SWAMI SAHAJANAND COLLEGE OF COMPUTER SCIENCE

BCA Semester – V

Subject : **Data Communication and Networking**

UNIT 4

Network Model

- Switching Technique: Circuit, Packet, and Message Switching
- Layered Tasks: Sender, Receiver.
- OSI Reference Model.
- Connection Less Vs Connection Oriented,
- Reliable Vs Unreliable Connections
- IP Packet Format and IP Addressing(IPV4)

Switching Techniques

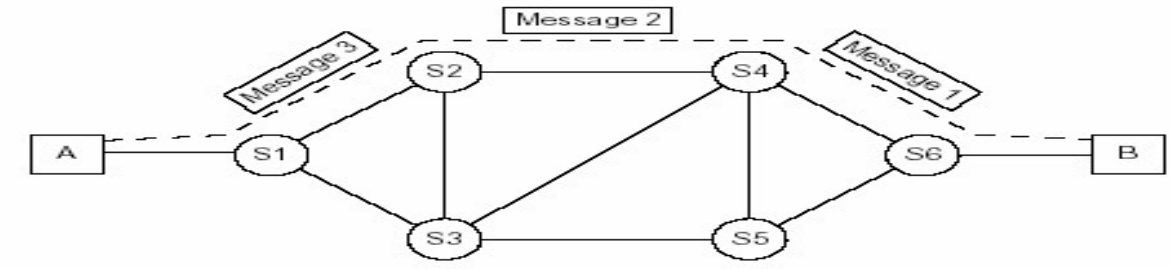
- Switching is a mechanism by which data/information sent from source to destination which are not directly connected.
- Networks have interconnecting devices, which receives data from directly connected sources, stores data, analyze it and then forwards to the next interconnecting device closest to the destination.
- So, Switching techniques are mechanisms for moving data from one network to another.

:: Switching techniques are as follows::

1. Circuit switching 2. Message switching 3. Packet switching

Explain Circuit switching

- Circuit switching is used for Analog Communication.
- Circuit switching establishes dedicated path that remains fixed for the duration of a connection between two stations.
- It has basically 3 phases as circuit establishment, data transfer and circuit disconnect.
- Path is a connected sequence of links between nodes.
- On each physical link, a channel is dedicated to the connection.
- **Example:** Telephone switching equipment establishes a path between two telephones. Connection path is established before transmission begins.
- Thus channel capacity must be available and reserved between each pair of nodes in the path to perform the connection.
- Circuit switching can be inefficient. Channel capacity is dedicated for the duration of a connection, even if no data are being transferred.
- There is a delay prior to data transfer for call establishment, However, once the circuit is established, the network is efficiently transparent to the users.
- The data are transmitted at a fixed rate with no delay.



The actual communication in a circuit-switched network requires 3 phases:

(1) Connection setup **(2)** Data transfer **(3)** Connection terminate.

1. Connection setup :

- Before the 2 or more nodes can communicate, a dedicated circuit needs to be established.
- Connection setup means creating dedicated channels switches.
- Circuit establish based on connection links, measure of availability and cost.

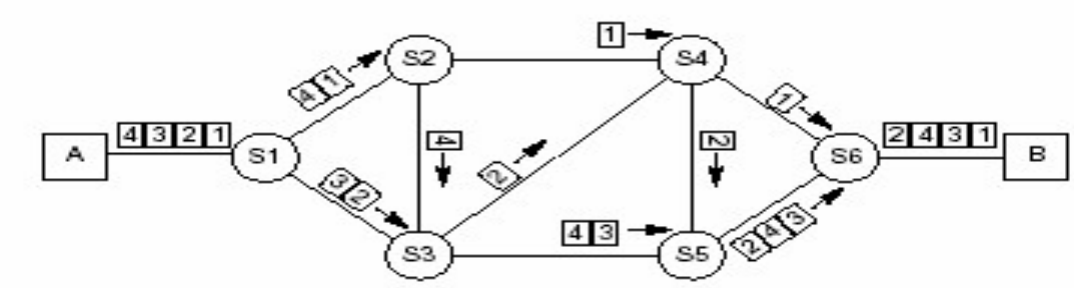
2. Data Transfer :

- After the establishment of the dedicated circuit (channels), the two nodes can transfer data.
- The data may be digital or analog.
- The signaling and transmission may each be either digital or analog. Generally, the connection is full duplex and data may be transmitted in both directions.

3. **Connection Terminate:** When one of the nodes needs to disconnect, Signal is sent to each switch to release the resources.

Explain Packet Switching

- Packet switching can be used as an alternate to circuit switching.
- Packet switching is used for Digital Communication.
- It is used in packet switched networks.
- Data is sent in units that have variable length. They are called as packets.
- There is a maximum limit on the size of packets in a packet switch network.
- In packet switching, messages are divided into smaller pieces called packets.
- The packet contains data and various control information.
- The packet switched networks allow any host to send data to any other host without reserving the circuit.
- Multiple paths between a pair of sender and receiver may exist in a packet switched network.
- Each packet includes source and destination address information so that individual packets can be routed through the internetwork independently.
- The packets that make up a message can take very different routes through the internetwork **(Shown in Figure).**



Advantages of Packet Switching

- ✓ The main advantage of packet switching is the efficiency of the network.
- ✓ The packet switching reduces network bandwidth wastage.
- ✓ Packet switching is highly reliable.
- ✓ The packets can be moved over to other path of the network.
- ✓ All the packets may follow a different route to the destination.

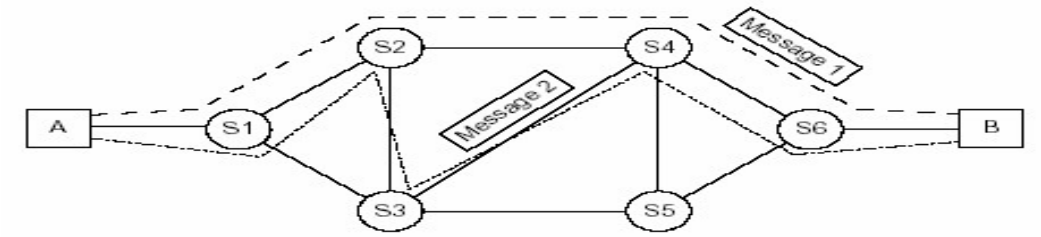
Disadvantages of Packet Switching

- ✓ Packets may be lost on their route, so sequence numbers are required to identify missing packets.
- ✓ Switching nodes requires more processing, as Packet switching protocols are more complex.
- ✓ Switching nodes for packet switching require large amount of memory to handle data.
- ✓ A large data transmission delay occurs.

Explain Message Switching

- A message is a logical unit of information and can be of any length.
- The messages are stored in the switch station's buffer memory and when a line is available the data are forwarded to the appropriate station.
- Message switched networks are called store and forward network.
- If a station wishes to send a message to another station, it first adds the destination address to the message.

- Message switching does not establish a dedicated path between the two communicating devices i.e. no direct link is established between sender and receiver.
- Each message is treated as an independent unit.
- Each complete message is then transmitted from device to device through the internetwork.
- The intermediate node stores the complete message temporarily, inspects it for errors and transmits the message to the next node based on an available free channel and its routing information.
- The actual path taken by the message to its destination is dynamic as the path is established as it travels along.
- When the message reaches a node, the channel on which it came is released for use by another message.
- There is no wait required for the station to open connection and then forward the data.
- Message switching is commonly used in email because some delay is permissible in the delivery of email. Message switching uses relatively low-cost devices to forward messages and can function well with relatively slow communication channels.



Advantages of Message Switching

- ✓ It provides efficient traffic management by assigning priorities to the messages to be switched.
- ✓ No physical connection is required between the source & destination.
- ✓ It reduces the traffic congestion on network because of store & forward facility.
- ✓ Each node can store the message until communication channel becomes available.
- ✓ Channels are used effectively and network devices share the data channels.
- ✓ It supports the message length of unlimited size.

Disadvantages of Message Switching

- ✓ Message length is unlimited, each switching node must have sufficient memory to store message.
- ✓ Storing & forwarding facility introduces delay
- ✓ Not Suitable for real time applications like voice and video.

State the Differences between Circuit Switching & Message Switching

Circuit Switching	Message Switching
➢ Dedicated transmission path	➢ No dedicated transmission path
➢ Continuous transmission of data	➢ Transmission of Message
➢ Path is established for entire conversation	➢ Route is established for each message
➢ Call setup delay	➢ Message Transmission delay
➢ Busy signal if call party is busy	➢ No busy signal
➢ Fixed bandwidth transmission	➢ Dynamic use of bandwidth
➢ No overhead bits after call setup	➢ Overhead bits in each message

Layered Tasks in Network Model: Sender, Receiver and carrier.

- We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail.
- The process of sending a letter to a friend would be complex if there were no services available from the post office. Figure shows the steps in this task.

Sender, Receiver, and Carrier

- In Figure we have a sender, a receiver, and a carrier that transports the letter. There is a hierarchy of tasks in a network model.

At the Sender Site :

Let us first describe, in order, the activities that take place at the sender site.

Higher layer.

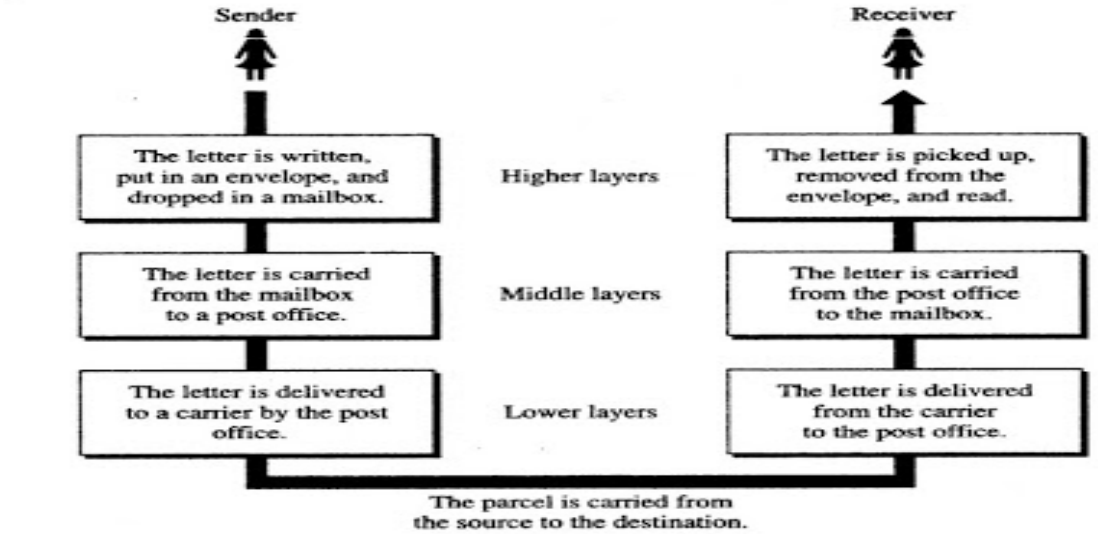
The sender writes the letter, inserts the letter in an envelope, writes the sender and receiver addresses, and drops the letter in a mailbox.

Middle layer.

The letter is picked up by a letter carrier and delivered to the post office.

Lower layer.

The letter is sorted at the post office; a carrier transports the letter.



On the Way :

The letter is then on its way to the recipient. On the way to the recipient's local post office, the letter may actually go through a central office.

At the Receiver Site :

Lower layer.

The carrier transports the letter to the post office.

Middle layer.

The letter is sorted and delivered to the recipient's mailbox.

Higher layer.

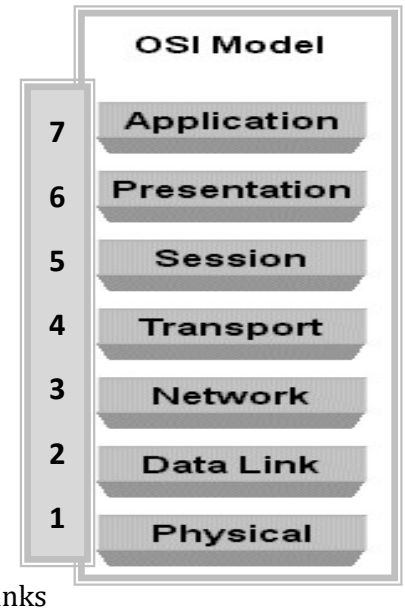
The receiver picks up the letter, opens the envelope, and reads it.

OSI REFERANCE MODEL

Introduction

- It is developed by International Standards Organization (ISO).
- It is a step towards international standardization of the protocols used in the networking.

- The model is called OSI (Open System Interconnection) because, systems that are open for communication with other systems.
- OSI is not a physical model; it is a set of guidelines.
- It provides framework for creating and implementing networking standards, devices, internetworking scheme.



(Layer -1) Physical Layer:

- This layer defines the electrical characteristics of the signals used to transmit the data, Physical characteristics of the network such as the type of cable, connectors, and the length of the cable.
- The physical layer transmits the binary data (bits) as signals depending on medium.
- **Function** - Line configuration, Transmission Modes (Simplex, Half/Full-Duplex).

(Layer -2) Data Link Layer:

- This layer defines how the signal will be placed and sets up links across the physical network.
- Encapsulate packets into network frames.
- It has 2 sub-layers, Logical Link Control (LLC) and Media Access Control Layer (MAC).
- If an acknowledgement is expected and not received, the frame will be resent.
- **Function:** Framing **-** Combine Packets into Bytes and bytes into Frame, Physical Addressing, Flow control, Access control, Error detection and correction**.**

(Layer -3) Network Layer:

- The network layer is concerned with Addressing and Routing.
- IP addresses are translated into physical addresses (MAC Address) and Vice-Versa for transmission at the network layer.
- The network layer also determines the Route from the source to the destination computer to deliver packets. Routes are determined based on Routing Algorithm.
- Traffic control measures are also implemented at the network layer.
- **Function: Routing,** Provides Logical addressing which router used for path determination.

(Layer -4) Transport Layer:

- The transport layer is responsible for the control of flow and ensuring that messages are delivered error free from source -to-destination (end-to-end).
- On the source side, messages are packaged for efficient transmission and assigned a tracking number.
- On the receiving side, the packets are re-assembled, checked for errors, and acknowledged.
- The transport layer performs error handling by ensuring that all data is received in the proper sequence without errors. If there are errors the data is retransmitted.
- **Function:** End-to-End Connection, Error correction, Connection control**.**

(Layer -5) Session Layer:

- The session layer is responsible for establishing, managing, and terminating a connection called session.
- A session is an exchange of messages between computers. Logon, name recognition and security functions occur while establishing a session.
- Managing the session involves synchronization of user tasks and messages.
- **Function**: Keeps different application data separate, Dialog control, Synchronization

(Layer -6) Presentation Layer:

- This layer converts incoming and outgoing data from one presentation format to another.
- This layer is concern with the syntax and semantics, translating, interpreting, and converting the data from various formats that exchanged between 2 systems.
- Encryption techniques are also implemented at the presentation layer.
- **Function:** Present Data, Encryption, Compression and Translation Services

(Layer -7) Application Layer:

- This layer provides the operational system with direct access to the network services.
- It also provides an interface so that Application (Web Browser) that are running on the local machine can access the network services. So It enables user/software to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

Difference between Connection Less & Connection Oriented

- Communication can be established in two ways between two or more devices.
- These are connection-oriented and connection-less.

BASIS OF COMPARISON	CONNECTION-ORIENTED SERVICE	CONNECTION-LESS SERVICE
Connection	It involves establishment and termination of the connection.	It doesn't require any connection creation and termination processes for transferring data.
Data	Uses stream of data and is at risk to router failure	It uses messages and is robust to router failure
Prior Connection Requirement	Necessary	Not Necessary
Reliability	Ensures Reliable transfer of data.	Not Reliable.
Congestion	Uncertain	Occur possible.
Transferring mode	Using circuit switching.	Using Packet switching.
Lost data retransmission	Possible	Not possible.
Suitability	Suitable for long and steady communication.	Suitable for small size Transmission.
Signaling	Used for connection establishment.	There is no concept of signaling.
Packet forwarding	Packets sequentially travel to their destination node and follow the same route.	Packets reach the destination randomly without following the same route.
Delay	Long Delay. Data transmission Slower	Very short Delay. Data transmission Faster

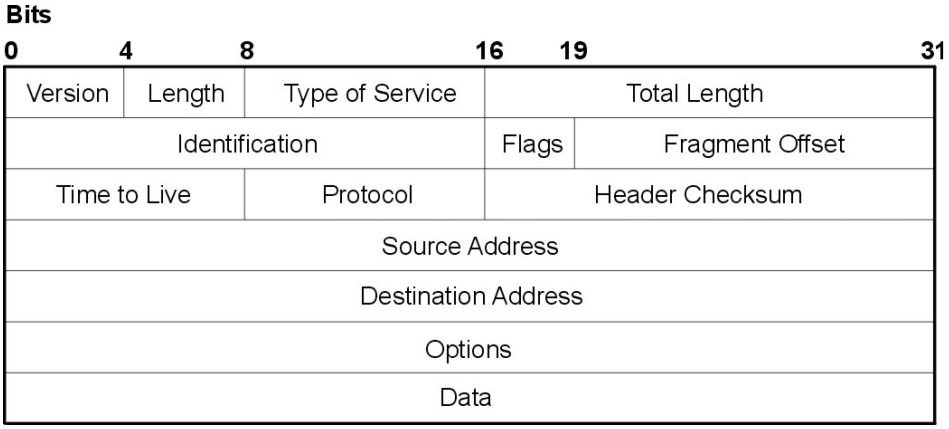
IP Protocol, IP Packet Format, IP Addressing

What Is IP protocol? Explain

- IP protocol is one of the main protocols in the TCP/IP stack.
- The most widely used version of IP today is Internet Protocol Version 4 (IPv4). However, IP Version 6 (IPv6) is also supported.
- It is in the form of IP datagrams that all the TCP, UDP, ICMP and IGMP data travels over the network.
- IP is connection less and unreliable protocol. It is connection less in the sense that no state related to IP datagrams is maintained either on source or destination side.
- IP is unreliable in the sense that it not guaranteed that an IP data gram will get delivered to the destination or not.
- If an IP datagram encounters some error at the destination or at some intermediate host (while traveling from source to destination) then the IP datagram is generally discarded and an ICMP error message is sent back to the source**.**

Explain - IP Packet Format

The TCP/IP Version 4 packet is composed of a number of different fields that can be used by the source and intermediary devices to determine the way a specific packet is treated when being transported. Figure shows the structure of the packet.



(1) Version Field (4 bits)

- It indicates Version of IP. There are 2 versions of TCP/IP used in networks, (1) IPV4) and (2) IPV6.

(2) Length (4 bits)

- It is used to indicate the total length of the IP packet including the data.
- This field is represented in octets (8 bits) and is provided a total of 16 bits in the header.

(3) Type of Service (TOS) (8 bits)

- This field is used to define value with Quality of Service (QoS) parameters for the packet.

(4) Total Length (IHL) (16 bits)

- The minimum valid value for the IHL 160 bits for IPV4.
- It includes IHL, TOS, Length, Identification, Flags, Fragment Offset, TTL, Protocol, Checksum, and Source and Destination Addresses.

(5) Identification (16 bits)

- The Identification field is used to identify specific packets when they are being reassembled from fragments.
- For fragmented packets, the value is the same across all of the fragments and is used by the destination device to reassemble the data.

(6) Flags (3 bits)

- The Flags field is used to control how a specific IP packet is treated by a device.
- The field is 3 bits and is formatted as follows:
  - First bit is always = 0
  - Second bit (0 = Packet is fragmented, 1 - Packet is NOT fragmented)
  - Third bit is the 'location' of a packet in a series of fragmented packets

    A value of 0 = packet is the last fragment in a series.

    A value of 1 = means that the packet is not the last fragment in a series

(7) Fragment Offset (13 bits)

- This field is used to indicate that packet is being reassembled at the destination device.
- The Fragment Offset, along with the Identification field, is used to identify packets that have been fragmented and reassemble them in the correct order.

(8)Time to Live (TTL) (8 bits)

- The TTL field is used to limit the amount of time that a packet is allowed to exist on the "network".
- It maintains a counter that gradually decrements down to 0, at which point the datagram is discarded.

(9) Protocol (8 bits)

- Indicates which upper-layer protocol receives incoming packets after processing is complete.

(10) Header Checksum (16 bits)

- This field helps to ensure IP header integrity.
- The Checksum field is computed for only the packet header.
- Checksum provides a method of verifying that the header has not been corrupted when being transmitted from one device to another.

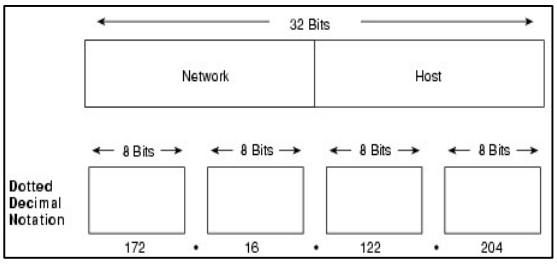
(11 & 12) Source Address and Destination Address (32 bits)

- Both the Source and Destination Address fields are 32 bits and indicate the source and destination IP addresses.

(13) Options (+ Padding) It is an optional field is not typically used.

(14) Data: Data or message, variable in length, can contain any number of different protocols.

Explain :- IP Address Scheme (Classification of IP Address)



- It is also known as Logical Addressing Scheme.
- It is based in Internet Protocol Version 4 (IPV4).
- It is 32 bit long, grouped into 8 bits, separated by dots, in decimal format (known as dotted decimal notation).
- Each bit in the octet (8 bit) has a binary weight (128, 64, 32, 16, 8, 4, 2, 1).
- The minimum value for an octet is 0, and the maximum value for an octet is 255.
- These IP addresses then classified as "**Class: *A, B,C, D, and E.***
- Only classes A, B, and C are available for commercial use.

Class A Addresses:

- Class A address must be between 0 and 127.
- This 1st byte is assigned to the network address, and remaining 3 bytes are used for host addresses. Class A format is: **Network. Host. Host. Host.**
- It is used for Large Size Enterprise Network and Internet.
- Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (22^4-2).

- **LoopBack Address**: The IP address range 127.0.0.0 – 127.255.255.255 is reserved for loopback, i.e. a Host's self-address.

Class B Addresses

- Class B addresses must be between 128 and 191.
- This 1st & 2nd byte is assigned to the network address, and 3rd & 4th bytes are used for Host addresses.
- Thus, Class B format is as follows: **Network . Network . Host . Host.**
- It is used for Medium Size Enterprise Network and Intranet.
- Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses.

Class C Addresses

- Class C addresses must be between 192 and 223.
- The 1st, 2nd & 3rd byte is assigned to the network address, and 4th byte is used for host addresses.
- Thus, Class C format is as follows: N**etwork . Network . Network . Host.**
- It is used for Small Size Network.
- Class C gives 2097152 (2^{21}) Network addresses and 254 (2^{8}-2) Host addresses

Class D Address

- Class D addresses must be between 224 and 239.
- Class D is reserved for Multicasting.
- In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address.
- Class D does not have any subnet mask.

Class E Address

- Class E addresses must be between 240 and 255.
- This IP Class is reserved for experimental purposes, R&D or Study.
- Class E does not set with any subnet mask.

CLASS	Purpose	Network & Address Range	Format	No. Bits Network/ Host	Max. Hosts
A	Large Oorganizations	**1**.0.0.0 to **126**.0.0.0	N.H.H.H	7/24	16777214 (2^{24} - 2)
B	Medium-size organizations	**128**.1.0.0 to **191**.254.0.0	N.N.H.H	14/16	65534 (2^{16} - 2)
C	Relatively small organizations	**192**.0.1.0 to **223**.255.254.0	N.N.N.H	21/8	254 (2^{8} - 2)
D	Multicast groups	**224**.0.0.0 to **239**.255.255.255	N/A	N/A	N/A
E	Experimental	**240**.0.0.0 to **254**.255.255.255	N/A	N/A	N/A