centralized management
  10) Private ownership of the LAN.

- **Attributes of LAN**

  1) The LAN transmits data amongst user stations.
  2) The LAN transmission capacity is more than 1 Mbps.
  3) The LAN channel is typically privately owned by the organization using the facility.
  4) The geographical coverage of LANs is limited to areas less than 5 square kilometers.

- LANs are typically identified by the following properties -

  1. Multiple systems attached to shared medium.
  2. High total bandwidth (~10 Mbps).
  3. Low delay.
  4. Low error rate.
  5. Broadcast / Multicast capability.
  6. Limited geography (1-2 km).
  7. Limited number of stations.
  8. Peer relationship between stations.
  9. Confined to private property.

- The low level protocols used in such environments are different from those used in wide area networks.

- The common forms of LAN are those described by the IEEE standard 802. This standard describes operation upto and including OSI layer 2. Individuals may build what they like on top of these basic protocols.

- A common set of higher level protocols is called TCP/IP which provides OSI layer 3 and 4 functionality, on top of this may be found a set of protocols commonly called Telnet protocols.

- At the lowest level the IEEE 802 specifications split into 3 corresponding to three different but common LAN structures. These are -
  802.3, 802.4, 802.5 standards for topology.

- LANs are capable of transmitting data at very fast rates, much faster than data can be transmitted over a telephone line ; but the distances are limited, and there is also a limit on the number of computers that can be attached to a single LAN.

- The following characteristics differentiate one LAN from another :

  1. **Topology** : The geometric arrangement of devices on the network. For example, devices can be arranged in a ring or in a straight line.
  2. **Protocols** : The rules and encoding specifications for sending data. The protocols also determine whether the network uses a peer-to-peer or client /server architecture.

3. **Media :** Devices can be connected by twisted-pair wire, co-axial cables, or fiber optic cables. Some networks do without connecting media altogether, communicating instead via radio waves.

1.2.2 Metropolitan Area Networks (MAN)

- A MAN, while larger than LAN is limited to city or group of nearby corporate offices. It uses similar technology of LAN.
- The Metropolitan Area Network standards are sponsored by the IEEE, ANSI and the Regional Bell operating companies. The MAN standard is organized around a topology and technique called Distributed Queue Dual Bus (DQDB).
- MAN provides the transfer rates from 34 to 150 Mbps.
- MAN is designed with two unidirectional buses. Each bus is independent of the other in the transfer of traffic. The topology can be designed as an open bus or a closed configuration.
- MANs are based on fiber optic transmission technology and provide high speed interconnection between sites. It can support both data and voice.
- MAN as a special category is that a standard has been adopted for them and this standard is now being implemented. It is called IEEE 802.6.

1.2.3 Wide Area Networks (WAN)

- A WAN provides long distance transmission of data and voice.
- A Network that covers a larger area such as a city, state, country or the world is called **wide area network.**
- The WAN contains host and collection of machines. User program is installed on the host and machines. All the host are connected by each other through communication subnet. Subnet carries messages from host to host.
- Fig. 1.2.2 shows the component of WAN.

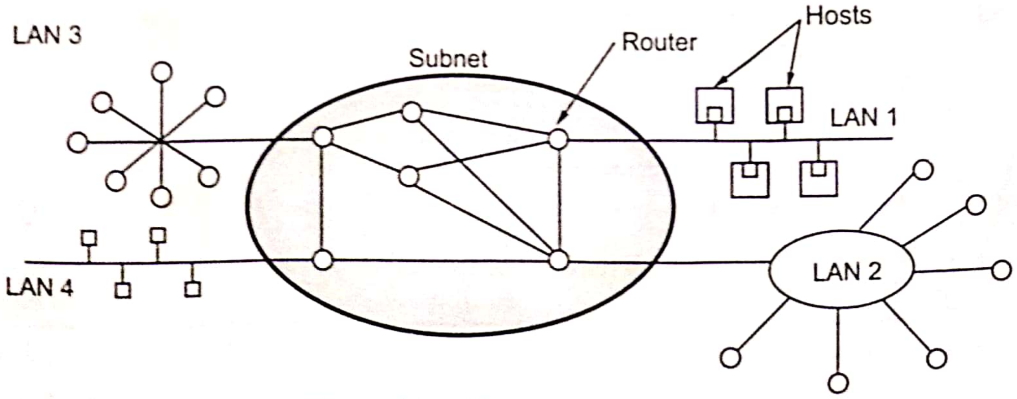


Fig. 1.2.2 Wide area network

- Subnet consists of transmission lines and switching elements. The transmission line is used for data transfer between two machines. Switching elements are used for connecting two transmission lines. Switching elements are specialized computers. It selects the proper outgoing line for incoming data and forward the data on that line.
- The switching elements are basically computers and they are called packet switching nodes, intermediate systems and data switching exchanges. These switching elements are also called routers.
- Each host is connected to a LAN on which a router is present. Sometimes the host can be directly connected to the router. The interconnection of routers forms the subnet.
- In the WAN, when the packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety. This packet is stored in that router until the required output line is free. The subnet which uses this principle is called point-to-point, store and forward, or packet switched subnet.
- Almost all the WANs use store and forward subnets.
- If the packets are small and of same size, they are also called cells.
- In the point-to-point subnet, the router interconnection topology becomes important. WANs can also use satellite or ground radio system. The routers have antenna, through which they can send or receive data, they can listen from satellite.
- WAN uses hierarchical addressing because they facilitate routing. Addressing is required to identify which network input is to be connected to which network output.

1.2.4 Comparison between LAN, WAN and MAN

Parameter	LAN	WAN	MAN
Area covered	Covers small area. i.e. within the building.	Covers large geographical area.	Covers larger than LAN & smaller than WAN.
Error rates	Lowest.	Highest.	Moderate.
Transmission speed	High speed.	Low speed.	Moderate speed.
Equipment cost	Uses inexpensive equipment.	Uses most expensive equipment.	Uses moderately expensive equipment.

1.2.5 Comparison between LAN and WAN

Sr. No.	LAN	WAN
1.	It covers small area.	WAN covers large geographical area.
2.	LAN operates on the principal of broadcasting.	WAN operates on the principal of point to point.
3.	Used for time critical application.	Not used for time critical application.
4.	Transmission speed is high.	Transmission speed is low.
5.	Easy to design and maintain.	Design and maintenance is not easy.
6.	LAN is broadcasting in nature.	WAN is point-to-point in nature.
7.	Transmission medium is co-axial or UTP cable.	Transmission or communication medium is PSTN or satellite link.
8.	LAN does not suffer form propagation delay.	WAN suffer from propagation delay.

1.2.6 Wireless Networks

- A wireless LAN or WLAN is a wireless local area network that uses radio waves as its carrier. The last link with the users is wireless, to give a network connection to all users in a building or campus. The backbone network usually uses cables.
- Wireless LANs operate in almost the same way as wired LANs, using the same networking protocols and supporting the most of the same applications.

=> Type
Ad-hoc
Inforstructure

How are WLANs Different ?

1. They use specialized **physical and data link** protocols
2. They integrate into existing networks through **access points** which provide a bridging function
3. They let you stay connected as you **roam** from one coverage area to another
4. They have unique **security** considerations
5. They have specific **interoperability** requirements
6. They require **different hardware**
7. They offer **performance** that differs from wired LANs.

- **Physical Layer :** The wireless **NIC** takes **frames** of data from the link layer, scrambles the data in a predetermined way, then uses the modified data stream to modulate a **radio carrier signal.**
- **Data Link Layer :** Uses Carriers-Sense-Multiple-Access with Collision Avoidance (CSMA/CA).

- Wireless Access Points (APs) is a small device that bridges wireless traffic to your network. Most access point's bridge wireless LANs into Ethernet networks, but Token-Ring options are available as well.
- A family of wireless LAN (WLAN) specifications developed by a working group at the Institute of Electrical and Electronic Engineers (IEEE). It defines standard for WLANs using the following four technologies
  1. Frequency Hopping Spread Spectrum (FHSS)
  2. Direct Sequence Spread Spectrum (DSSS)
  3. Infrared (IR)
  4. Orthogonal Frequency Division Multiplexing (OFDM)
- WLAN versions are : 802.11a, 802.11b, 802.11g, 802.11e, 802.11f, 802.11i

1.3 Network Topology

all topology

GTU : Winter-13,14

- The physical topology of LAN refers to the way in which the stations are physically interconnected.
- Topology is also defined as, the manner in which nodes are geometrically arranged and connected is known as the topology of the network.
- Physical topology of a local area network should have the following desirable features.
  1. The topology should be flexible to accommodate changes in physical locations of the stations, increase in the number of stations and increase in the LAN geographic coverage.
  2. The cost of physical media and installation should be minimum.
  3. The network should not have any single point of complete failures.
- Network topology refers to the physical layout of the network. Each topology has its own strengths and weaknesses.
- Four types of topologies are commonly used in the network. They are bus, star, ring and mesh topology.

1.3.1 Bus Topology

- Bus topology also called horizontal topology.
- In bus topology, multiple devices are connected one by one, by means of connectors or drop cables.
- When one computer sends a signal up (and down) the wire, all the computers on the network receive the information, but only one accepts the information (using address matching). The rest discard the message.

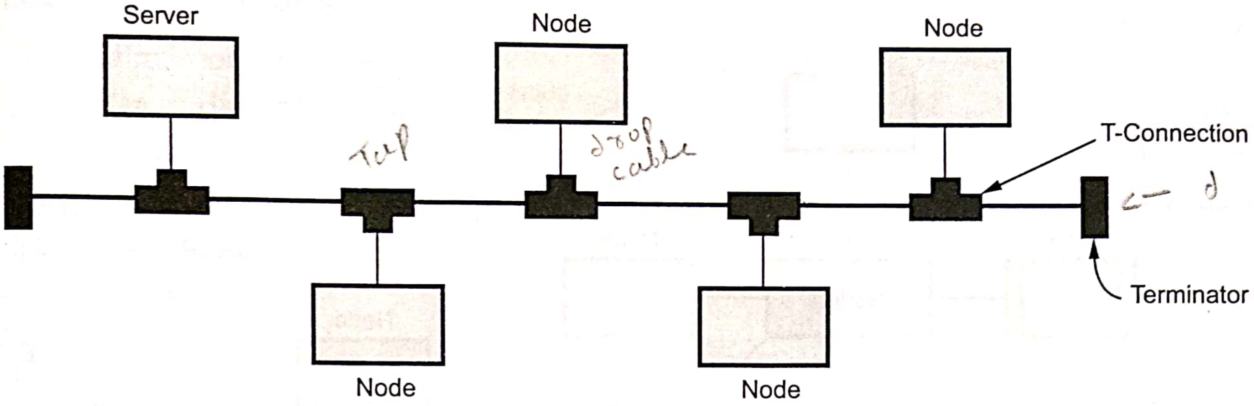


Fig. 1.3.1 Bus topology

- Bus is passive topology because it requires termination. Cable cannot be left unterminated in a bus network. Terminators were the 50 Ω resistors that were connected to each end of cable.

Advantages of Bus :

1) Easy to use and easy to install.

2) Needs fewer physical connectivity devices.

3) A repeater can also be used to extend a bus topology network.

4) Low cost.

Disadvantages of Bus :

1) Heavy network traffic can slow a bus considerably.

2) It is difficult to troubleshoot a bus.

3) Failure of cable affects all devices on the network.

4) Difficult to add new node.

1.3.2 Star Topology

- A star topology consists of a number of devices connected by point-to-point links to a central hub.
- Easy to control and traffic flow is simple.
- Data travels from the sender to central hub and then to the receiver.

Advantages of Star Topology :

1) It is easy to modify and add new nodes to a star network without disturbing the rest of the network.

2) Troubleshooting techniques are easy.

3) Failures of any node do not bring down the whole star network.

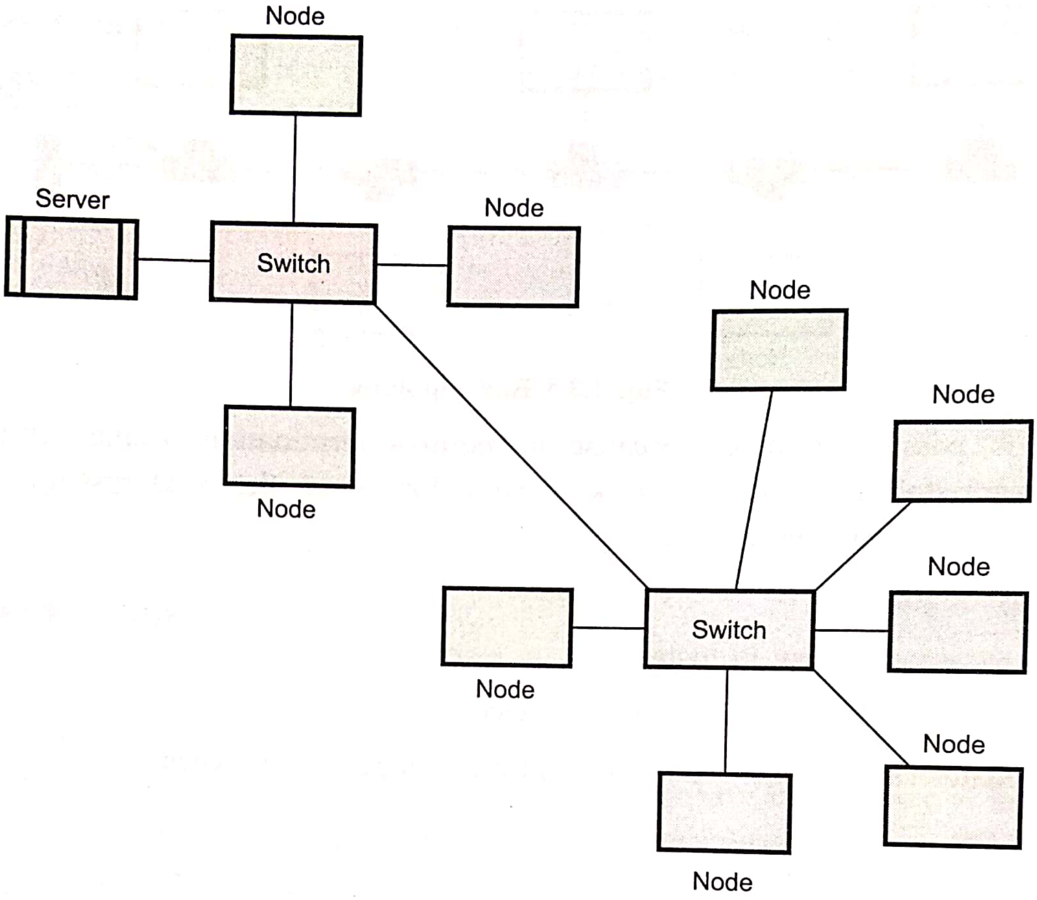


Fig. 1.3.2 Star topology

Disadvantages of Star Network :

1) If the central hub fails, the whole network fails to operate.

2) Each device requires its own cable segment.

3) Installation can be moderately difficult, especially in the hierarchical network.

1.3.3 Ring Topology

- In a ring topology, each computer is connected to the next computer, with the last one connected to the first. The signals travel on the cable in only one direction. Since each computer retransmits what it receives.
- Ring is an active network. Termination is not required.

Advantages of Ring :

1) Cable failures are easily found.

2) Because every node is given equal access to the token, no one node can monopolize the network.

Disadvantages of Ring :

1) Adding or removing nodes disrupts the network.
2) It is difficult to troubleshoot a ring network.
3) Failure of one node on the ring can affect the whole network.
4) Cost of cable is more in ring network.

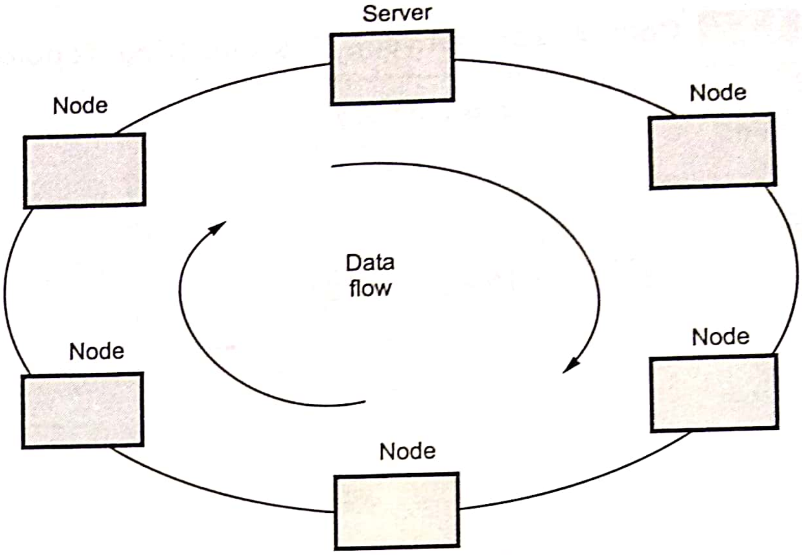


Fig. 1.3.3 Ring topology

1.3.4 Mesh Topology

- The mesh topology has a link between each device in the network. It is more difficult to install as the number of devices increases.
- Mesh networks are easy to troubleshoot.
- Much of the bandwidth available in mesh configuration is wasted.
- Most mesh topology networks are not true mesh networks. Rather, they are hybrid mesh networks, which contain some most important sites with multiple links.

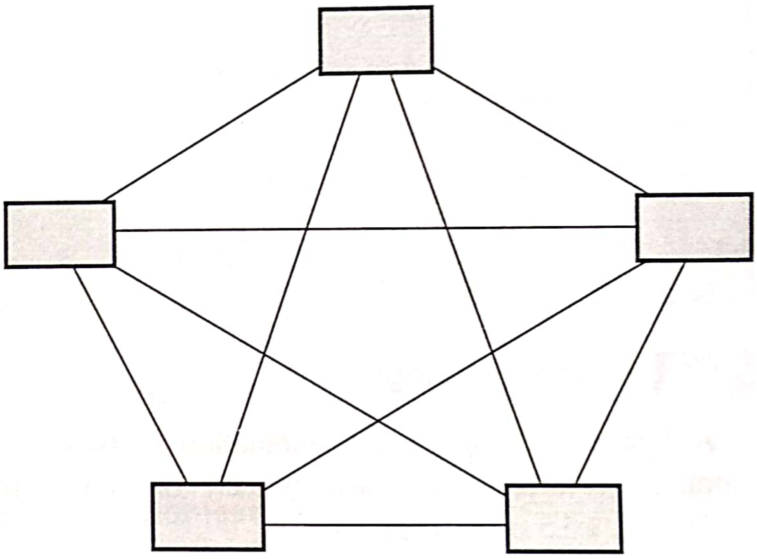


Fig. 1.3.4 True mesh topology

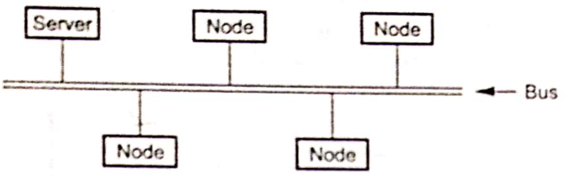
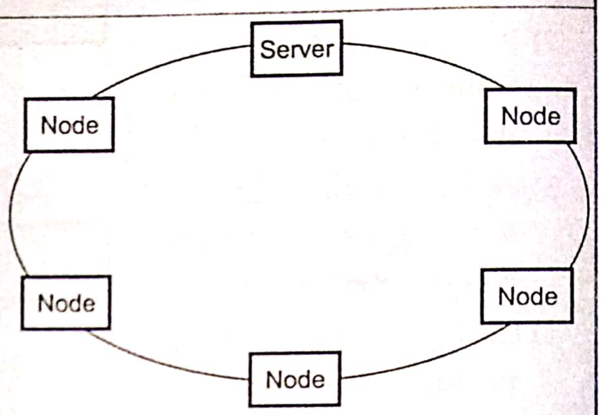
Advantages of Mesh :

1) Troubleshooting is easy. 2) Isolation of network failures is easy.

Disadvantages of Mesh :

1) Difficulty of installation.
2) Costly because of maintaining redundant links.
3) Difficulty of reconfiguration.

1.3.5 Comparison between Bus and Ring Topology

Sr. No.	Bus topology	Ring topology
1.		
2.	Bus requires proper termination. Cable cannot be left unterminated.	Termination is not required.
3.	Bus is a passive network topology.	Ring is an active network topology.
4.	There is loss in data integrity as the bus length increases.	Transmission errors are minimized because transmitted signal is regenerated at each node.
5.	It uses point to multipoint communication links.	It uses point-to-point communication links.
6.	Recommended when large number of devices are to be attached.	Recommended when moderate number of devices are to be attached.

1.3.6 Hybrid Topology

A hybird topology is a combination of two or more topologies. For example, bus topology connected in each branch of star network is shown in the Fig. 1.3.5. (Refer Fig. 1.3.5 on next page).

Tell

University Question

1. *What is topology ? Give different type of topology and its use.* **GTU : Dec.-11, Marks 5**

1.4 The Network Edge

1.4.1 End System, Clients and Servers

- In computer networks the computers connected to Internet are referred as **end systems**. The end systems are also called as **hosts** as they host application programs such as web browser program, a web server program an e-mail reader program.

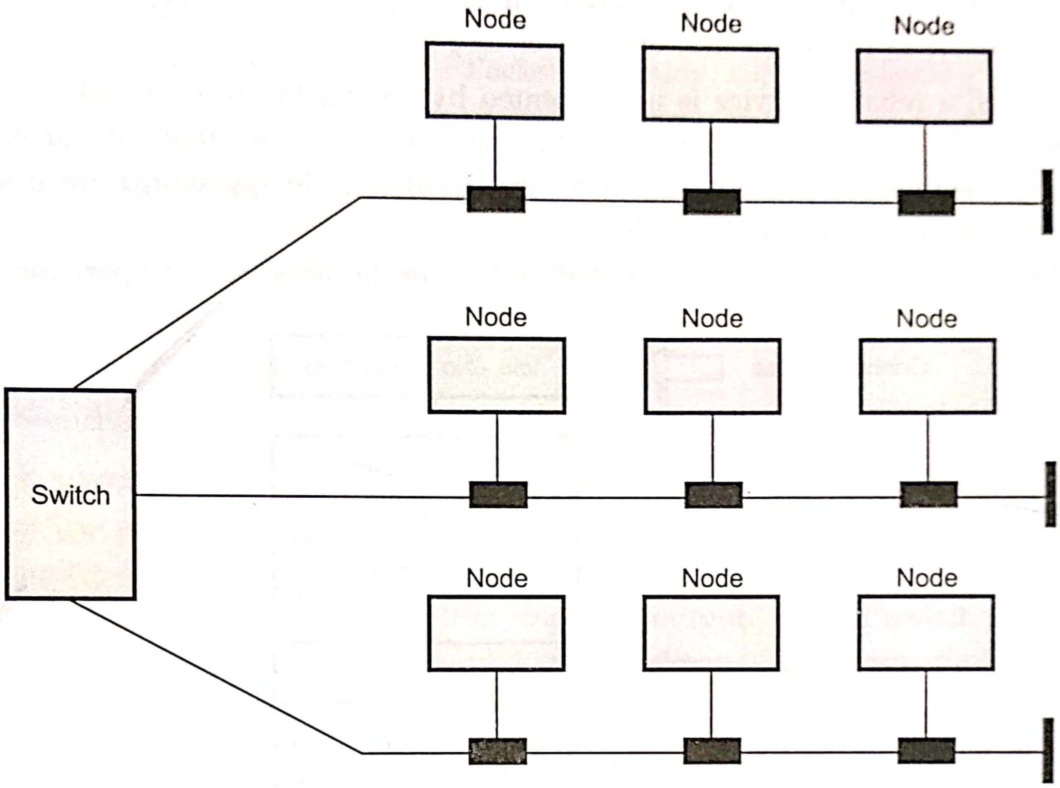


Fig. 1.3.5 Hybrid topology

- The hosts are further divided into clients and servers. Clients are desktop and mobile PCs whereas servers are more powerful devices such as web servers and mail servers.

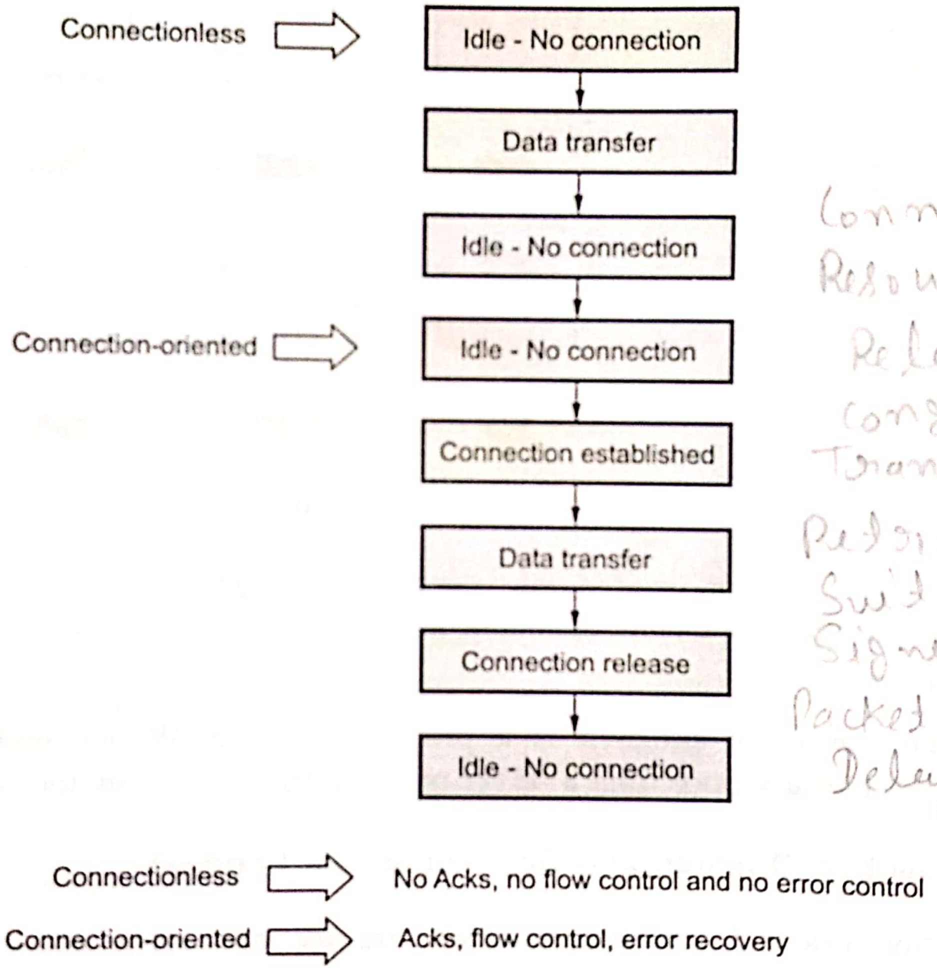
Client program : A client program is a program running on one end system that requests and receives a service from a server program running on another end system.

1.4.2 Connection Oriented and Connectionless Services

- Connection oriented and connectionless are the two types of services, that is offered by the layer.
- In **connection oriented,** direct path is established between source and destination. The telephone system is the example of the connection oriented service. This type of service provides a substantial amount of care for the user data.
- The **connectionless** (also called datagram) service goes directly from an idle condition into a data transfer mode, followed directly by the idle condition.
- The connectionless service is comparable to mailing a letter. Each message carries the full destination address, and each one is routed through the system independent of all the others.

- Each service can be characterized by a Quality Of Service (QOS). Some services are reliable in the sense that they never lose data.
- Usually, a reliable service is implemented by having the receiver acknowledge the receipt of each message, so the sender is sure that it arrived. The acknowledgement process introduces overhead and delays, which are often worth it but are sometimes undesirable.

Fig. 1.4.1 shows the connection oriented and connectionless service operation.



Connection
Resource Allocat
Reliability
Congestion
Transfer Mode
Retransmission
Suitability
Signaling
Packet Travel
Delay

Fig. 1.4.1 Connectionless and connection oriented service

University Question

1. *Give difference between connection oriented versus connectionless services.*

GTU : Winter-13,14, Marks 7

1.5 Network Core

- The **network core** is referred as the mesh of routers that interconnect the Internet's end systems.

- Different switching techniques are used for data transmission within the network. Basic methods of switching are : Packet switching, Circuit switching and Message switching.

1.5.1 Switching Fabric

- Component of packet switching are as follows :
  1. Input ports
  2. Number of output ports
  3. Switching fabric
  4. Routing processor
- Capacity of switch is the maximum rate at which it can move information, assuming all data paths are simultaneously active. Circuit switch must reject call if cannot find a path for samples from input to output . Packet switch must reject a packet if it can find a buffer to store it awaiting access to output trunk.
- Fig. 1.5.1 shows packet switch components.
- In packet switch, physical and data link function are performed by input ports. It constructs the packets from bits and perform error correction and detection.

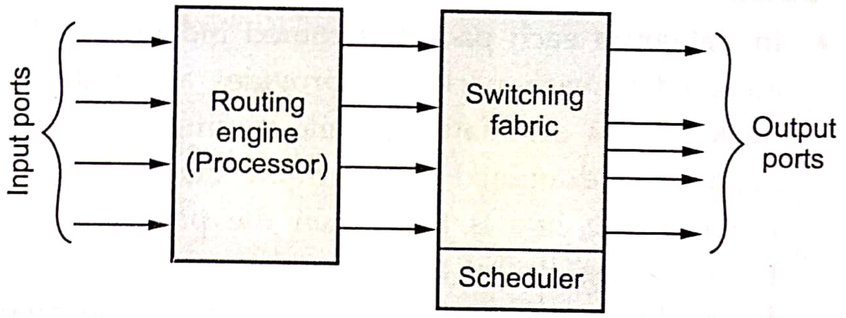


Fig. 1.5.1 Packet switch components

- It transfer data from input to output. It usually consists of links and switching elements.
- The routing engine looks-up the packet address in routing table and determines which output port to send the packet. It performs functions of network layer. Each packet is tagged with port number. The switch uses the tag to send the packet to the proper output port.
- Simplest switch fabric is a shared bus. Switch fabrics are created from certain building blocks of smaller switches arranged in stages.
- The simplest switch is a 2×2 switch, which can be either in the through or crossed position.

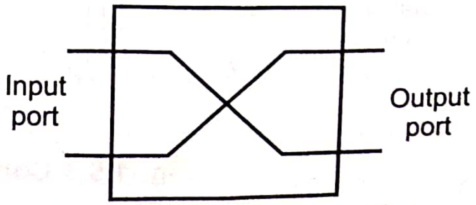


Fig. 1.5.2 Crossed position

1.5.2 Packet Switching

- Packet switching is often used in computer networks where individual users have need of the channel intermittently. While using the channel the application requires high bandwidth, but most of the time, each user does not require that channel at all. Such applications, characterized by a high peak to average requirement for capacity, are called **bursty** and are ideal for packet switching.
- In packet switching, messages are broken into short blocks and interleaved with other messages. Thus, users queue for the channel and share it with one another efficiently. Data is sent in individual packets. Each packet is forwarded from switch to switch, eventually reaching its destination. Each switching node has a small amount of buffer space to temporarily hold packets. If the outgoing line is busy, the packet stay in queue until the line becomes available. Packet switching handles burstly traffic well.
- Packet switching method uses two routing approaches :

  1. **Datagram** and 2. **Virtual circuit.**

1) Datagram Packet Switching

- In **datagram** each packet is routed independently through the network. Header is attached to each packet. It provides all of the information required to route the packet to its destination. While routing the packet, the destination address in the header are examined to determine the next hop in the path to the destination. If the required line is busy then the packet is placed in the queue until the line becomes free. Packet share the transmission line with other packets. Then it deliver to the destination. Datagram approach is also called **connectionless**.
- Disadvantage of datagram approach is a lot of overhead because of independent routing. Another disadvantage is that packet may not arrive in the order at destination in which they were sent.
- Since each packet is routed independently, packets from the same source to the same destination may traverse through different paths. This is shown in Fig. 1.5.3.

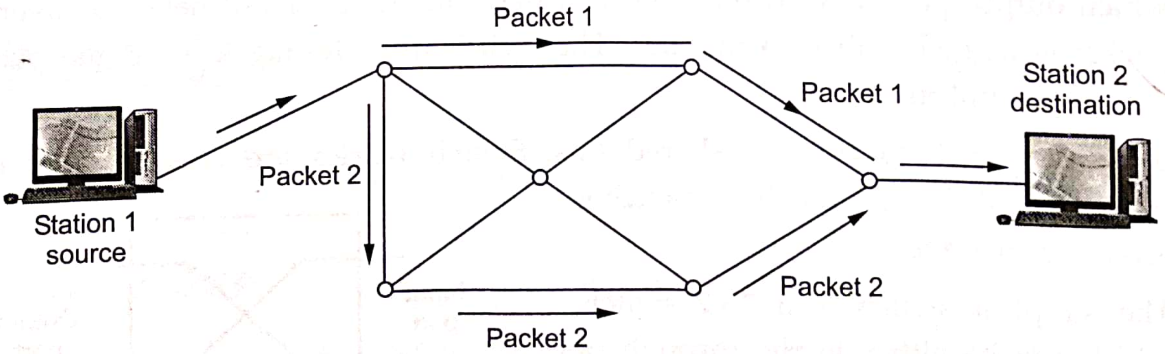


Fig. 1.5.3 Connectionless packet switching

- The packets at station 2 or destination may arrive out of order, and resequencing may be required at the destination. At each node a routing table is maintained which specifies the next hops that is to be taken by packets for the given destination.

2) Virtual Circuit Packet Switching

- In **virtual circuit packet switching** a fixed path between a source and a destination is established prior to transfer of packets.
- Connection-oriented network is also known as **virtual circuit.** Virtual circuit is similar to telephone system. A route, which consists of a logical connection is first established between two users. The connection that is established is not a dedicated path between stations. The path is generally shared by many other virtual connections.
- The process is completed in three main phases -
  - i) Establishment phase.
  - ii) Data transfer phase.
  - iii) Connection release phase.

i) Establishment phase :

- During setting up of logical connection, the two users not only agree to setup a connection between them but also decide upon the quality of service associated with the connection. After this the sequences of packetized information are transmitted bidirectionally between the nodes. The information is delivered to the receiver in the same order as transmitted by sender.

ii) Data transfer phase :

- During this phase it performs flow control and error control services.
- The error control service ensures correct sequencing of packets and correct arrival of packets.
- Flow control service ensures a slow receiver from being overwhelming with data from a faster transmitter.

iii) Connection release :

- When the station wish to close down the virtual circuit, one station can terminate the connection with a clear request packet. Fig. 1.5.4 shows the virtual circuit packet switching.

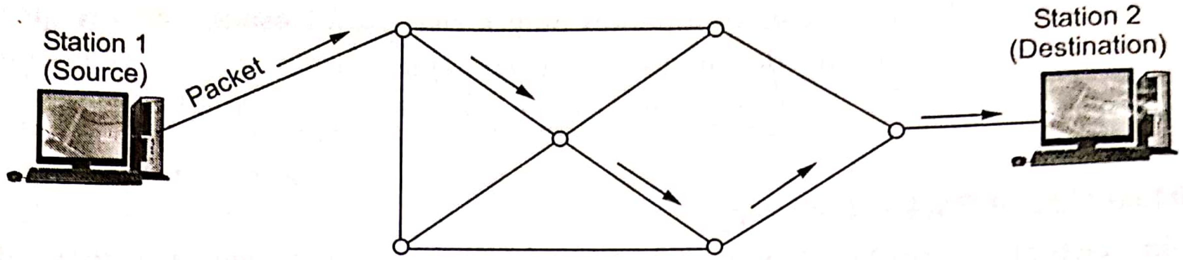


Fig. 1.5.4 Virtual circuit packet switching

1.5.2.1 Advantages of Packet Switching

1. Uses resources more efficiently.
2. Very little setup or tear down time.
3. It is more flexible. i.e. packets can be routed through any switching node.
4. Improved bandwidth.
5. Small sized packet reduces transmission delay.

1.5.2.2 Disadvantages of Packet Switching

1. Complex protocol for packet switching.
2. Algorithms are more complicated.
3. Difficults to bill customers.
4. Switching processor must be powerful.
5. Packets may lost during switching.

1.5.3 Circuit Switching

- The telephone system as it historically developed was designed for voice and analog signals. Sending data requires bandwidth. The amount of bandwidth needed is directly related to the data rate that is desired. An analog voice signal contains its data in a relatively narrow bandwidth, in proportion to the amount of data it carries.
- For voice signals, a relatively large amount of distortion is acceptable, since the human ear can understand voice even with distortion that looks severe to the eye. For digital signals, these distortions may cause the receiver to misinterpret the signal that is sent and so produce an error. The regular telephone loop from the local office to the phone is guaranteed by the phone company to have some specific characteristics. This type of line is the lowest performance line, called voice grade conditioning.
- Similar line characteristics are offered by telephone companies on the lines that go between phone company offices. These interoffice lines are called trunks. Any phone line can connect one user to another user through the phone system, the

user has a line assigned randomly, through the phone offices. This is called the dial-up or switched network.

- Telephone networks are connection oriented because they require the setting up of connection before the actual transfer of information can take place.
- An end-to-end path setup beginning of a session, dedicated to the application, and then released at the end of session. This is called **circuit switching.** Circuit switching is effective for application which make comparatively steady use of channel. Fig. 1.5.5 shows the circuit switching.

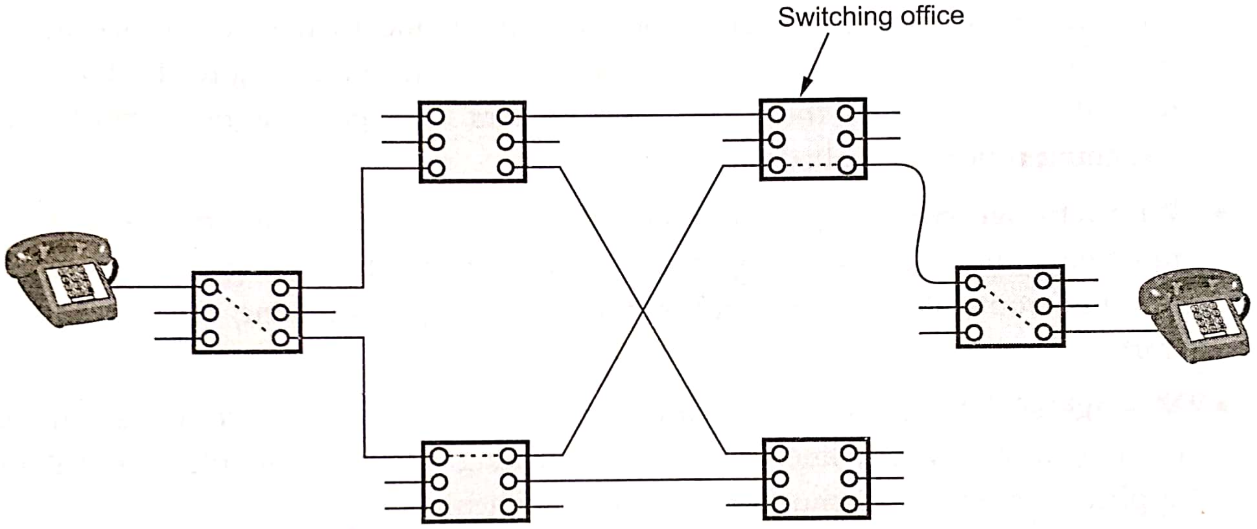


Fig. 1.5.5 Circuit switching

For application which need greater performance than these dial up lines can offer, telephone companies offer specially conditional lines. These lines both from the phone to the office and between phone offices, provide better frequency response and time delay characteristics. This kind of conditioned line is leased by the user. The term dedicated and leased are used when the phone company has set a side a conditional line for a communications link.

Advantages of Circuit Switching

1. Fixed bandwidth, guaranteed capacity.
2. Low variance end to end delay.

Disadvantages

1. Connection setup and tear down introduces extra overhead.
2. User pay for circuit, even when not sending data.
3. Other user cannot use circuit even if it is free of traffic.

1.5.4 Message Switching

- Message switching is used to describe the telegraph network. When this form of switching is used, no physical copper path is established in advance between sender and receiver. When the sender has a block of data to be sent, it is stored in the first switching office i.e. router and then forwarded later, one hope at a time. Each block is received in its entirely, inspected for errors, and then transmitted. A network using this technique is called a **store and forward network.**
- The message was punched on paper tape off line at the sending office and then read in and transmitted over a communication line to the next office along the way, where it was punched out on paper tape. An operator tore the tape off and read it in on one of the many tape readers, one per outgoing trunk. Such a switching office was called a torn tape office.
- With message switching, there is no limit on block size, which means that routers must have disks to buffer long blocks. It also means that a single block may tie up a router, router line for minutes, rendering message switching uses for interactive traffic.
- Message switching does not involve a call setup. It can achieve a high utilization of the transmission line. Message switching is not suitable for interactive applications. Fig. 1.5.6 shows the message switching.

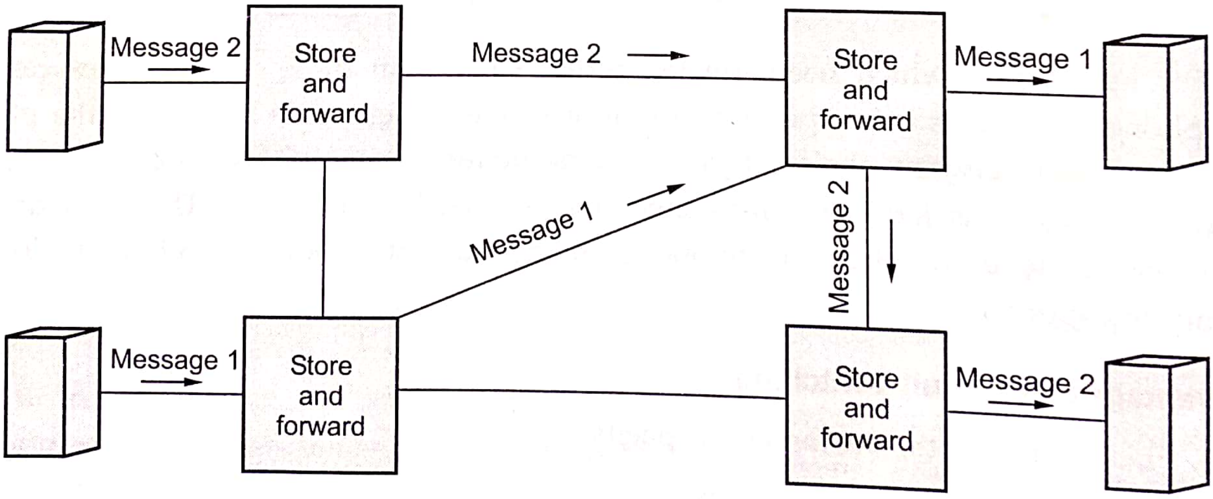


Fig. 1.5.6 Message switching

Advantages of Message Switching

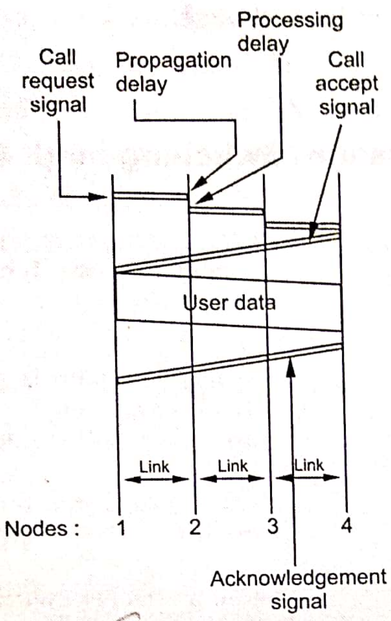
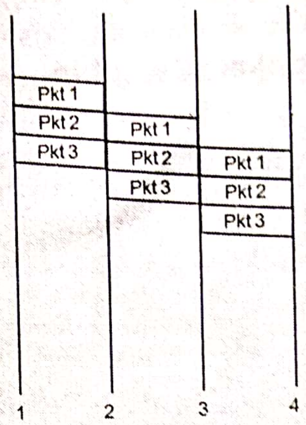
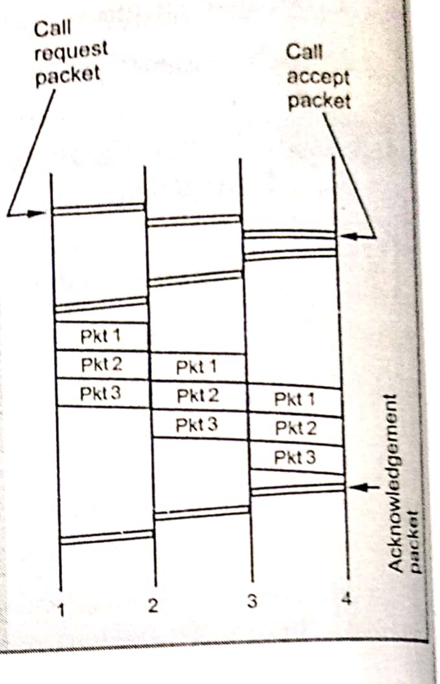
1. Efficient traffic management.
2. Reduces network traffic congenstion.
3. Efficient use of transmission channel.

Disadvantages of Message Switching

1. Because of store and forward, transmission delay is in deduced.
2. Each node requires large capacity for storing.

1.5.5 Comparison of Packet Switching, Message Switching and Circuit Switching

Sr. No.	Circuit switching	Packet switching	Message switching
1.	There is physical connection between transmitter and receiver.	No physical path is established between transmitter and receiver.	No physical path is set in advance between transmitter and receiver.
2.	All the packet uses same path.	Packet travels independently.	Packets are stored and forward.
3.	Needs an end to end path before the data transmission.	No needs of end to end path before data transmission.	Same as packet switching.
4.	Reverses the entire bandwidth in advance.	Does not reserve the bandwidth in advance.	Same as packet switching.
5.	Charge is based on distance and time, but not on traffic.	Charge is based on both number of bytes and connect time.	Charge is based on number of bytes and distance.
6.	Waste of bandwidth is possible.	No waste of bandwidth.	No waste of bandwidth.
7.	Congestion occur for per minute.	Congestion occurs for per packet.	No congestion or very less congestion.
8.	It cannot support store and forward transmission.	It support store and forward transmission.	It also support store and forward transmission.
9.	Not suitable for handling interactive traffic.	Suitable for handling interactive traffic.	Same as circuit switching.
10.	Recording of packet can never happen with circuit switching.	Recording of packet is possible.	Same as packet switching.

11.	Timing diagram  Processing delay Call request signal Propagation delay Call accept signal User data Link Link Link Nodes : 1 2 3 4 Acknowledgement signal	Timing diagram  	Timing diagram  Call request packet Call accept packet Pkt 1 Pkt 2 Pkt 3 Acknowledgement packet 1 2 3 4

1.6 Delay and Loss in Packet-Switched Networks

- A packet during its travel from one node to the subsequent node (host or router) it suffers from different types of delays at each node.
- Some inportant types of delays are :
  1. Processing delay
  2. Queuing delay
  3. Transmission delay
  4. Propagation delay
- All delays accumulated together and result in a larger delay called total nodal delay.

1.6.1 Processing Delay

- Processing delay is a nodal delay and it is defined as the time required examining the packet's header and determining where to direct the packet.
- The processing delay is denoted by d_{proc}.
- Processing delay also include delay due to the time needed to check for bit-level errors in the packet that occurred in transmitting the packet's bits from the upstream router to other router.

1.6.2 Queuing Delay

- After nodal processing delay, the router directs the packet to the queue that precedes the link to subsequent router.
- The queuing delay is denoted by d_{queue}.
- The queuing delay is observed at the queue, the packet experiences a **queuing delay** as it waits to be transmitted over the link.
- The queuing delay of a specific packet depends on earlier-arriving packets that are queued and waiting for transmission across the link.
- The delay of a packet can vary significantly from packet to packet. If the queue is empty and no other packet is currently being transmitted, then packet's queuing delay zero.
- When the traffic heavy and various other packets are waiting to be transmitted, the queuing delay will be long..

1.6.3 Transmission Delay

- The **transmission delay** is defined as the amount of time required to transmit all of the packet bits over the link.
- The transmission delay is denoted by d_{trans}.
- The transmission delay is also called as store-and-forward delay.
- The transmisssion delay is expressed as the ratio of packet length (bits) to transmission rate of the link (bits/sec).

$$\text{Transmission delay} = \frac{\text{Packet length}}{\text{Transmisssion rate}} = \frac{L}{R}$$

1.6.4 Propagation Delay

- The propagation delay is defined as time required by a packet to propagate from transmitting node to the receiving node.
- The propagation delay is denoted by d_{prop}.
- The propagation speed of a packet depends on characteristic of physical medium of the link and the distance between the nodes.

1.6.5 Total Nodal Delay

- The total nodal delay exprienced by a packet is sum of processing delay, queuing delay, transmission delay and propagation delay within a network.
- The total delay is very significant parameter of a network.

$$\boxed{\text{Total nodal delay} = d_{proc} + d_{queue} + d_{trans} + d_{prop}}$$

1.7 Protocol Layers and Their Service Models

- A computer network must provide general, cost effective, fair and robust connectivity among a large number of computers. Designing a network to meet these requirements is no small task.
- To deal with this complexity, network designers have developed general blue prints - usually called network architectures. It guides the design and implementation of networks.

1.7.1 Layered Architecture

- Computer network is designed around the concept of layered protocols or functions. For exchange of data between computers, terminals or other data processing devices, there is data path between two computers, either directly or via a communication network.
- Following factors should be considered.
  1. The source system must either activate the direct data communication path or inform the communication network to the identity of the desired destination system.
  2. Provide for standard interface between network functions.
  3. Provide for symmetry in function performed at each node in the network. Each layer performs the same functions as its counter part in the other node of network.
- The network software is now highly structured.

1.7.2 Protocol Hierarchies

- Most of all networks are organized as a series of layers, each one built upon the one below it. Because of layer, it reduces the design complexity.
- In layer protocols, a layer is a service provider and may consists of several service functions. Function is a sub system of a layer.
- Each subsystem may also be made up of entities. An entity is a specialized module of a layer or subsystem.
- Name of the layer, total number of layer, function and content of each layer differ from network to network.
- Protocols are the rules that govern network communication.

- Fig. 1.7.1 shows the five layer network.

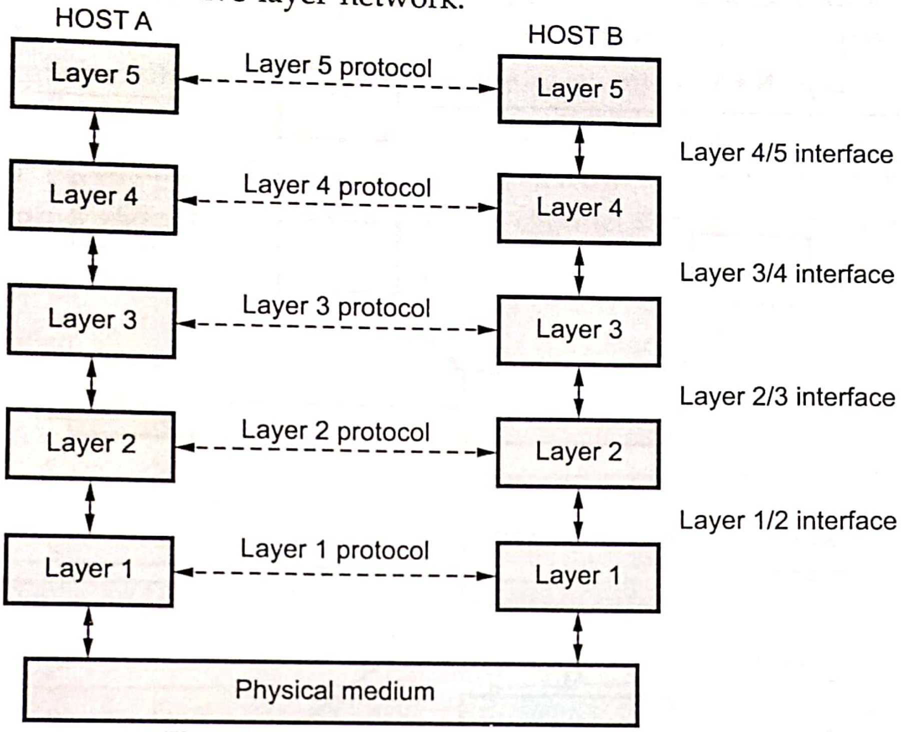


Fig. 1.7.1 Layers, protocols and interfaces

- Layer n on one node carries on a conversation with layer n on other node.
- The entities comprising the corresponding layers on different machine are called **peers.**
- The actual data flow is from upper layer to its below layer and then from physical medium to destination layer.
- Between each pair of adjacent layers is called **interface.** The interface defines which primitive operations and services the lower layer offers to the upper one.
- A set of layers and protocols is called a **network architecture.**

1.7.3 Interfaces and Services

- The process provides a common technique for the layer to communicate with each other. The standard terminology used for layered networks to request services is provided.
- In Fig. 1.7.2 the layers N+1, N and N–1 are involved in the communication process for layer communication, with each other.
- Following components are involved and their function is as follows :

1. Service Data Unit (SDU)
2. Protocol Control Information (PCI)
3. Protocol Data Unit (PDU)
4. Interface Control Information (ICI)
5. Interface Data Unit (IDU)

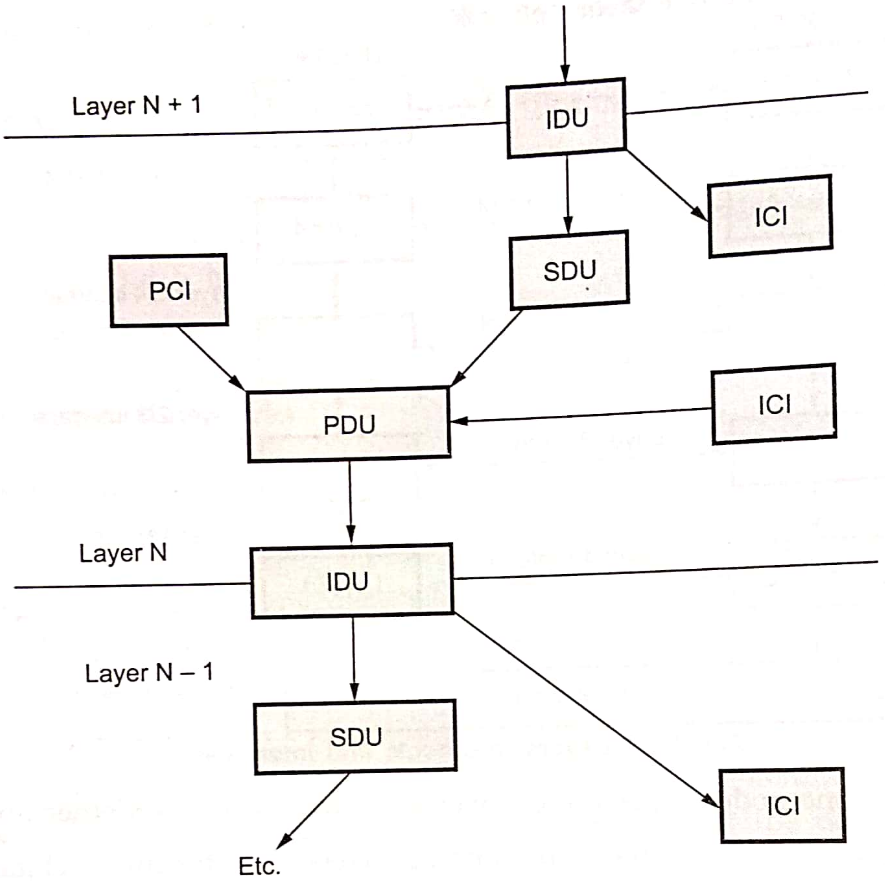


Fig. 1.7.2 Communication between layers

Sr. No.	Name	Function
1.	SDU	Transfer user data by layer N+1 to layer N and N–1.
2.	PCI	To perform service function, it is used to exchange information by peer entities at different sites on the network.
3.	PDU	Combination of the SDU and PCI.
4.	ICI	It passes temporary parameter between N and N–1 to invoke service function.
5.	IDU	The total unit of information transferred across the layer boundaries.

- When the IDU from layer N+1 passes to layer N, it becomes the SDU to that layer. PCI is added to SDU at layer N. ICI performs its function and is discarded. Another ICI is added to PDU at layer N and it becomes IDU to layer N–1. Thus a full protocol unit is passed through each layer.
- Each layer adds header to data. This header is used by the peer layer entity at another node of the network to invoke function. This process repeats itself through each layer.

- As each unit traverses through the layer, it has a header added to it i.e. user data and header (SDU and PCI). This full protocol data unit is passed onto the communication path, where it arrives at the receiving site.
- In short, each layer added its header to user's data and passes to its next layer. This layer process on that data and adds its own header and provides to next layer for processing. Through transmission channel data passes to receiving site.
- Fig. 1.7.3 shows the communication between two sites in a network.

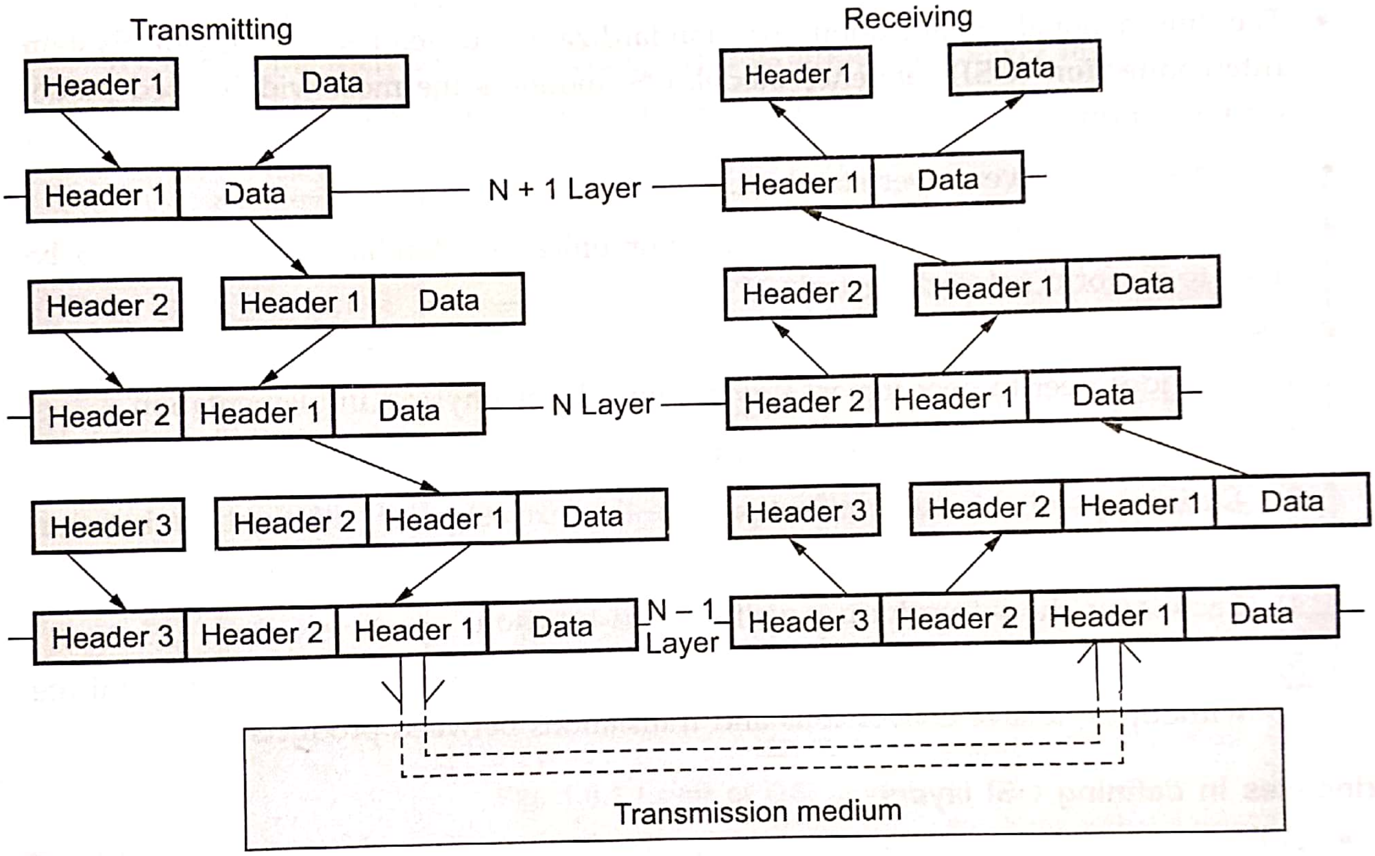


Fig. 1.7.3 Communication between two sites in a network

1.7.4 Relationship of Services to Protocols

- Service interface provides an entry point that users use to access the functionality exposed by the application.
- Service interface is usually network addressable.
- Service interface provides a much more coarse-grained interface while preserving the semantics and finer granularity of the application logic. It also provides a barrier that enables the application logic to change without affecting the users of the interface.
- The service interface should encapsulate all aspects of the network protocol used for communication between the user and service. For example, suppose that a

service is exposed to consumers through HTTP over a TCP/IP network. User can implement the service interface as an ASP.NET component published to a well-known URL.

Q

1.8 OSI Reference Model

Gnct .

GTU : Winter-13,14, Dec.-10,11, Summer-14

- The ISO was one of the first organizations to formally define a common way to connect computers. Their architecture, called the Open System Interconnection (OSI).
- The International organization for standardization developed the **Open System Interconnection (OSI)** reference model. OSI model is the most widely used model for networking.
- OSI model is a seven layer standard.
- The OSI model does not specify the communication standard or protocols to be used to perform networking tasks.
- OSI model provides following services.
  1) Provides peer-to-peer logical services with layer physical implementation.
  2) Provides standards for communication between system.
  3) Defines point of interconnection for the exchange of information between system.
  4) Each layer should perform a well defined function.
  5) Narrows the options in order to increase the ability to communicate without expansive conversions and translations between products.

Principles in defining OSI layers

- Following principles are used in defining the OSI layers.
  1. Do not create so many layers as to make the system engineering task of describing and integrating the layers more difficult than necessary.
  2. Create a boundary at a point where the description of services can be small and the number of interrelations across the boundary are minimized.
  3. Create separate layers to handle function that are manifestly different in the process performed.
  4. Collect similar functions into the same layer.
  5. Select the boundaries at a point which past experience has demonstrated to be successful.
  6. Create a layer of easily localized functions so that the layer could be totally redesigned and its protocols changed in a major way to take advantage of new

advances in architecture, hardware or software technology without changing the services expected from and provided to the adjacent layers.

7. Create a boundary where it may be useful at some points in time to have the corresponding interface standardized.
8. Create a layer where there is a need for a different level of abstraction in the handling of data.
9. Allow changes of functions or protocols to be made within a layer without affecting other layers.
10. Create for each layer boundaries with its upper and lower layer only.

- Fig. 1.8.1 shows the OSI 7 layer reference model.

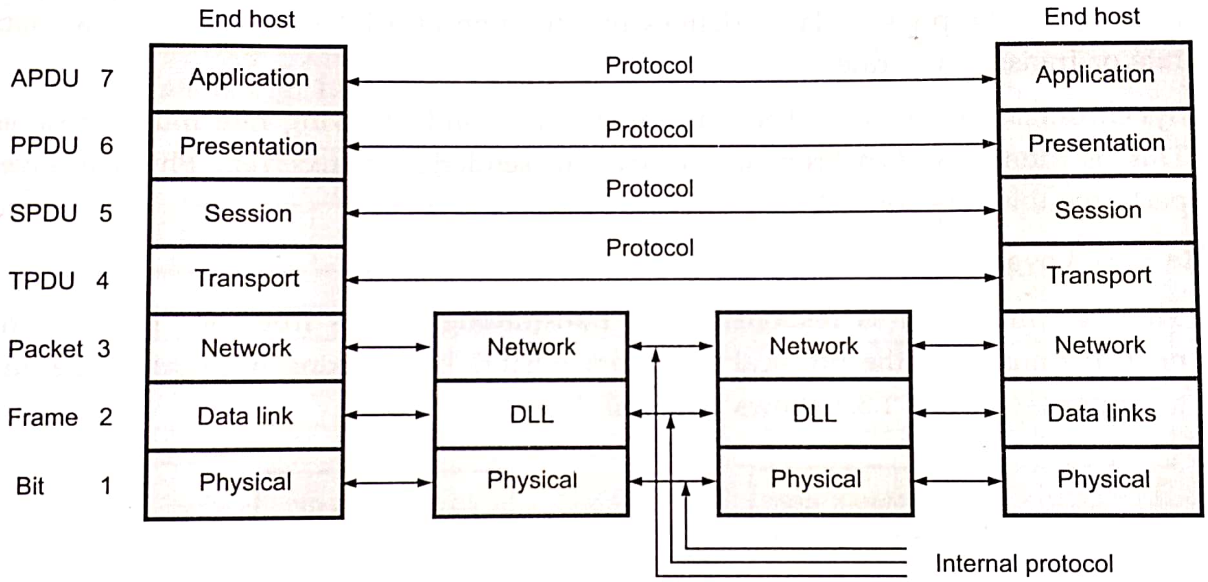


Fig. 1.8.1 Layer of OSI model

1.8.1 Layers in OSI Models

1. Physical Layer

- Physical layer is the lowest layer of the OSI model. Physical layer co-ordinates the functions required to transmit a bit stream over a communication channel. It deals

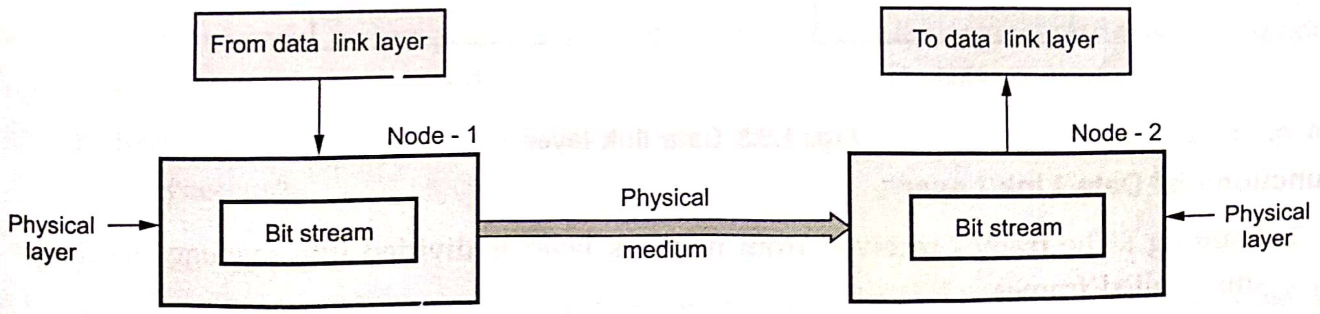


Fig. 1.8.2 Physical layer

with electrical and mechanical specifications of interface and transmission media. It also deals with procedures and functions required for transmission.

- The position of physical layer with transmission medium and the next layer (data link layer) is shown in Fig. 1.8.2

Functions of Physical Layer

1. **Physical characteristics of interfaces and media :** The design issue of physical layer considers the characteristics of interface between devices and transmission media.
2. **Representation of bits :** Physical layer encodes the bit stream into electrical or optical signal.
3. **Data rate :** The physical layer defines the duration of a bit which is called as data rate or transmission rate.
4. **Synchronization of bits :** The transmission rate and receiving rate must be same. This is done by synchronizing clocks at sender and receiver. Physical layer performs this function.

2. Data Link Layer

- The data link layer is responsible for transmitting frames from one node to the next. It transforms the physical layer to a reliable link making it an error free link to upper layer. Fig. 1.8.3 shows data link layer.

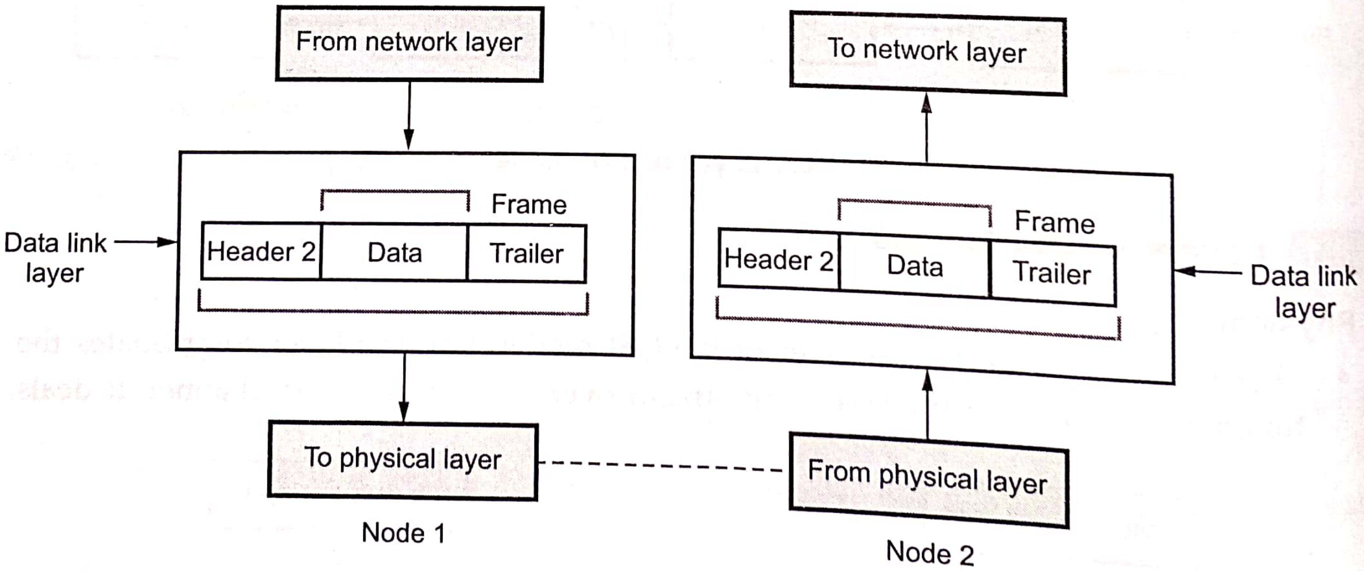


Fig. 1.8.3 Data link layer

Functions of Data Link Layer

1. **Framing :** The frames received from network layer is divided into manageable data units called frames.

2. **Physical addressing :** When frames are to be sent to different LANs, the data link layer adds a header to the frame to define sender or receiver.
3. **Flow control :** When the rate of the data transmitted and rate of data reception by receiver is not same, some data may be lost. The data link layer imposes a flow control mechanism to prevent overwhelming the receiver.
4. **Error control :** Data link layer incorporates reliability to the physical layer by adding mechanism to detect and retransmit damaged or lost frames.
5. **Access control :** When multiple devices are connected to same link, the data link layer determines which device has control over link.

3. Network Layer :

- The network layer is responsible for the delivery of packets from the source to destination. Fig. 1.8.4 shows network layer.

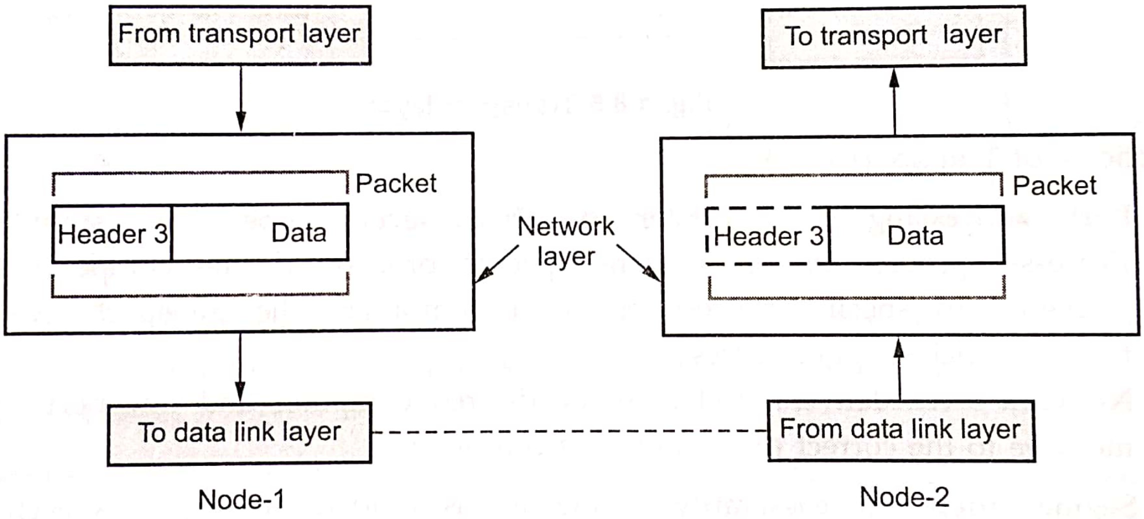


Fig. 1.8.4 Network layer

Functions of Network Layer

1. **Logical addressing :** Data link layer implements physical addressing. When a packet passes network boundary, an addressing system is needed to distinguish source and destination, network layer performs these function. The network layer adds a header to the packet of upper layer includes the logical addresses of sender and receiver.
2. **Routing :** Network layer route or switch the packets to its final destination in an internetwork.

4. Transport Layer :

- The transport layer is responsible for delivery of message from one process to another. The network does the host to destination delivery of individual packets considering it as independent packet. But transport layer ensures that the whole message arrives intact and in order with error control and process control. Fig. 1.8.5 shows transport layer.

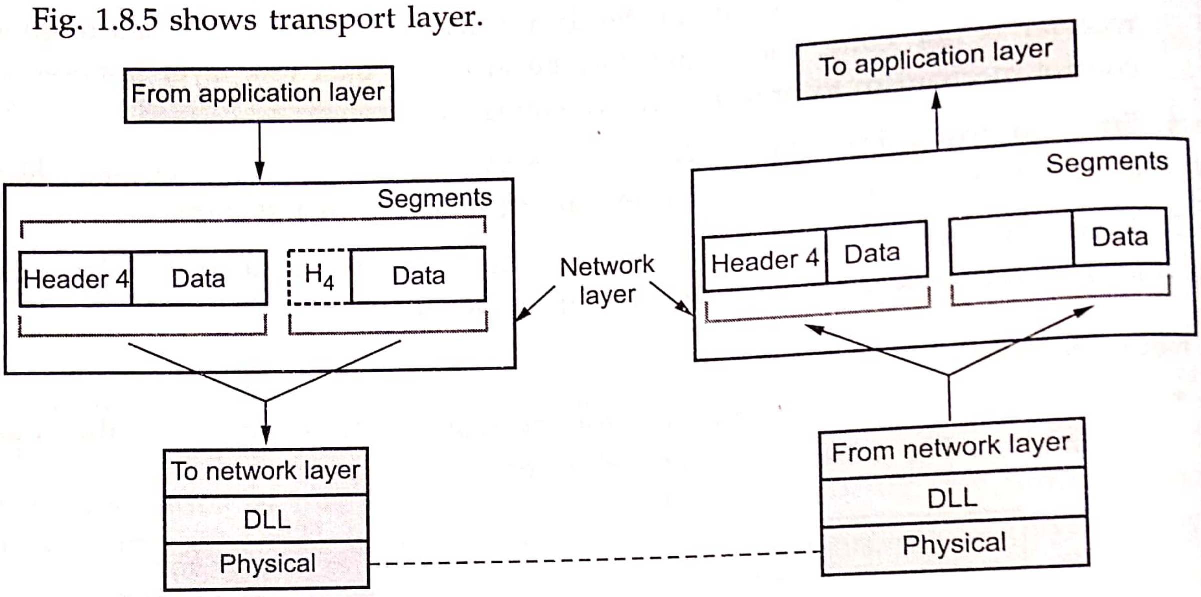


Fig. 1.8.5 Transport layer

Functions of Transport Layer

1. **Port addressing :** Computer performs several operations simultaneously. Process-to-process delivery means specific process of one computer must be delivered to specific process on other computer. The transport layer header therefore include port address.

   Network layer delivers packet to the desired computer and transport layer, gets message to the correct process on that computer.

2. **Segmentation and reassembly :** A message is divided into segments, each segment contains a sequence number which enables transport layer to reassemble at destination.

3. **Connection control :** Transport layer performs connectionless or connection oriented services with the destination machine.

4. **Flow control :** Transport layer performs end-to-end flow control while data link layer performs it across the link.

5. **Error control :** Error control at this layer is performed on end-to-end basis rather than across the link. The transport layer ensures error free transmission.

5. Session Layer :

- The session layer is network dialog controller i.e. it establishes and synchronizes the interaction between communication system. Fig. 1.8.6 shows session layer.

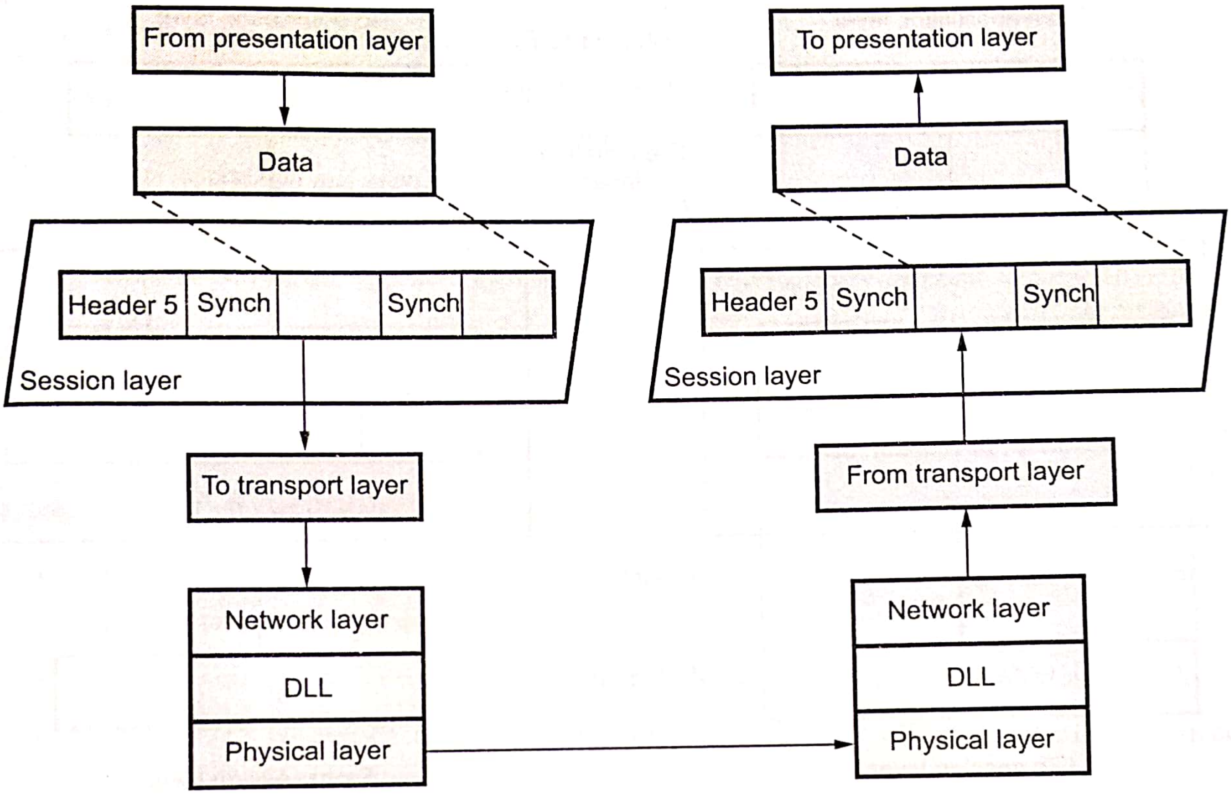


Fig. 1.8.6 Session layer

Functions of Session Layer

1. **Dialog control :** Communication between two processes take place in either half duplex or full-duplex mode. The session layer manages dialog control for this communication.
2. **Synchronization :** Session layer adds synchronization points into stream of data.

6. Presentation Layer :

- The presentation layer deals with syntax and semantics of the information being exchanged. Fig. 1.8.7 shows presentation layer.

Functions of Presentation Layer

1. **Translation :** Different computers use different encoding systems. The presentation layer maintains interoperability between the two encoding systems.
2. **Encryption :** Encryption is transforming sender information to other form to ensure privacy while transmission. Decryption is a reverse process.
3. **Compression :** Compression is a technique of reducing number of bits required to represent the data.

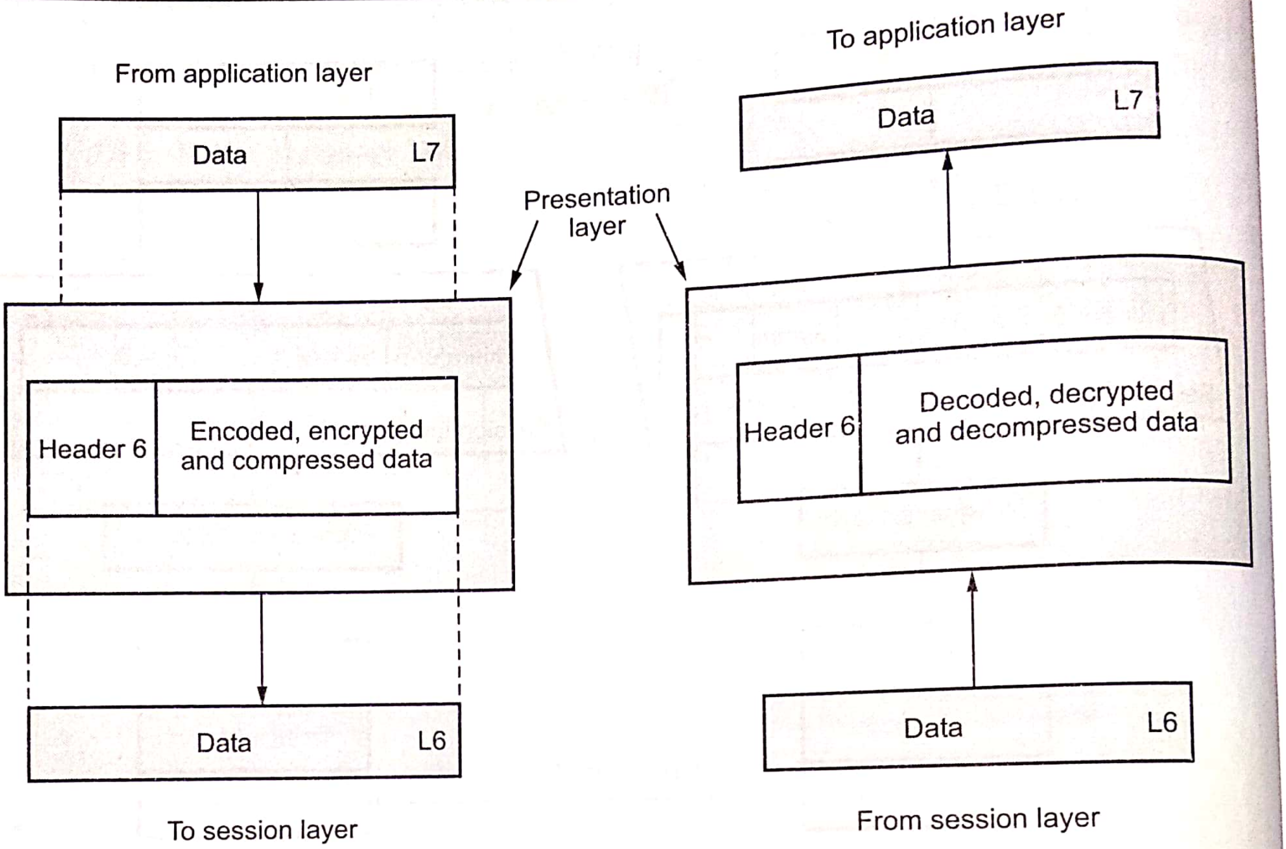


Fig. 1.8.7 Presentation layer

7. Application Layer

- Application layer is responsible for accessing the network by user. It provides user interfaces and other supporting services such as e-mail, remote file access, file transfer, sharing database, message handling (X.400), directory services (X.500).

Functions of Application Layer

1. **Network virtual terminal** : It is a software version of physical terminal that allows a user to log onto a remote host.
2. **File Transfer, Access and Management (FTAM)** : FTAM allows user to access files in remote hosts, to retrieve files and to manage files in remote computer.
3. **Mail services** : E-mail forwarding, storage are the services under this category.
4. **Directory services** : Directory services include access for global information and distributed database.

University Questions

1. *Draw diagram of OSI reference model ? What are the benefits of layering approach in OSI model ?*

GTU : Winter-14, Marks 7

2. *Which of the OSI layers handles each of the following :*
   a) Determine which route through the subnet to use.
   b) Dividing the transmitted bit stream into frames.
   c) Encryption and compression of the information.
   d) Flow control between source and destination node. **GTU : Dec.-10, Marks 4**
3. *What is OSI model ? Draw diagram and explain physical, data link and network layer with its functions.* **GTU : Dec.-11, Marks 5**
4. *Explain for OSI reference model with diagram.* **GTU : Winter-13, Marks 8**
5. *Explain functions of different layers of OSI model.* **GTU : Summer-14, Marks 7**

1.9 TCP/IP Protocol (r/ ed ·)

- The internet architecture, which is also sometimes called the TCP/IP architecture after its two main protocols.
- TCP/IP stands for Transmission Control Protocol / Internet Protocol.
- The TCP/IP reference model is a set of protocols that allow communication across multiple diverse networks.
- TCP/IP is normally considered to be a four layer system. Layers of TCP/IP are Application layer, Transport layer, Internet layer, Host to network layer.
- Host to network layer is also called physical and data link layer.
- The application layer in TCP/IP can be equated with the combination of session, presentation, application layer of the OSI reference model.
- Fig. 1.5.1 shows TCP/IP reference model.
- TCP/IP defines two protocol at transport layer : TCP and UDP.
- **User Datagram Protocol (UDP)** is connectionless protocol.
- UDP is used for application that requires quick but necessarily reliable delivery.
- Internet layer also called **network layer.** Internet layer handles communication from one machine to the other. Routing of packet takes place in internet layer.

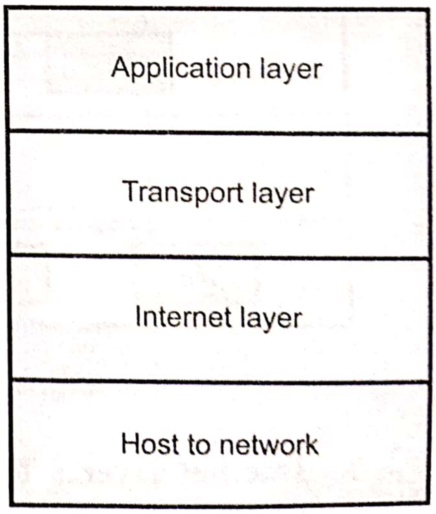


Fig. 1.9.1 TCP/IP reference model

- TCP/IP does not define any specific protocol in host to network layer. This layer is responsible for accpeting and transmitting IP datagrams. This layer normally includes the device driver in the operating system.

- Detailed function of each layer is given below.

1. **Application layer :** Application layer includes all process and services that use the transport layer to deliver data. The most widely known application protocols are : TELNET, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP). TELNET is the Network Terminal Protocol, which provides remote login over the network. FTP is used for interactive file transfer. SMTP delivers the electronic mail.

2. **Transport layer :** Application programs send data to the transport layer protocols TCP and UDP. An application is designed to choose either TCP or UDP based on the services it needs.

- The transport layer provides peer entities on the source and destination hosts to carry on a conversation. Both ends protocol is defined in this layer. TCP is reliable connection oriented protocol that allows a byte stream originating on one computer to be delivered without error or any other computer in the internet. It converts the incoming byte stream into discrete message and passes each one onto the internet layer. At the destination side, the receiving TCP reassembles the received data or messages into the output format. TCP also handles flow control. It synchronizes between fast sender and slow receiver. UDP is a connectionless protocol. Sometimes this type of protocol is used for prompt delivery. The relation of the protocols is shown in the Fig. 1.9.2.

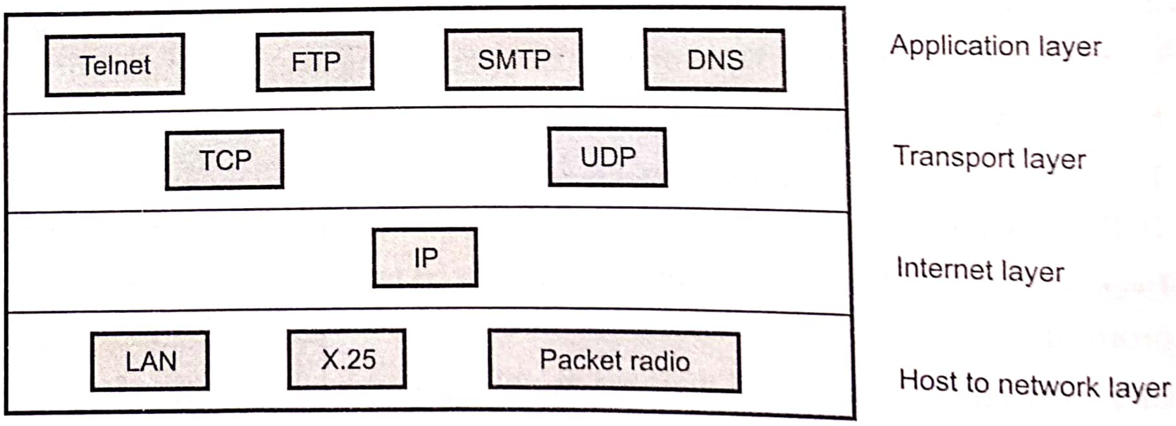


Fig. 1.9.2 Relation of protocol in TCP/IP model

3. **Internet layer :** The Internet network level protocol (IP, ARP, ICMP) handle machine to machine communications.

- These protocols provide for transmission and reception of transport requests and handle network level control. The TCP/IP internet layer moves data from one host to another; even if the hosts are on different networks. The primary protocol used to move data is the Internet Protocol (IP), which provides the following services :

a. **Addressing :** Determining the route to deliver data to the destination host.

b. **Fragmentation :** Breaking the messages into pieces if an intervening network cannot handle a large message.

- It provides a connectionless method of delivering data from one host to another. It does not guarantee delivery and does not provide sequencing of datagrams. It attaches a header to datagram that includes source address and the destination address, both of which are unique internet addresses.

4. **Host to network :** This layer is also called network interface layer. This layer is same as **physical and data link layer** of **OSI model. Host to network layer cannot define any protocol.** It is responsible for accpeting and transmitting IP datagrams. This layer may consist of a device driver in the operating system and the corresponding network interface card in the machine.

1.9.1 Comparison of the OSI and TCP/IP

(CT) (cell)

Fig. 1.9.3 shows the OSI and TCP/IP model.

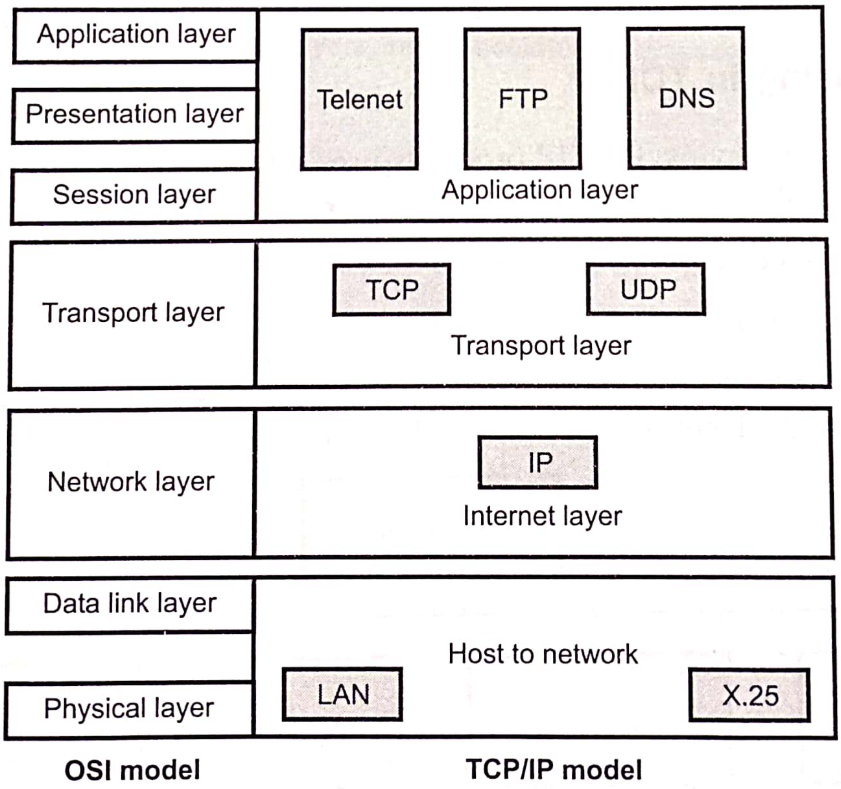


Fig. 1.9.3 OSI and TCP/IP model

Sr. No.	OSI	TCP/IP
1.	7 layers	4 layers
2.	Model was first defined before implementation takes place.	Model defined after protocol were implemented.
3.	OSI model based on three concept i.e. service, interface and protocol.	TCP/IP model did not originally clearly distinguish between service, interface and protocol.
4.	OSI model gives guarantee of reliable delivery of packet.	Transport layer does not always guarantee the reliable delivery of packet.
5.	OSI does not support internet working.	TCP/IP support.
6.	Strict layering.	Lossely layered.
7.	Support connectionless and connection-oriented communication in the network layer.	Support only connection-oriented communication in the transport layer.

1.10 Addressing in TCP/IP

- An Internet employing TCP/IP protocols uses four levels of addresses :
  1. Physical (Link) addresses
  2. Logical (IP) addresses
  3. Port addresses
  4. Specific addresses
- Fig. 1.10.1 shows level of addresses in TCP/IP.

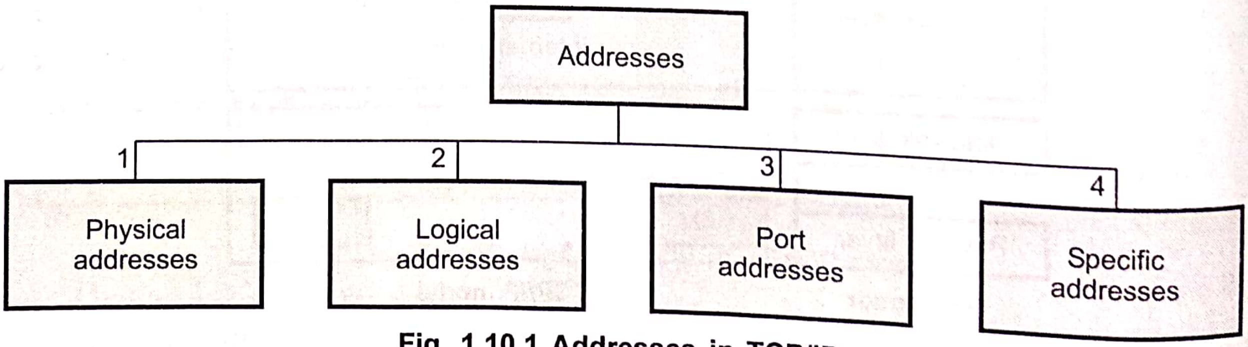


Fig. 1.10.1 Addresses in TCP/IP

- Each address type is related to a specific layer in TCP/IP architecture. Fig. 1.10.2 shows the relationship of layers and addresses in TCP/IP.

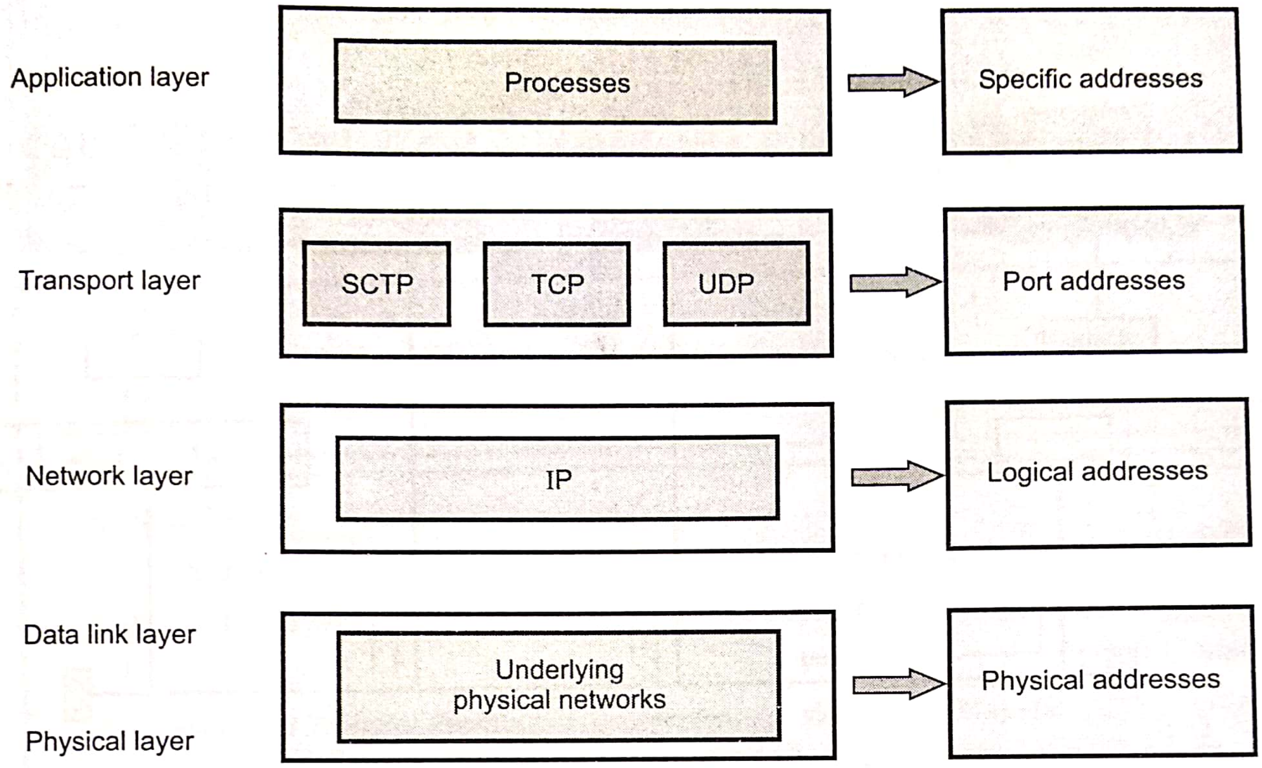


Fig. 1.10.2 TCP/IP layers and associated addresses

1.10.1 Physical Addresses

- The physical address is the lowest level address and is also referred as link address. The physical address of a node is defined by its LAN or WAN. The physical address is included in the frame by the data link layer.
- The size and format of physical addresses vary depending on the network. It has authority over the network. At data link layer, the frame contains physical (link) addresses in the header. The data link layer at sender receives data from upper layer, encapsulates the data in a frame, adds an header and trailer. Only the station having matched address with destination address accepts the frames. The frame is checked, the header and trailer are dropped and data is decapsulated and delivered to upper layer. (See Fig. 1.10.3 on next page)

1.10.2 Logical Addresses

- Logical addresses are independent of underlying physical networks. Since different networks can have different address formats hence a universal address system is required which can identify each host uniquely irrespective of underlying physical networks. Logical addresses are necessary for universal communications. It is a 32-bit address which uniquely defines host connected to Internet.
- The physical addresses changes from hop to hop, but the logical address usually remains the same.

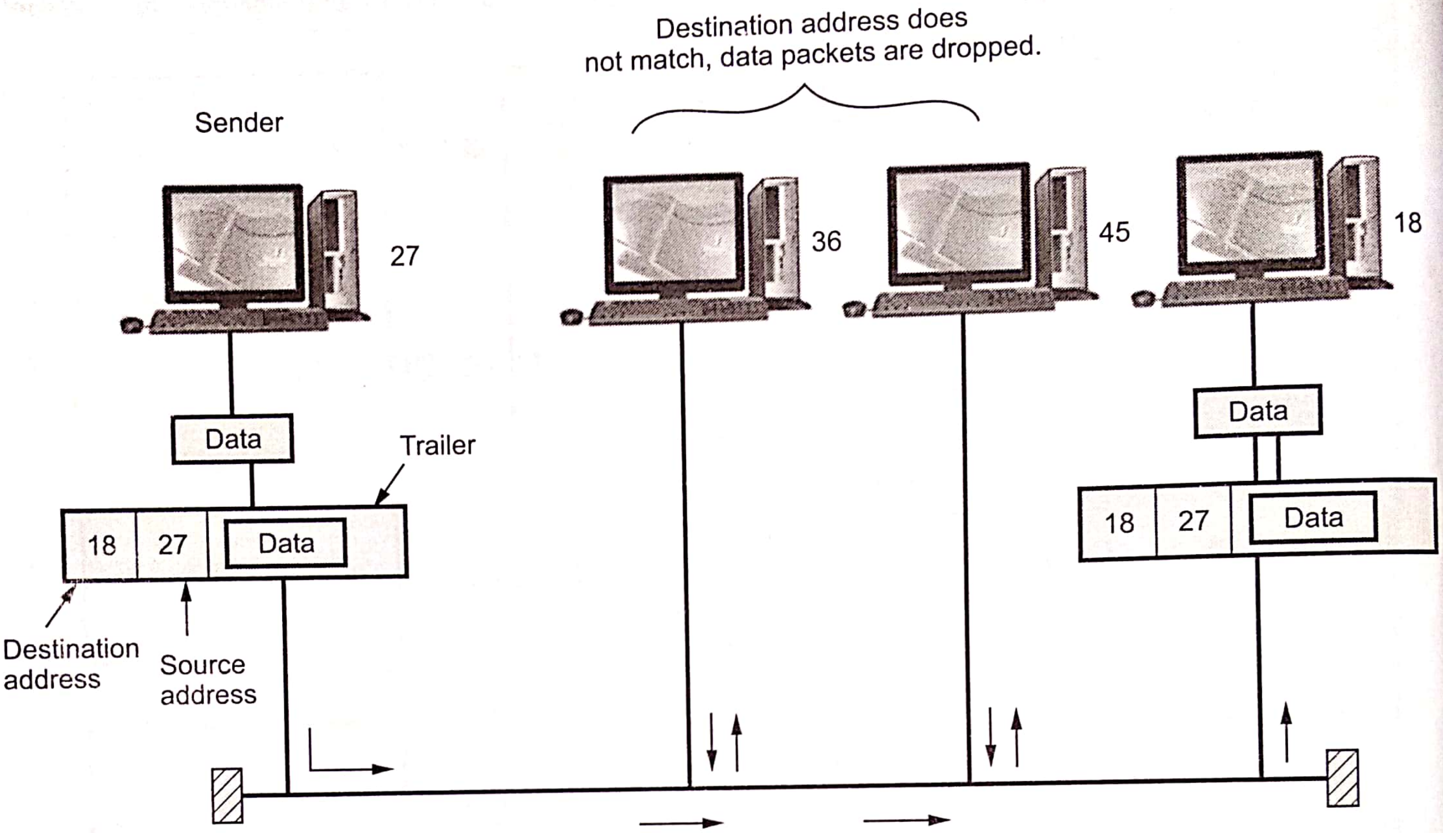


Fig. 1.10.3 Physical addresses

1.10.3 Port Addresses

- The IP address and physical address are necessary for data to travel from source to destination. But a communication process involves TELNET and FTP which requires addresses. In TCP/IP architecture, the label assigned to a process is called port address. In TCP/IP the port address is of 16-bit.

1.10.4 Specific Addresses

- Specific addresses are designed by users for some applications. For example, evilaas@in.com and the Universal Resource Locator (URL), www.vtubooks.com. The first example defines the recipient of e-mail and second example is used to find a document on the world wide web.
- The specific addresses gets changed to corresponding port and logical addresses by the station or host who sends it.

❑❑❑