UNIT 2 Data Link Layer

CO 1 Explain Basic concept, OSI reference Model. Services .Role of each layer in OSI Model. TCP/IP. Network devices. Transmission Media, Analog and Digital Transmission

CO 2 Apply Channel allocation . Framing. Frame control and Error Control Techniques

CO 3 Describe the function of Network Layer, Logical addressing and Subletting, Routing Mechanism

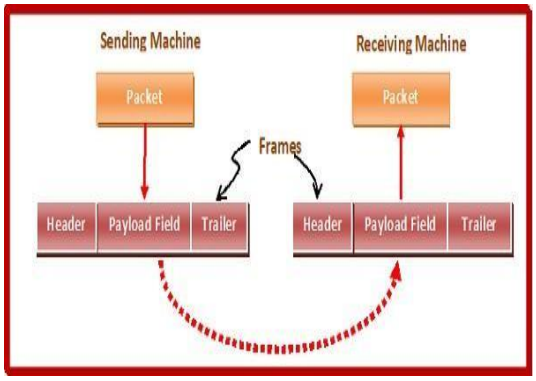
CO 4 Explain the function of Session and Presentation Layer.

CO 5 Explain different Protocol used at different Application layer HTTP.SNMP..FTP.TELNET. VPN

1.1 Framing in Data Link Layer

Data-link layer takes the packets from the Network Layer and encapsulates them into frames. If the frame size becomes too large, then the packet may be divided into small sized frames. Smaller sized frames make flow control and error control more efficient.

Then, it sends each frame bit-by-bit on the hardware. At receiver's end, data link layer picks up signals from hardware and assembles them into frames.



Parts of a Frame

A frame has the following parts −

Frame Header − It contains the source and the destination addresses of the frame.

Payload field − It contains the message to be delivered.

Trailer − It contains the error detection and error correction bits.

Flag − It marks the beginning and end of the frame.

Types of Framing

Framing can be of two types, fixed sized framing and variable sized framing.

Fixed-sized Framing

Here the size of the frame is fixed and so the frame length acts as delimiter of the frame. Consequently, it does not require additional boundary bits to identify the start and end of the frame.

Example-ATM cells.

Variable – Sized Framing

Here, the size of each frame to be transmitted may be different. So additional mechanisms are kept to mark the end of one frame and the beginning of the next frame.

It is used in local area networks.

Two ways to define frame delimiters in variable sized framing are −

Length Field − Here, a length field is used that determines the size of the frame. It is used in Ethernet (IEEE 802.3).

1.2 Simplex Protocol

The Simplex protocol is hypothetical protocol designed for unidirectional data transmission over an ideal channel, i.e. a channel through which transmission can never go wrong. It has distinct procedures for sender and receiver. The sender simply sends all its data available onto the channel as soon as they are available its buffer. The receiver is assumed to process all incoming data instantly. It is hypothetical since it does not handle flow control or error control.

Stop – and – Wait Protocol

Stop – and – Wait protocol is for noiseless channel too. It provides unidirectional data transmission without any error control facilities. However, it provides for flow control so that a fast sender does not drown a slow receiver. The receiver has a finite buffer size with finite processing speed. The sender can send a frame only when it has received indication from the receiver that it is available for further data processing.

Stop – and – Wait ARQ

Stop – and – wait Automatic Repeat Request (Stop – and – Wait ARQ) is a variation of the above protocol with added error control mechanisms, appropriate for noisy channels. The sender keeps a copy of the sent frame. It then waits for a finite time to receive a positive acknowledgement from receiver. If the timer expires or a negative acknowledgement is received, the frame is retransmitted. If a positive acknowledgement is received then the next frame is sent.

Go – Back – N ARQ

Go – Back – N ARQ provides for sending multiple frames before receiving the acknowledgement for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgement of a frame is not received within the time period, all frames starting from that frame are retransmitted.

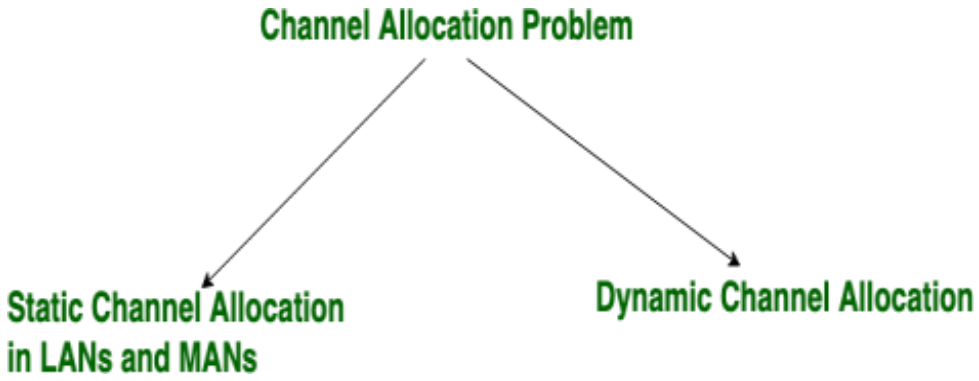
Selective Repeat ARQ

This protocol also provides for sending multiple frames before receiving the acknowledgement for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

1.3 Channel Allocation

Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. There are user's quantity may vary every time the process takes place. If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion. If the number of users are small and don't vary at times, then Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.

Channel allocation problem can be solved by two schemes: Static Channel Allocation in LANs and MANs, and Dynamic Channel Allocation.



These are explained as following below.

1. Static Channel Allocation in LANs and MANs:
It is the classical or traditional approach of allocating a single channel among multiple competing users using Frequency Division Multiplexing (FDM). if there are N users, the frequency channel is divided into N equal sized portions (bandwidth), each user being assigned one portion. since each user has a private frequency band, there is no interference between users.
It is not efficient to divide into fixed number of chunks.

2. Dynamic Channel Allocation:
Possible assumptions include:

1. Station Model:
   Assumes that each of N stations independently produce frames. The probability of producing a packet in the interval IDt where I is the constant arrival rate of new frames.

2. Single Channel Assumption:
   In this allocation all stations are equivalent and can send and receive on that channel.

3. Collision Assumption:
   If two frames overlap in time-wise, then that's collision. Any collision is an error, and both frames must re transmitted. Collisions are only possible error.

4. Time can be divided into Slotted or Continuous.

5. Stations can sense a channel is busy before they try it.

1.4 Multiple Access Protocols

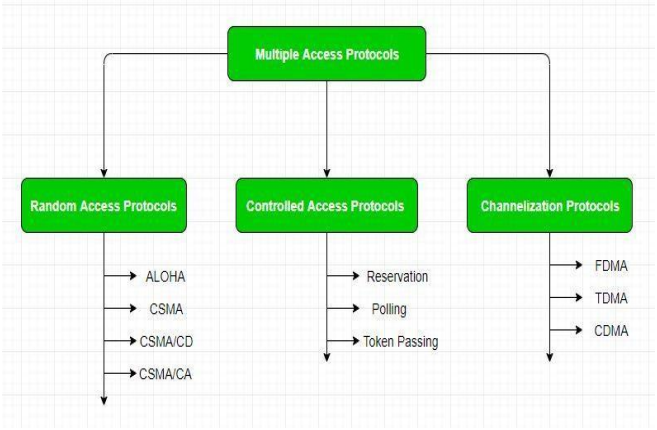
The Data Link Layer is responsible for transmission of data between two nodes. Its main functions are-

- Data Link Control
- Multiple Access Control

- Data Link control –
- The data link control is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control and flow control.

- Multiple Access Control –
- If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk. For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created (data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.

- Thus, protocols are required for sharing data on non dedicated channels. Multiple access protocols can be subdivided further as –



1. Random Access Protocol: In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state(idle or busy). It has two features:

1. There is no fixed time for sending data
2. There is no fixed sequence of stations sending data

The Random access protocols are further subdivided as:

ALOHA – It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

- **Pure Aloha:**
  When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.
  Vulnerable Time = 2* Frame transmission time

Throughput = G exp{-2*G}

Maximum throughput = 0.184 for G=0.5

- **Slotted Aloha:**
  It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

Vulnerable Time = Frame transmission time

Throughput = G exp{-*G}

Maximum throughput = 0.368 for G=1

b) CSMA – Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium.If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA access modes-

- 1-persistent: The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.
- Non-Persistent: The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- P-persistent: The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.
- O-persistent: Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

(c)CSMA/CD – Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected.

(d) CSMA/CA – Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal (its own) then the data is successfully sent but if there are two signals (its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case.

CSMA/CA avoids collision by:

1. Interframe space – Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.
2. Contention Window – It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process,

rather it restarts the timer when the channel is found idle again.

3. Acknowledgement – The sender re-transmits the data if acknowledgement is not received before time-out.

2. Controlled Access:

In this, the data is sent by that station which is approved by all other stations.

3. Channelization:

In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

- Frequency Division Multiple Access (FDMA) – The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no two bands overlap to avoid crosstalk and noise.
- Time Division Multiple Access (TDMA) – In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.
- Code Division Multiple Access (CDMA) – One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly, data from different stations can be transmitted simultaneously in different code languages.
- Orthogonal Frequency Division Multiple Access (OFDMA) – In OFDMA the available bandwidth is divided into small subcarriers in order to increase the overall performance, Now the data is transmitted through these small subcarriers. it is widely used in the 5G technology.

Advantages:

- Increase in efficiency
- High data rates
- Good for multimedia traffic

Disadvantages:

- Complex to implement
- High peak to power ratio

Spatial Division Multiple Access (SDMA) – SDMA uses multiple antennas at the transmitter and receiver to separate the signals of multiple users that are located in different spatial directions. This technique is commonly used in MIMO (Multiple-Input, Multiple-Output) wireless communication systems.

Advantages :

- Frequency band uses effectively
- The overall signal quality will be improved
- The overall data rate will be increased

- **Disadvantages:**
- It is complex to implement
- It require the accurate information about the channel

- ## Switching

- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as switching.
- Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- Network switches operate at layer 2 (Data link layer) in the OSI model.
- Switching is transparent to the user and does not require any configuration in the home network.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.
- It is operated in full duplex mode.
- Packet collision is minimum as it directly communicates between source and destination.
- It does not broadcast the message as it works with limited bandwidth.

- Why is Switching Concept required?

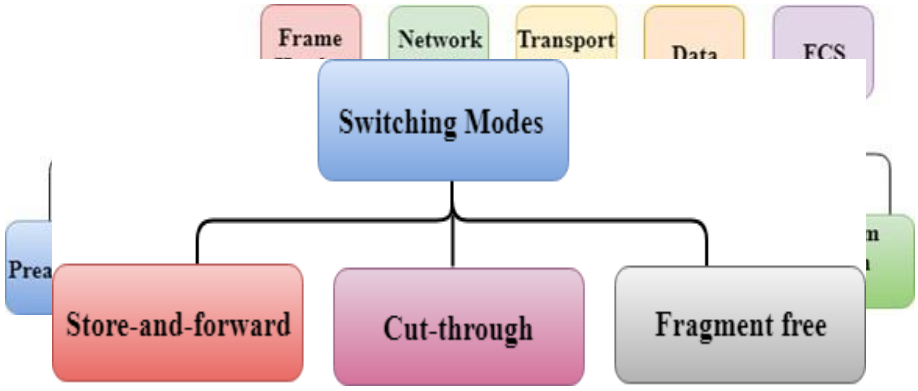
- Switching concept is developed because of the following reasons:

- Bandwidth: It is defined as the maximum transfer rate of a cable. It is a very critical and expensive resource. Therefore, switching techniques are used for the effective utilization of the bandwidth of a network.
- Collision: Collision is the effect that occurs when more than one device transmits the message over the same physical media, and they collide with each other. To overcome this problem, switching technology is implemented so that packets do not collide with each other.

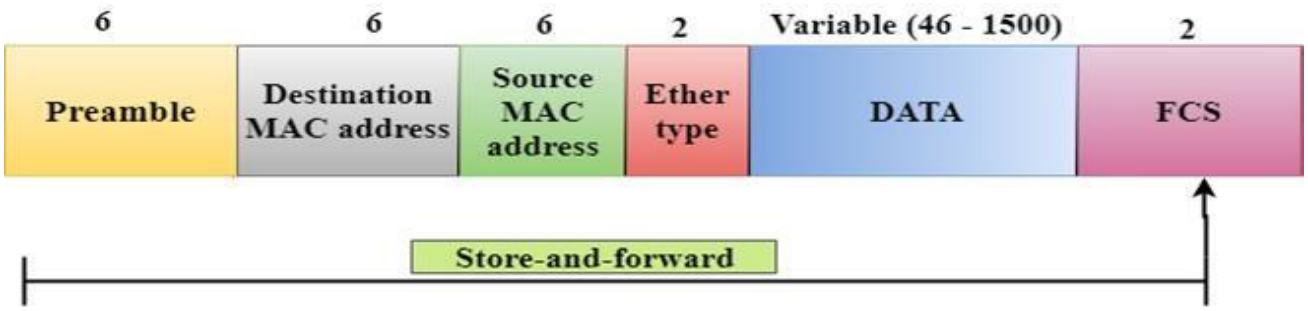
- **Advantages of Switching:**
- Switch increases the bandwidth of the network.
- It reduces the workload on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision as switch creates the collision domain for each connection.
-
- **Disadvantages of Switching:**
- A Switch is more expensive than network bridges.
- A Switch cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.
- Error checking on transmitted and received frames.
-
- The layer 2 switches forward the packets with the help of MAC address.
- Different modes are used for forwarding the packets known as Switching modes.
- In switching mode, Different parts of a frame are recognized. The frame consists of several parts such as preamble, destination MAC address, source MAC address, user's data, FCS.

  There are three types of switching modes:
- **1 Store-and-forward**

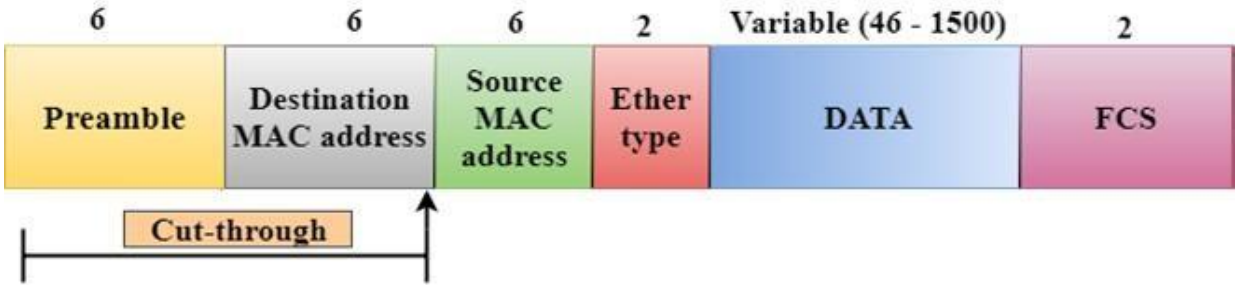
- Cut-through



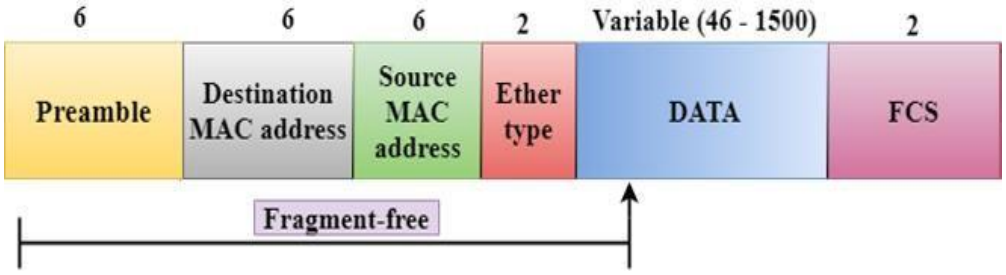
- Fragment-free



- Store-and-forward is a technique in which the intermediate nodes store the received frame and then check for errors before forwarding the packets to the next node.
- The layer 2 switch waits until the entire frame has received. On receiving the entire frame, switch store the frame into the switch buffer memory. This process is known as storing the frame.
- When the frame is stored, then the frame is checked for the errors. If any error found, the message is discarded otherwise the message is forwarded to the next node. This process is known as forwarding the frame.
- CRC (Cyclic Redundancy Check) technique is implemented that uses a number of bits to check for the errors on the received frame.
- The store-and-forward technique ensures a high level of security as the destination network will not be affected by the corrupted frames.
- Store-and-forward switches are highly reliable as it does not forward the collided frames.



- **Cut-through switching** is a technique in which the switch forwards the packets after the destination address has been identified without waiting for the entire frame to be received.
- Once the frame is received, it checks the first six bytes of the frame following the preamble, the switch checks the destination in the switching table to determine the outgoing interface port, and forwards the frame to the destination.
- It has low latency rate as the switch does not wait for the entire frame to be received before sending the packets to the destination.
- It has no error checking technique. Therefore, the errors can be sent with or without errors to the receiver.
- A Cut-through switching technique has low wait time as it forwards the packets as soon as it identifies the destination MAC address.
- In this technique, collision is not detected, if frames have collided will also be forwarded.



- A Fragment-free switching is an advanced technique of the Cut-through Switching.
- A Fragment-free switching is a technique that reads atleast 64 bytes of a frame before forwarding to the next node to provide the error-free transmission.
- It combines the speed of Cut-through Switching with the error checking functionality.
- This technique checks the 64 bytes of the ethernet frame where addressing information is available.
- A collision is detected within 64 bytes of the frame, the frames which are collided will not be forwarded further.

Differences b/w Store-and-forward and Cut-through Switching.

Store-and-forward Switching	Cut-through Switching

Store-and-forward Switching is a technique that waits until the entire frame is received.	Cut-through Switching is a technique that checks the first 6 bytes following the preamble to identify the destination address.
It performs error checking functionality. If any error is found in the frame, the frame will be discarded otherwise forwarded to the next node.	It does not perform any error checking. The frame with or without errors will be forwarded.
It has high latency rate as it waits for the entire frame to be received before forwarding to the next node.	It has low latency rate as it checks only six bytes of the frame to determine the destination address.
It is highly reliable as it forwards only error-free packets.	It is less reliable as compared to Store-and-forward technique as it forwards error prone packets as well.
It has a high wait time as it waits for the entire frame to be received before taking any forwarding decisions.	It has low wait time as cut-through switches do not store the whole frame or packets.

Switching techniques

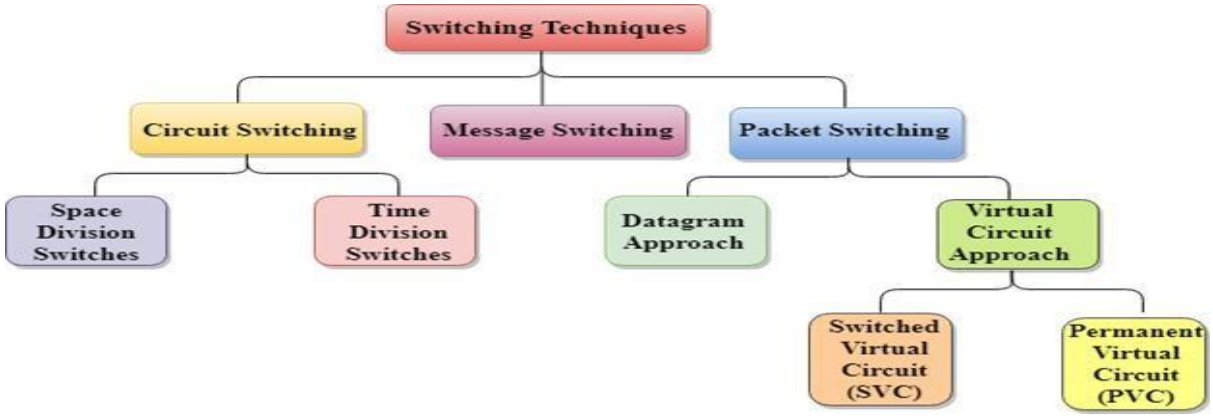
In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

Classification of Switching Techniques

Circuit Switching

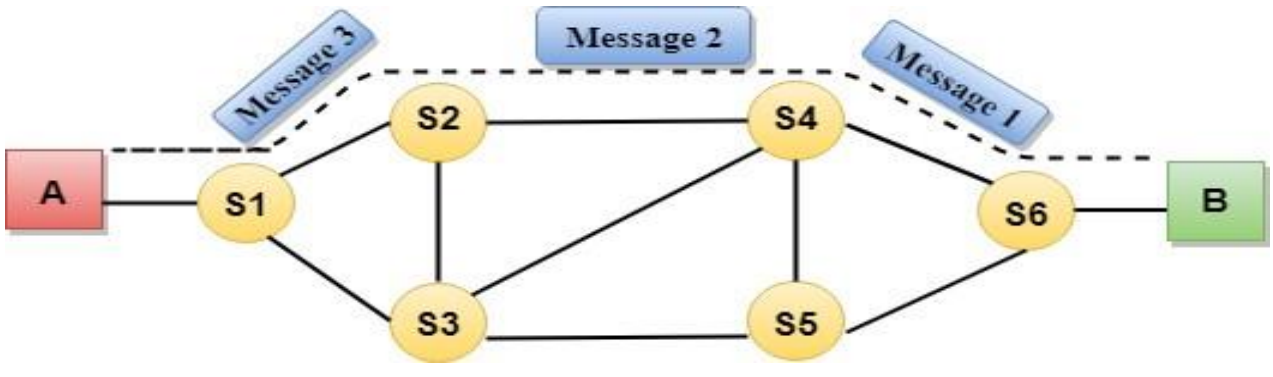
- Circuit switching is a switching technique that establishes a dedicated path between



  sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer



Circuit Disconnect Circuit Switching can use either of the two technologies:

Space Division Switches:

- Space Division Switching is a circuit switching technology in which a single transmission path is accomplished in a switch by using a physically separate set of crosspoints.
- Space Division Switching can be achieved by using crossbar switch. A crossbar switch is a metallic crosspoint or semiconductor gate that can be enabled or disabled by a control unit.
- The Crossbar switch is made by using the semiconductor. For example, Xilinx crossbar switch using FPGAs.
- Space Division Switching has high speed, high capacity, and nonblocking switches.

Space Division Switches can be categorized in two ways:

- **Crossbar Switch**
- *Multistage Switch*

Crossbar Switch

The Crossbar switch is a switch that has n input lines and n output lines. The crossbar switch has n^2 intersection points known as **crosspoints.**

Disadvantage of Crossbar switch:

The number of crosspoints increases as the number of stations is increased. Therefore, it becomes very expensive for a large switch. The solution to this is to use a multistage switch.

Multistage Switch

- Multistage Switch is made by splitting the crossbar switch into the smaller units and then interconnecting them.
- It reduces the number of crosspoints.
- If one path fails, then there will be an availability of another path.

Advantages Of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

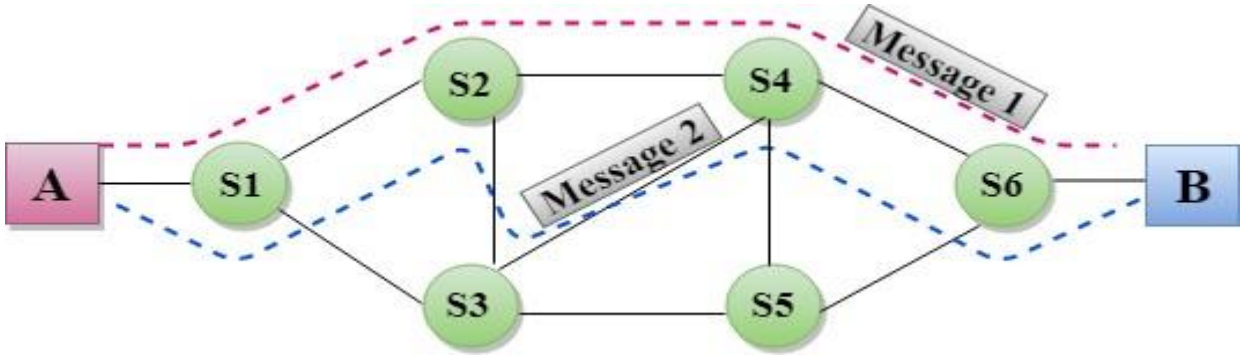
Disadvantages Of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.

- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.
-



Advantages of Message Switching

- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

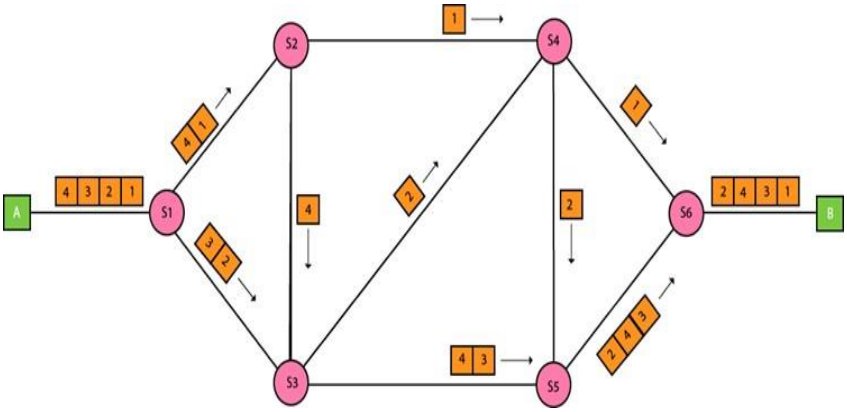
Disadvantages Of Message Switching

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The Long delay can occur due to the storing and forwarding facility provided by the

message switching technique.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



Approaches Of Packet Switching:

There are two approaches to Packet Switching:

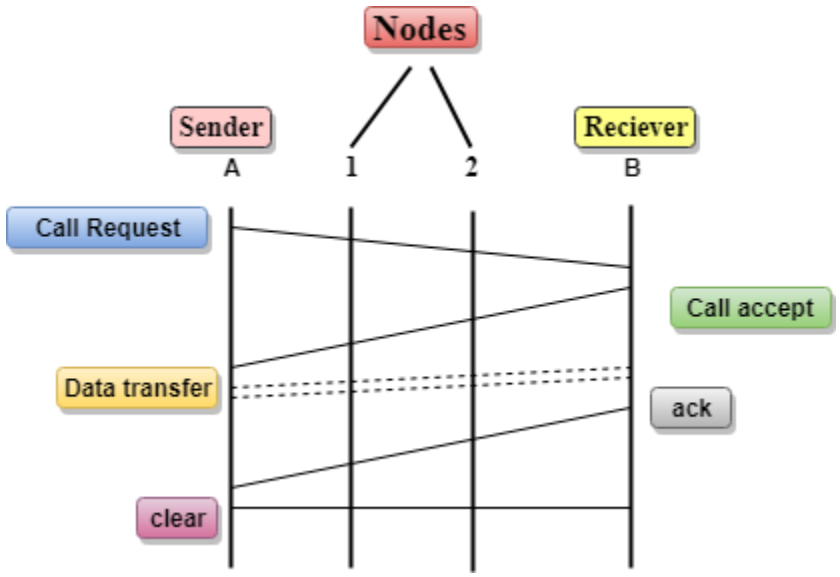
Datagram Packet switching:

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a pre planned route is established before themessages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Let's understand the concept of virtual circuit switching through a diagram:



- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.
- Call request and call accept packets are used to establish a connection between the sender and receiver.
- When a route is established, data will be transferred.

- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	**Virtual Circuit approach**
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

Advantages of Packet Switching:

- Cost-effective:
- Reliable
- Efficient:

Disadvantages of Packet Switching:

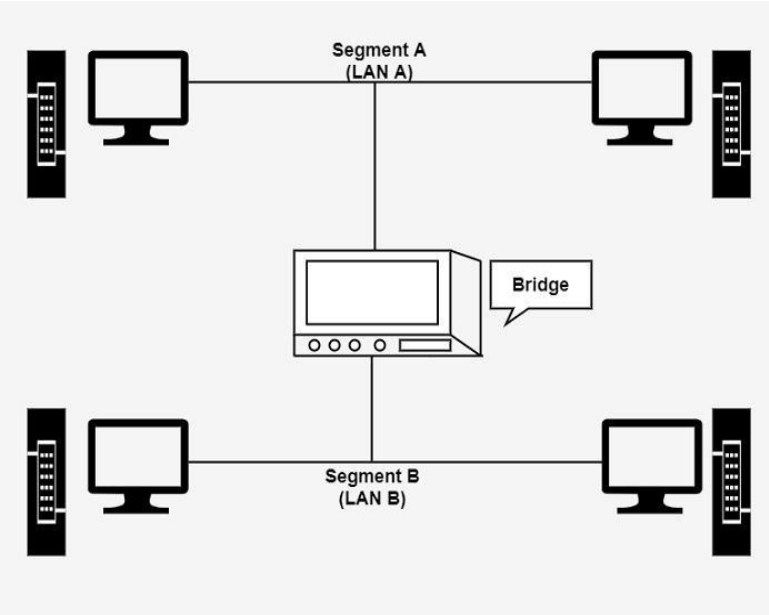
- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

Bridges

Bridges are used to connect two sub networks that use interchangeable protocols. It combines two LANs to form an extended LAN. The main difference between the bridge and repeater is that the bridge has a penetrating efficiency.

Working of Bridges

A bridge accepts all the packets and amplifies all of them to the other side. The bridges are intelligent devices that allow the passing of only selective packets from them. A bridge only passes those packets addressed from a node in one network to another node in the other network.

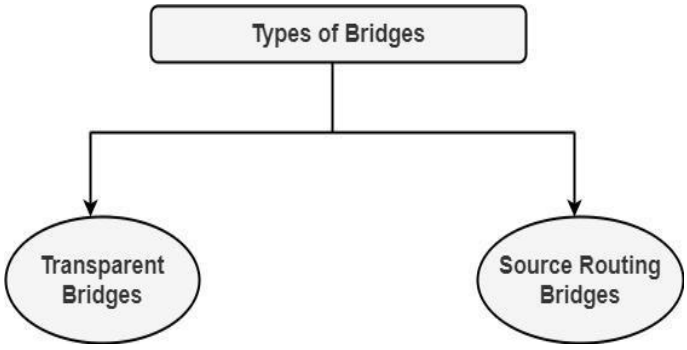


A bridge performs in the following aspect −

- A bridge receives all the packets or frame from both LAN (segment) A and B.
- A bridge builds a table of addresses from which it can identify that the packets are sent from which LAN (or segment) to which LAN.
- The bridge reads the send and discards all packets from LAN A sent to a computer on LAN A and that packets from LAN A send to a computer on LAN B are retransmitted to LAN B.
- The packets from LAN B are considered in the same method.

Types of Bridges

There are generally two types of bridges which are as follows −



Transparent Bridges

- It is also called learning bridges. Bridge construct its table of terminal addresses on its own as it implements connecting two LANs. It facilitates the source location to create its table. It is self- updating. It is a plug and plays bridge.

Source Routing Bridge

- This sending terminal means the bridges that the frames should stay. This type of bridge is used to prevent looping problem.

Uses of Bridges

- The main uses of bridges are −
- Bridges are used to divide large busy networks into multiple smaller and interconnected networks to improve performance.
- Bridges also can increase the physical size of a network.

Faculty: Dr Naveen Singh
+91-9953320298 drnaveenkrsingh@gmail.com