UNIT V DATA LINK AND PHYSICAL LAYERS

Data Link Layer – Framing – Flow control – Error control – Data-Link Layer Protocols – HDLC – PPP - Media Access Control – Ethernet Basics – CSMA/CD – Virtual LAN – Wireless LAN (802.11) - Physical Layer: Data and Signals - Performance – Transmission media- Switching – Circuit Switching.

1.DATA LINK LAYER

The Data-link layer is the second layer from the bottom in the OSI (Open System Interconnection) network architecture model. It is responsible for the node-to-node delivery of data. Its major role is to ensure error-free transmission of information. DLL is also responsible to encode, decode and organize the outgoing and incoming data. This is considered the most complex layer of the OSI model as it hides all the underlying complexities of the hardware from the other above layers.

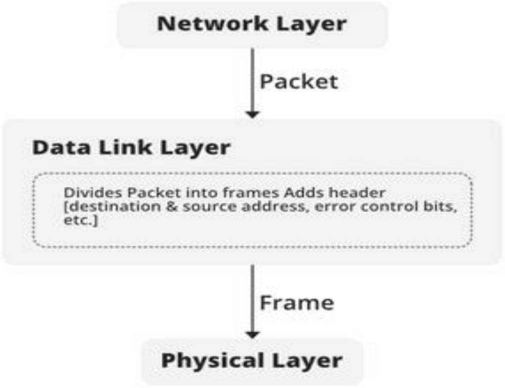
Sub-layers of Data Link Layer:
The data link layer is further divided into two sub-layers, which are as follows:

Logical Link Control (LLC):This sublayer of the data link layer deals with multiplexing, the flow of data among applications and other services, and LLC is responsible for providing error messages and acknowledgments as well.

Media Access Control (MAC):MAC sublayer manages the device's interaction, responsible for addressing frames, and also controls physical media access.

The data link layer receives the information in the form of packets from the Network layer, it divides packets into frames and sends those frames bit-by-bit to the underlying physical layer.

Functions of the Data-link Layer:


Network Layer
Packet
Data Link Layer
Divides Packet into frames Adds header [destination & source address, error control bits, etc.]
Frame
Physical Layer

1. **Framing:** The packet received from the Network layer is known as a frame in the Data link layer. At the sender's side, DLL receives packets from the Network layer and

divides them into small frames, then, sends each frame bit-by-bit to the physical layer. It also attaches some special bits (for error control and addressing) at the header and end of the frame. At the receiver's end, DLL takes bits from the Physical layer organizes them into the frame, and sends them to the Network layer.

2. **Addressing:** The data link layer encapsulates the source and destination's MAC address/ physical address in the header of each frame to ensure node-to-node delivery. MAC address is the unique hardware address that is assigned to the device while manufacturing.

3. **Error Control:** Data can get corrupted due to various reasons like noise, attenuation, etc. So, it is the responsibility of the data link layer, to detect the error in the transmitted data and correct it using error detection and correction techniques respectively. DLL adds error detection bits into the frame's header, so that receiver can check received data is correct or not.

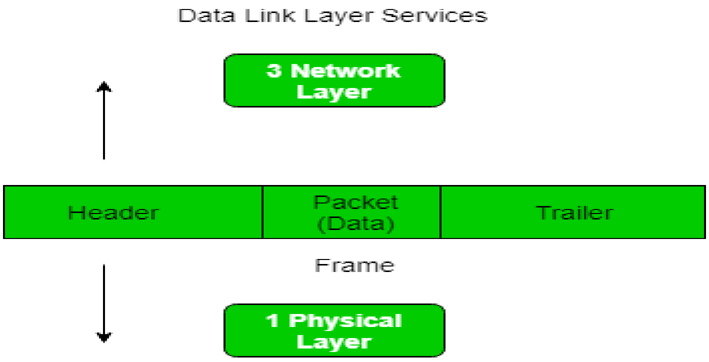
4. **Flow Control:** If the receiver's receiving speed is lower than the sender's sending speed, then this can lead to an overflow in the receiver's buffer and some frames may get lost. So, it's the responsibility of DLL to synchronize the sender's and receiver's speeds and establish flow control between them.

5. **Access Control**: When multiple devices share the same communication channel there is a high probability of collision, so it's the responsibility of DLL to check which device has control over the channel and CSMA/CD and CSMA/CA can be used to avoid collisions and loss of frames in the channel.

2.FRAMING IN DATA LINK LAYER

Frames are the units of digital transmission, particularly in computer networks and telecommunications. Frames are comparable to the packets of energy called photons in the case of light energy. Frame is continuously used in Time Division Multiplexing process.

Framing is a point-to-point connection between two computers or devices consisting of a wire in which data is transmitted as a stream of bits. However, these bits must be framed into discernible blocks of information. Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Ethernet, token ring, frame relay, and other data link layer technologies have their own frame structures. Frames have headers that contain information such as error-checking codes.



At the data link layer, it extracts the message from the sender and provides it to the receiver by providing the sender's and receiver's addresses. The advantage of using frames is that data is broken up into recoverable chunks that can easily be checked for corruption.

The process of dividing the data into frames and reassembling it is transparent to the user and is handled by the data link layer.

Framing is an important aspect of data link layer protocol design because it allows the transmission of data to be organized and controlled, ensuring that the data is delivered accurately and efficiently.

Problems in Framing

- Detecting start of the frame: When a frame is transmitted, every station must be able to detect it. Station detects frames by looking out for a special sequence of bits that marks the beginning of the frame i.e. SFD (Starting Frame Delimiter).
- How does the station detect a frame: Every station listens to link for SFD pattern through a sequential circuit. If SFD is detected, sequential circuit alerts station. Station checks destination address to accept or reject frame.
- Detecting end of frame: When to stop reading the frame.
- Handling errors: Framing errors may occur due to noise or other transmission errors, which can cause a station to misinterpret the frame. Therefore, error detection and correction mechanisms, such as cyclic redundancy check (CRC), are used to ensure the integrity of the frame.
- Framing overhead: Every frame has a header and a trailer that contains control information such as source and destination address, error detection code, and other protocol-related information. This overhead reduces the available bandwidth for data transmission, especially for small-sized frames.
- Framing incompatibility: Different networking devices and protocols may use different framing methods, which can lead to framing incompatibility issues. For example, if a device using one framing method sends data to a device using a different framing method, the receiving device may not be able to correctly interpret the frame.
- Framing synchronization: Stations must be synchronized with each other to avoid collisions and ensure reliable communication. Synchronization requires that all stations agree on the frame boundaries and timing, which can be challenging in complex networks with many devices and varying traffic loads.
- Framing efficiency: Framing should be designed to minimize the amount of data overhead while maximizing the available bandwidth for data transmission. Inefficient framing methods can lead to lower network performance and higher latency.

Types of framing

There are two types of framing:

1. Fixed-size: The frame is of fixed size and there is no need to provide boundaries to the frame, the length of the frame itself acts as a delimiter.

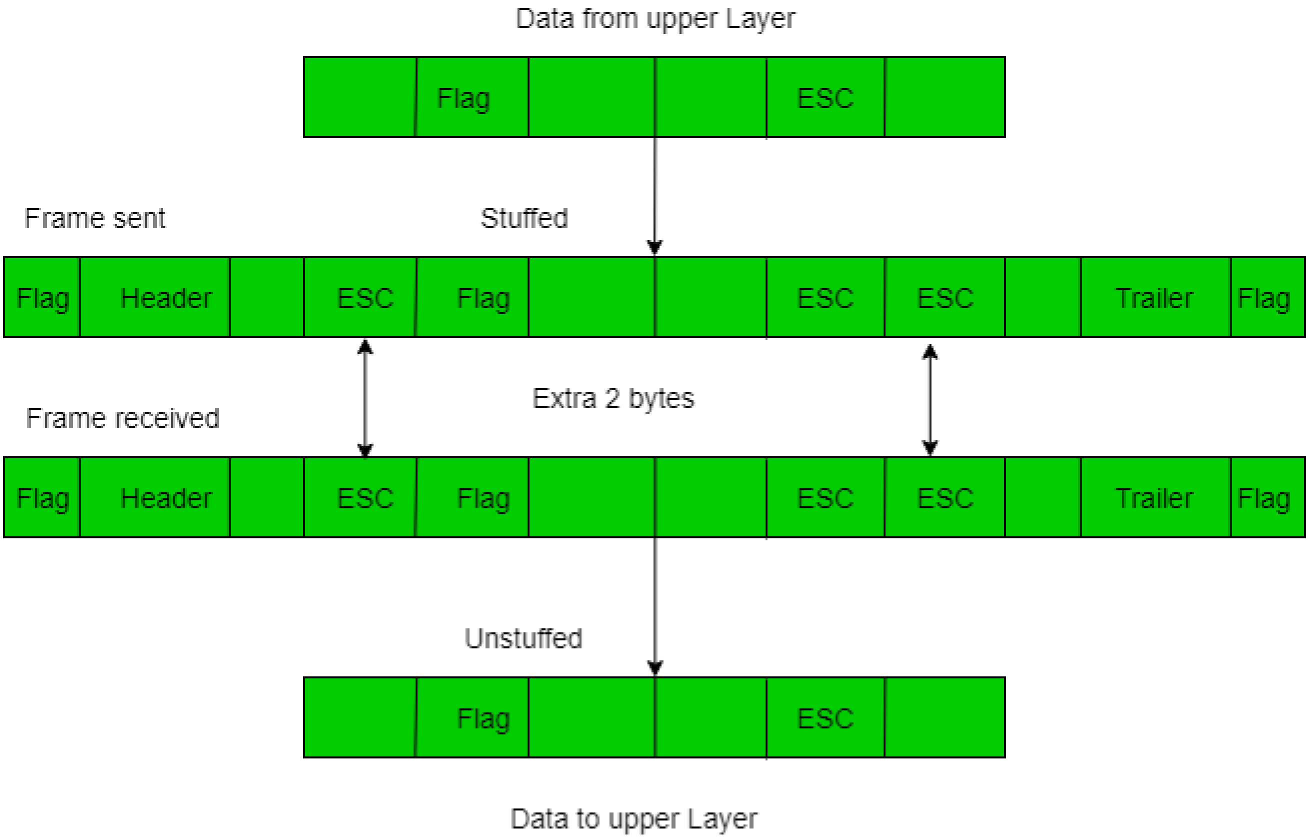
- Drawback: It suffers from internal fragmentation if the data size is less than the frame size

- Solution: Padding

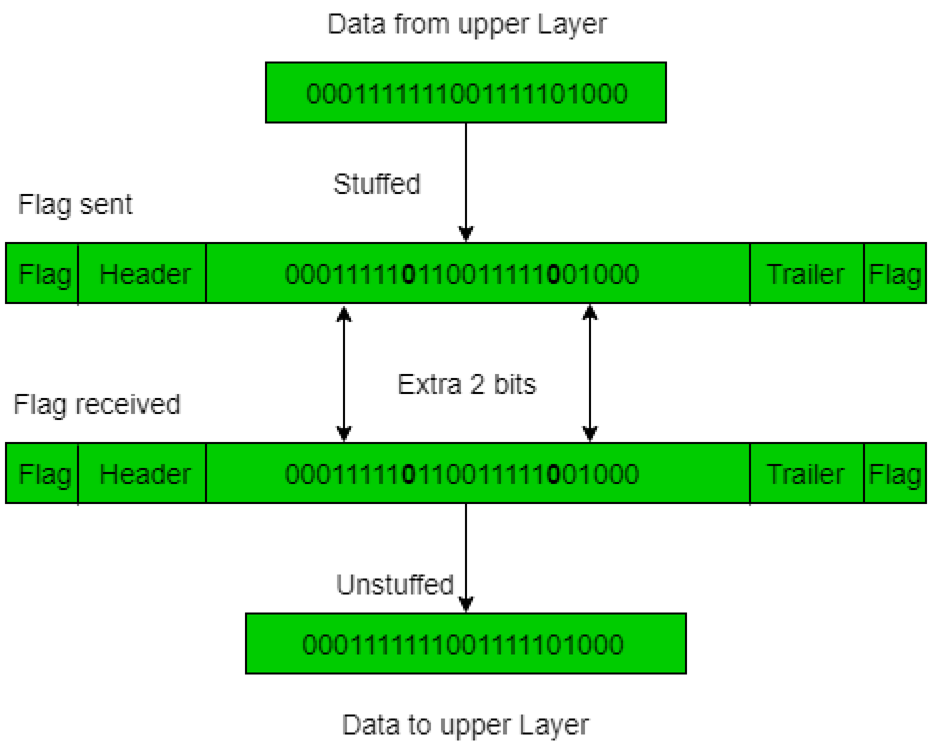
2. Variable size: In this, there is a need to define the end of the frame as well as the beginning of the next frame to distinguish. This can be done in two ways:

1. Length field – We can introduce a length field in the frame to indicate the length of the frame. Used in Ethernet(802.3). The problem with this is that sometimes the length field might get corrupted.
2. End Delimiter (ED) – We can introduce an ED(pattern) to indicate the end of the frame. Used in Token Ring. The problem with this is that ED can occur in the data. This can be solved by:
   1. Character/Byte Stuffing: Used when frames consist of characters. If data contains ED then, a byte is stuffed into data to differentiate it from ED.
   Let ED = “$” –> if data contains ‘$’ anywhere, it can be escaped using ‘\O’ character.

   –> if data contains ‘\O$’ then, use ‘\O\O\O$'($ is escaped using \O and \O is escaped using \O).



Disadvantage – It is very costly and obsolete method.
2. Bit Stuffing: Let ED = 01111 and if data = 01111
–> Sender stuffs a bit to break the pattern i.e. here appends a 0 in data = 011101.
–> Receiver receives the frame.
–> If data contains <u>0111</u>01, receiver removes the 0 and reads the data.



Examples:

- If Data –> 011100011110 and ED –> 0111 then, find data after bit stuffing.

--> 011010001101100

- If Data –> 110001001 and ED –> 1000 then, find data after bit stuffing?

--> 11001010011

framing in the Data Link Layer also presents some challenges, which include:

Variable frame length: The length of frames can vary depending on the data being transmitted, which can lead to inefficiencies in transmission. To address this issue, protocols such as HDLC and PPP use a flag sequence to mark the start and end of each frame.

Bit stuffing: Bit stuffing is a technique used to prevent data from being interpreted as control characters by inserting extra bits into the data stream. However, bit stuffing can lead to issues with synchronization and increase the overhead of the transmission.

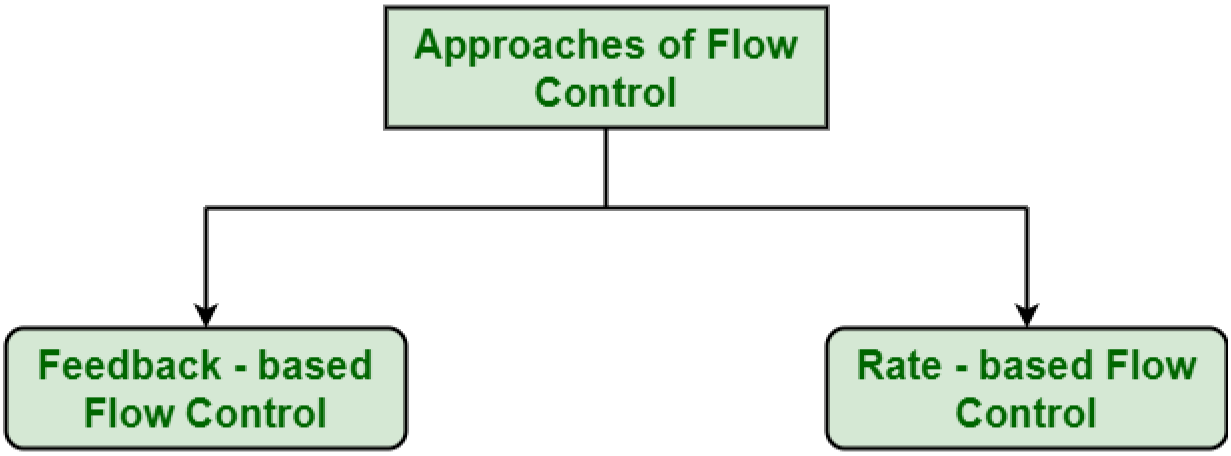
Synchronization: Synchronization is critical for ensuring that data frames are transmitted and received correctly. However, synchronization can be challenging, particularly in high-speed networks where frames are transmitted rapidly.

Error detection: Data Link Layer protocols use various techniques to detect errors in the transmitted data, such as checksums and CRCs. However, these techniques are not foolproof and can miss some types of errors.

Efficiency: Efficient use of available bandwidth is critical for ensuring that data is transmitted quickly and reliably. However, the overhead associated with framing and error detection can reduce the overall efficiency of the transmission.

3.FLOW CONTROL IN DATA LINK LAYER

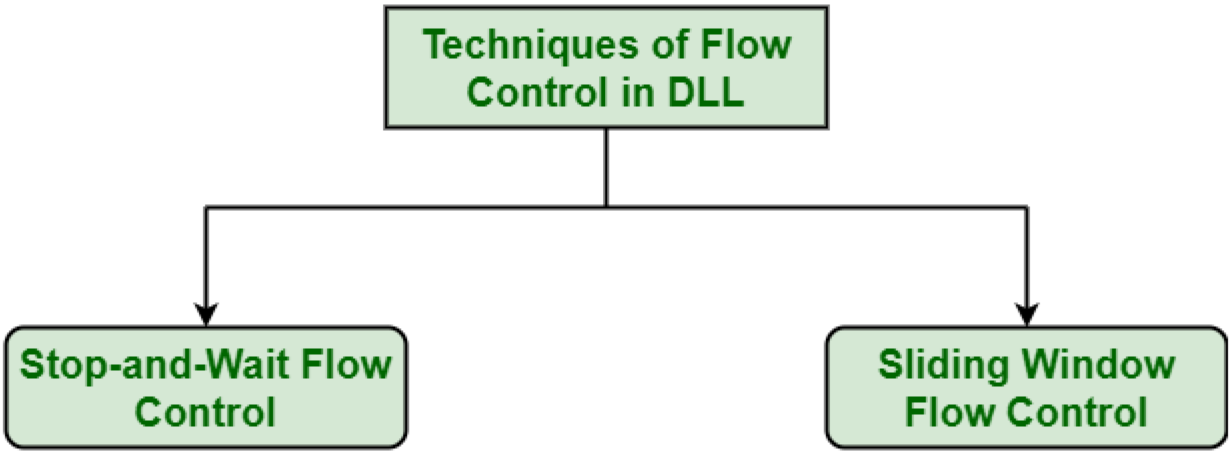
Flow control is design issue at Data Link Layer. It is a technique that generally observes the proper flow of data from sender to receiver. It is very essential because it is possible for sender to transmit data or information at very fast rate and hence receiver can receive this information and process it. This can happen only if receiver has very high load of traffic as compared to sender, or if receiver has power of processing less as compared to sender. Flow control is basically a technique that gives permission to two of stations that are working and processing at different speeds to just communicate with one another. Flow control in Data Link Layer simply restricts and coordinates number of frames or amount of data sender can send just before it waits for an acknowledgement from receiver. Flow control is actually set of procedures that explains sender about how much data or frames it can transfer or transmit before data overwhelms receiver. The receiving device also contains only limited amount of speed and memory to store data. This is why receiving device should be able to tell or inform the sender about stopping the transmission or transferring of data on temporary basis before it reaches limit. It also needs buffer, large block of memory for just storing data or frames until they are processed flow control can also be understand as a speed matching mechanism for two stations.


Approaches of Flow Control
Feedback - based Flow Control
Rate - based Flow Control

Approaches to Flow Control : Flow Control is classified into two categories:

- **Feedback** – based Flow Control : In this control technique, sender simply transmits data or information or frame to receiver, then receiver transmits data back to sender and also allows sender to transmit more amount of data or tell sender about how receiver is processing or doing. This simply means that sender transmits data or frames after it has received acknowledgements from user.
- **Rate** – based Flow Control : In this control technique, usually when sender sends or transfer data at faster speed to receiver and receiver is not being able to receive data at the speed, then mechanism known as built-in mechanism in protocol will just limit or restricts overall rate at which data or information is being transferred or transmitted by sender without any feedback or acknowledgement from receiver.

Techniques of Flow Control in Data Link Layer : There are basically two types of techniques being developed to control the flow of data


Techniques of Flow Control in DLL
Stop-and-Wait Flow Control
Sliding Window Flow Control

1. Stop-and-Wait Flow Control : This method is the easiest and simplest form of flow control. In this method, basically message or data is broken down into various multiple frames, and then receiver indicates its readiness to receive frame of data. When acknowledgement is received, then only sender will send or transfer the next frame. This process is continued until sender transmits EOT (End of Transmission) frame. In this method, only one of frames can be in transmission at a time. It leads to inefficiency i.e. less productivity if propagation delay is very much longer than the transmission delay and Ultimately In this method sender sent single frame and receiver take one frame at a time and sent acknowledgement(which is next frame number only) for new frame.

Advantages –

- This method is very easiest and simple and each of the frames is checked and acknowledged well.
- This method is also very accurate.

Disadvantages –

- This method is fairly slow.
- In this, only one packet or frame can be sent at a time.
- It is very inefficient and makes the transmission process very slow.

2. Sliding Window Flow Control : This method is required where reliable in-order delivery of packets or frames is very much needed like in data link layer. It is point to point protocol that assumes that none of the other entity tries to communicate until current data or frame transfer gets completed. In this method, sender transmits or sends various frames or packets before receiving any acknowledgement. In this method, both the sender and receiver agree upon total number of data frames after which acknowledgement is needed to be transmitted. Data Link Layer requires and uses this method that simply allows sender to have more than one unacknowledged packet "in-flight" at a time. This increases and improves network throughput. and Ultimately In this method sender sent multiple frame but receiver take one by one and after completing one frame acknowledge(which is next frame number only) for new frame.

Advantages –

- It performs much better than stop-and-wait flow control.
- This method increases efficiency.
- Multiples frames can be sent one after another.

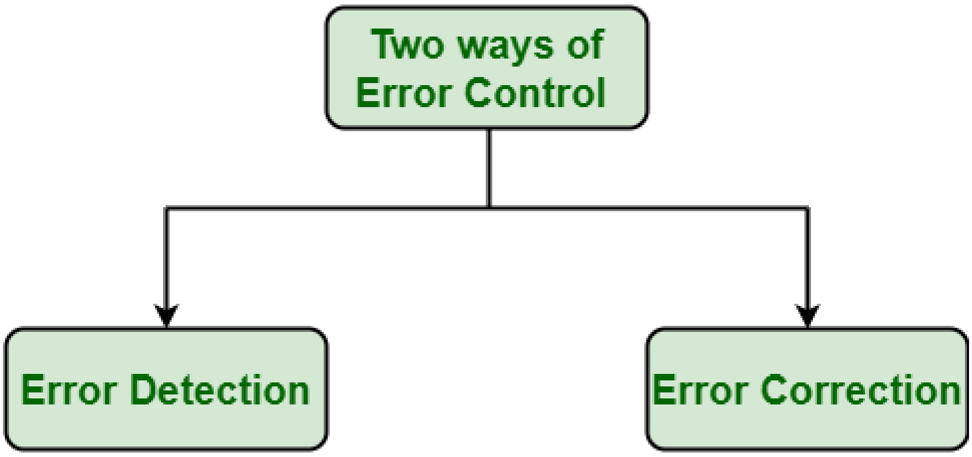
Disadvantages –

- The main issue is complexity at the sender and receiver due to the transferring of multiple frames.
- The receiver might receive data frames or packets out the sequence.

4.ERROR CONTROL

Data-link layer uses the techniques of error control simply to ensure and confirm that all the data frames or packets, i.e. bit streams of data, are transmitted or transferred from sender to receiver with certain accuracy. Using or providing error control at this data link layer is an optimization, it was never a requirement. Error control is basically process in data link layer of detecting or identifying and re-transmitting data frames that might be lost or corrupted during transmission. In both of these cases, receiver or destination does not receive correct data frame and sender or source does not even know anything about any such loss regarding data frames. Therefore, in such type of cases, both sender and receiver are provided with some essential protocols that are required to detect or identify such types of errors as loss of data frames. The Data-link layer follows a technique known as re-transmission of frames to detect or identify transit errors and also to take necessary actions that are required to reduce or remove such errors. Each and every time an error is detected during transmission, particular data frames are retransmitted and this process is known as ARQ (Automatic Repeat Request).

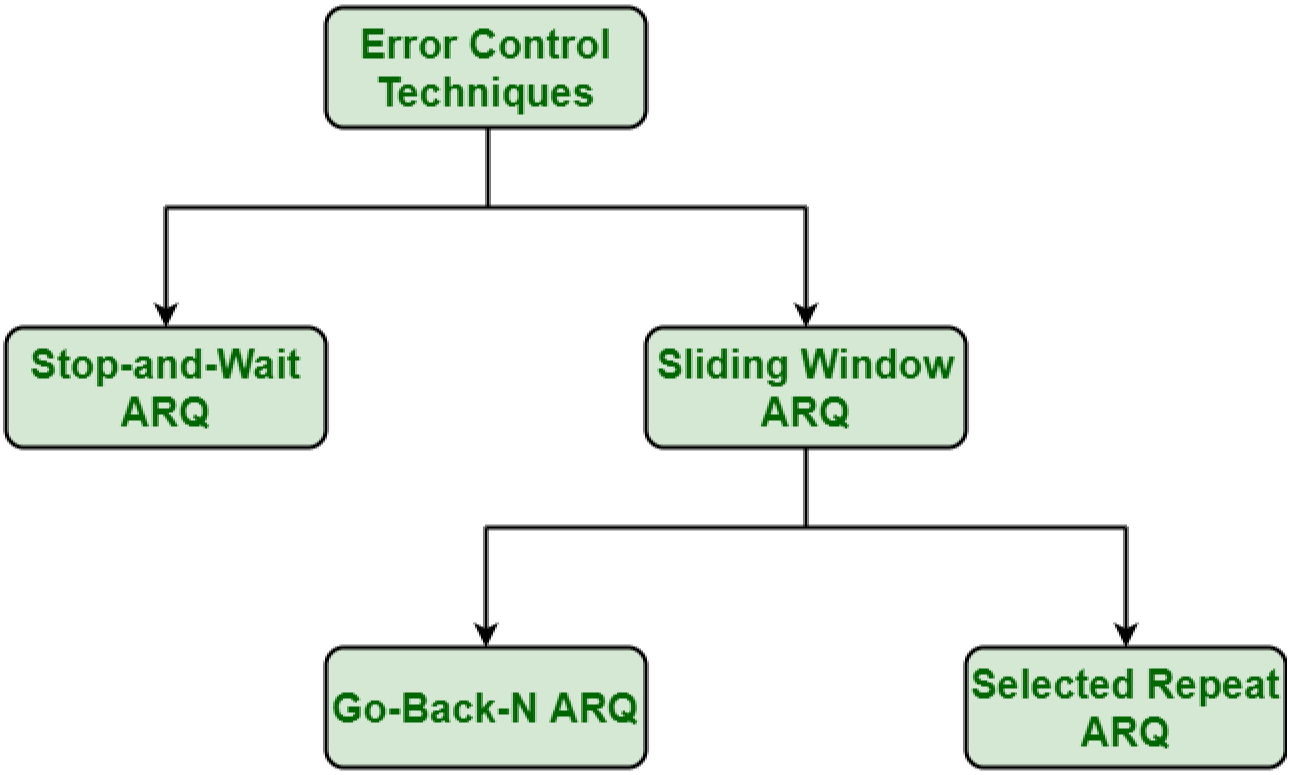
Ways of doing Error Control : There are basically two ways of doing Error control as given below :



Ways of Error Control

1. **Error Detection** : Error detection, as the name suggests, simply means detection or identification of errors. These errors may occur due to noise or any other impairments during transmission from transmitter to the receiver, in communication system. It is a class of techniques for detecting garbled i.e. unclear and distorted data or messages.
2. **Error Correction** : Error correction, as the name suggests, simply means correction or solving or fixing of errors. It simply means reconstruction and rehabilitation of original data that is error-free. But error correction method is very costly and very hard.

Various Techniques for Error Control : There are various techniques of error control as given below :



Techniques of Error Control

1. <u>Stop-and-Wait ARQ</u> : Stop-and-Wait ARQ is also known as alternating bit protocol. It is one of the simplest flow and error control techniques or mechanisms. This mechanism is generally required in telecommunications to transmit data or information between two connected devices. Receiver simply indicates its readiness to receive data for each frame. In these, sender sends information or data packets to receiver. Sender then stops and waits for ACK (Acknowledgment) from receiver. Further, if ACK does not arrive within given time period i.e., time-out, sender then again resends frame and waits for ACK. But, if sender receives ACK, then it will transmit the next data packet to receiver and then again wait for ACK from receiver. This process to stop and wait continues until sender has no data frame or packet to send.
2. **<u>Sliding Window ARQ</u>** : This technique is generally used for continuous transmission error control. It is further categorized into two categories as given below :

- **<u>Go-Back-N ARQ</u>** : Go-Back-N ARQ is form of ARQ protocol in which transmission process continues to send or transmit total number of frames that are specified by window size even without receiving an ACK (Acknowledgement) packet from the receiver. It uses sliding window flow control protocol. If no errors occur, then operation is identical to sliding window.
- **<u>Selective Repeat ARQ</u> :** Selective Repeat ARQ is also form of ARQ protocol in which only suspected or damaged or lost data frames are only retransmitted.

This technique is similar to Go-Back-N ARQ though much more efficient than the Go-Back-N ARQ technique due to reason that it reduces number of retransmission. In this, the sender only retransmits frames for which NAK is received. But this technique is used less because of more complexity between sender and receiver and each frame must be needed to be acknowledged individually.

The main difference between Go Back ARQ and Selective Repeat ARQ is that in Go Back ARQ, the sender has to retransmit the whole window of frame again if any of the frame is lost but in Selective Repeat ARQ only the data frame that is lost is retransmitted.

6.DATA-LINK LAYER PROTOCOLS

The Data Link Layer protocols are Ethernet, token ring, FDDI and PPP. An important characteristic of a Data Link Layer is that datagram can be handled by different link layer protocols on different links in a path. For example, the datagram is handled by Ethernet on the first link, PPP on the second link.

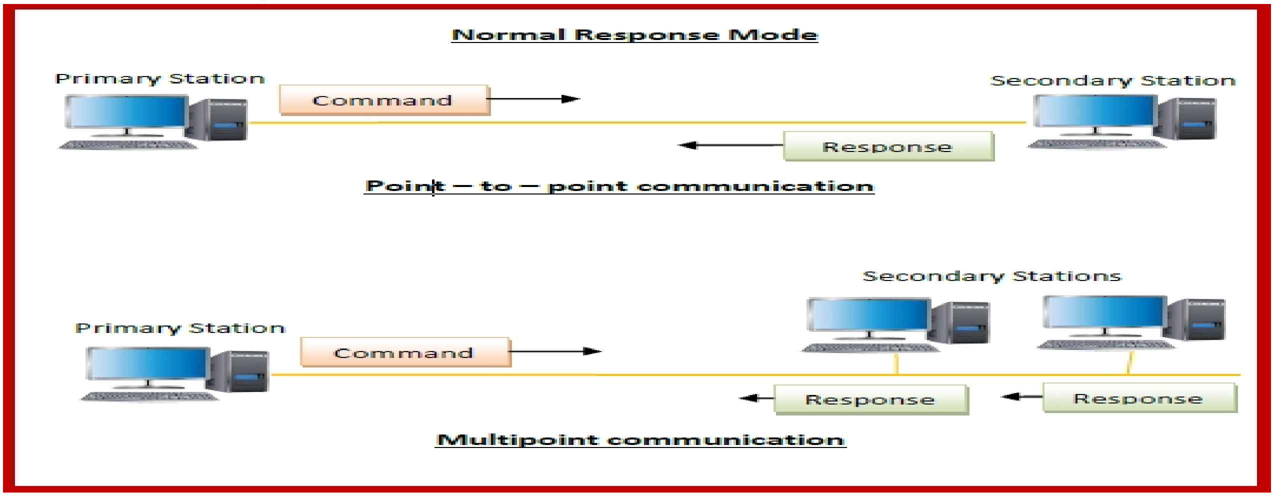
7.HIGH-LEVEL DATA LINK CONTROL (HDLC)

High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.

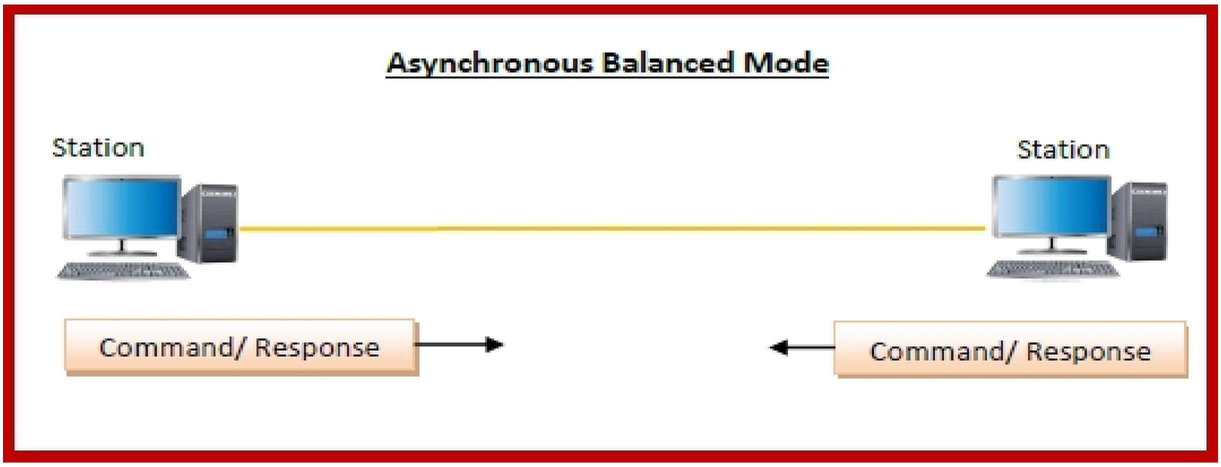
Transfer Modes

HDLC supports two types of transfer modes, normal response mode and asynchronous balanced mode.

- **Normal Response Mode (NRM)** – Here, two types of stations are there, a primary station that send commands and secondary station that can respond to received commands. It is used for both point - to - point and multipoint communications.



- Asynchronous Balanced Mode (ABM) − Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.

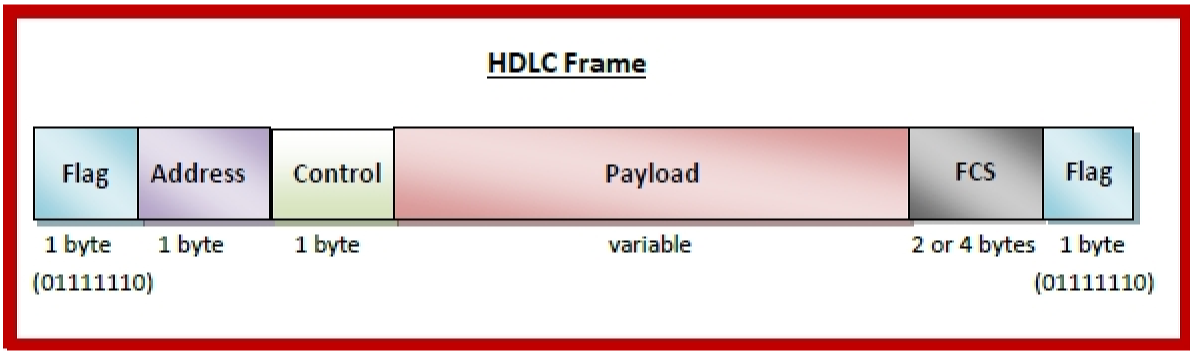


-

HDLC Frame

HDLC is a bit - oriented protocol where each frame contains up to six fields. The structure varies according to the type of frame. The fields of a HDLC frame are −

- Flag − It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- Address − It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
- Control − It is 1 or 2 bytes containing flow and error control information.
- Payload − This carries the data from the network layer. Its length may vary from one network to another.
- FCS − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code).

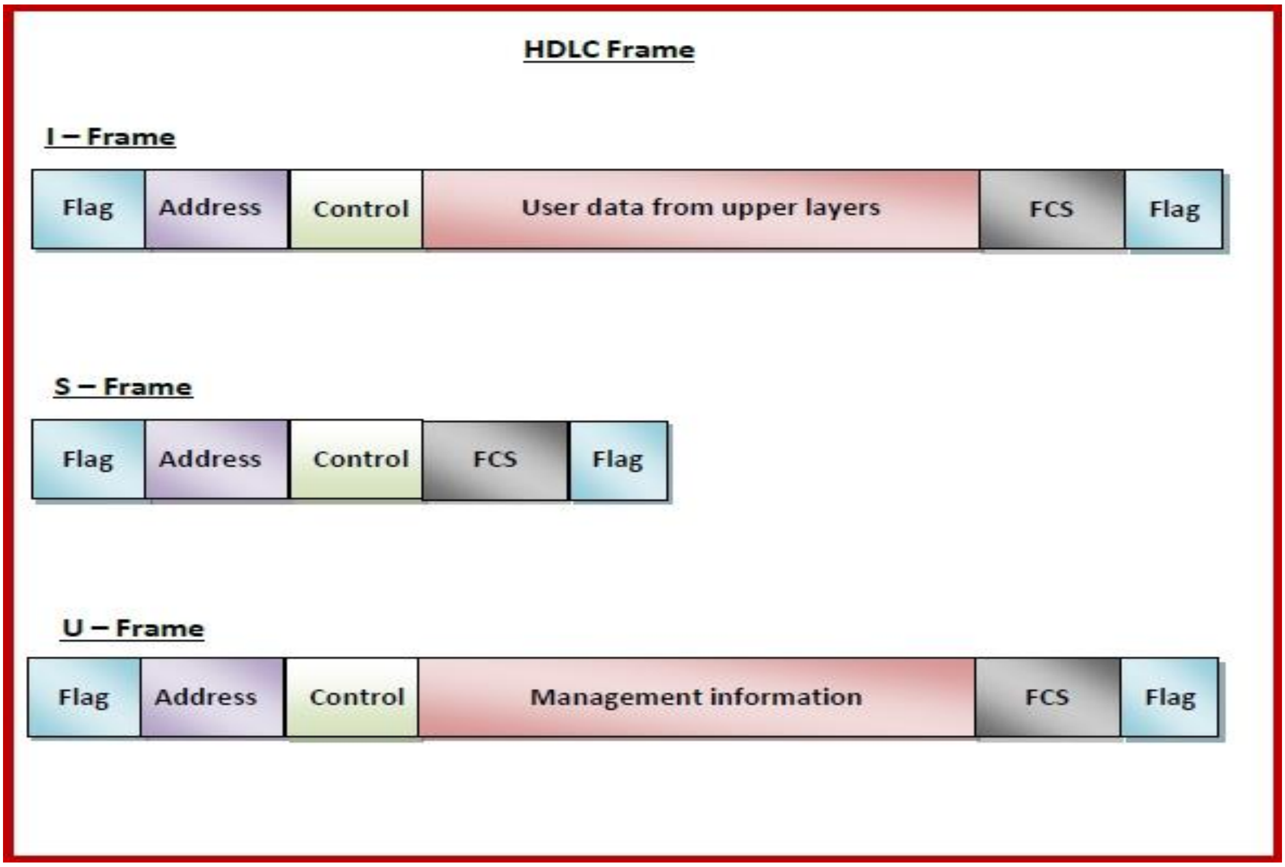


Types of HDLC Frames

There are three types of HDLC frames. The type of frame is determined by the control field of the frame −

- I-frame − I-frames or Information frames carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of control field of I-frame is 0.

- S-frame – S-frames or Supervisory frames do not contain information field. They are used for flow and error control when piggybacking is not required. The first two bits of control field of S-frame is 10.
- U-frame – U-frames or Un-numbered frames are used for myriad miscellaneous functions, like link management. It may contain an information field, if required. The first two bits of control field of U-frame is 11.



8.POINT-TO-POINT PROTOCOL (PPP)

Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds. Since it is a data link layer protocol, data is transmitted in frames. It is also known as RFC 1661.

Services Provided by PPP

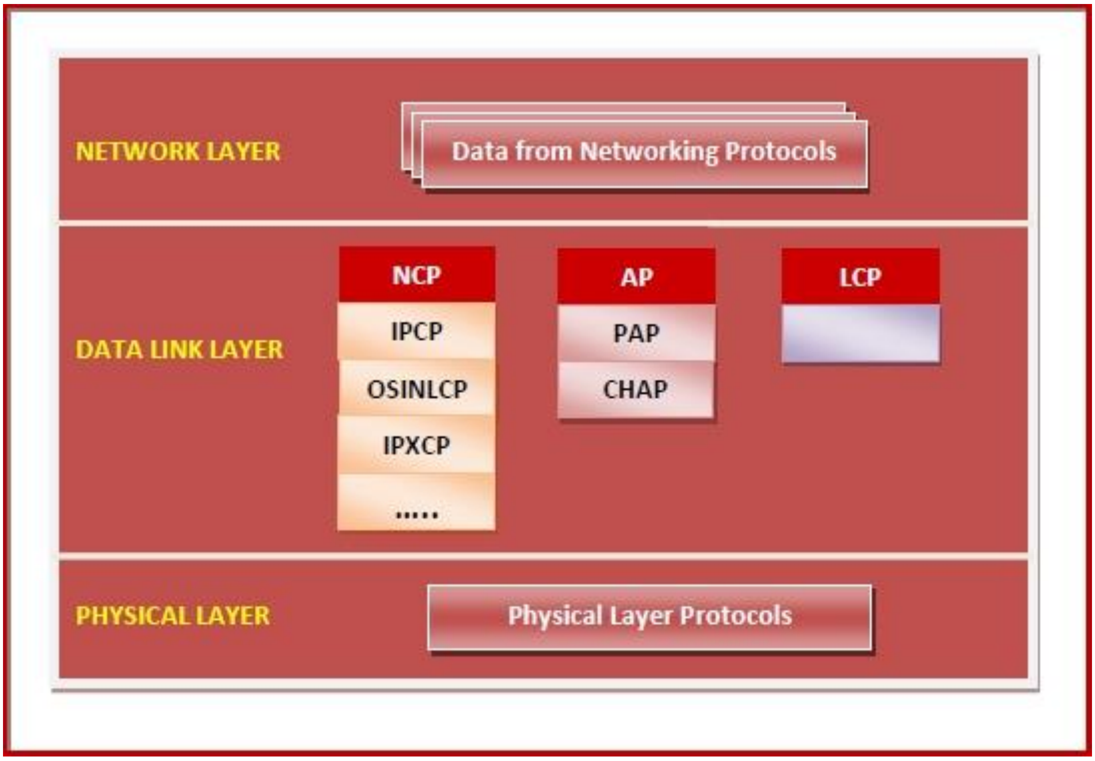
The main services provided by Point - to - Point Protocol are –

- Defining the frame format of the data to be transmitted.
- Defining the procedure of establishing link between two points and exchange of data.
- Stating the method of encapsulation of network layer data in the frame.
- Stating authentication rules of the communicating devices.
- Providing address for network communication.
- Providing connections over multiple links.
- Supporting a variety of network layer protocols by providing a range os services.

Components of PPP

Point - to - Point Protocol is a layered protocol having three components –

- Encapsulation Component – It encapsulates the datagram so that it can be transmitted over the specified physical layer.
- Link Control Protocol (LCP) – It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links.
- Authentication Protocols (AP) – These protocols authenticate endpoints for use of services. The two authentication protocols of PPP are –
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
- Network Control Protocols (NCPs) – These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there. Some of the NCPs of PPP are –
  - Internet Protocol Control Protocol (IPCP)
  - OSI Network Layer Control Protocol (OSINLCP)
  - Internetwork Packet Exchange Control Protocol (IPXCP)
  - DECnet Phase IV Control Protocol (DNCP)
  - NetBIOS Frames Control Protocol (NBFCP)
  - IPv6 Control Protocol (IPV6CP)

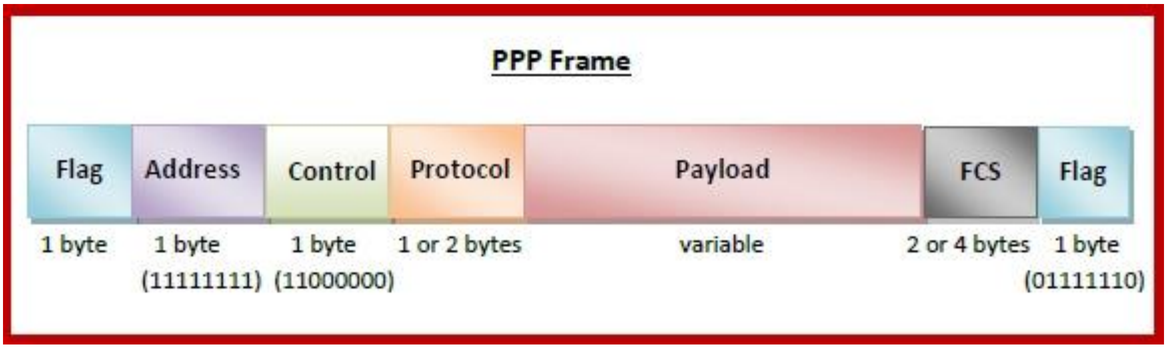


PPP Frame

PPP is a byte - oriented protocol where each field of the frame is composed of one or more bytes. The fields of a PPP frame are –

- Flag – 1 byte that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.

- Address – 1 byte which is set to 11111111 in case of broadcast.
- Control – 1 byte set to a constant value of 11000000.
- Protocol – 1 or 2 bytes that define the type of data contained in the payload field.
- Payload – This carries the data from the network layer. The maximum length of the payload field is 1500 bytes. However, this may be negotiated between the endpoints of communication.
- FCS – It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



Byte Stuffing in PPP Frame – Byte stuffing is used is PPP payload field whenever the flag sequence appears in the message, so that the receiver does not consider it as the end of the frame. The escape byte, 01111101, is stuffed before every byte that contains the same byte as the flag byte or the escape byte. The receiver on receiving the message removes the escape byte before passing it onto the network layer.

9.MEDIA ACCESS CONTROL

A media access control is a network data transfer policy that determines how data is transmitted between two computer terminals through a network cable. The media access control policy involves sub-layers of the data link layer 2 in the OSI reference model.

The essence of the MAC protocol is to ensure non-collision and eases the transfer of data packets between two computer terminals. A collision takes place when two or more terminals transmit data/information simultaneously. This leads to a breakdown of communication, which can prove costly for organizations that lean heavily on data transmission.

Media Access Control Methods

This network channel through which data is transmitted between terminal nodes to avoid collision has three various ways of accomplishing this purpose. They include:

- Carrier sense multiple access with collision avoidance (CSMA/CA)
- Carrier sense multiple access with collision detection (CSMA/CD)
- Demand priority
- Token passing

10.CARRIER SENSE MULTIPLE ACCESS WITH COLLISION AVOIDANCE (CSMA/CA)

Carrier sense multiple access with collision avoidance (CSMA/CA) is a media access control policy that regulates how data packets are transmitted between two computer nodes. This method avoids collision by configuring each computer terminal to make a signal before transmission. The signal is carried out by the transmitting computer to avoid a collision.

Multiple access implies that many computers are attempting to transmit data. Collision avoidance means that when a computer node transmitting data states its intention, the other waits at a specific length of time before resending the data.

CSMA/CA is data traffic regulation is slow and adds cost in having each computer node signal its intention before transmitting data. It used only on Apple networks.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

Carrier sense multiple access with collision detection (CSMA/CD) is the opposite of CSMA/CA. Instead of detecting data to transmit signal intention to prevent a collision, it observes the cable to detect the signal before transmitting.

Collision detection means that when a collision is detected by the media access control policy, transmitting by the network stations stops at a random length of time before transmitting starts again.

It is faster than CSMA/CA as it functions in a network station that involves fewer data frames being transmitted. CSMA/CD is not as efficient as CSMA/CA in preventing network collisions. This is because it only detects huge data traffic in the network cable. Huge data traffic increases the possibility of a collision taking place. It is used on the Ethernet network.

Demand Priority

The demand priority is an improved version of the Carrier sense multiple access with collision detection (CSMA/CD). This data control policy uses an ‘active hub’ in regulating how a network is accessed. Demand priority requires that the network terminals obtain authorization from the active hub before data can be transmitted.

Another distinct feature of this MAC control policy is that data can be transmitted between the two network terminals at the same time without collision. In the Ethernet media, demand priority directs that data is transmitted directly to the receiving network terminal.

Token Passing

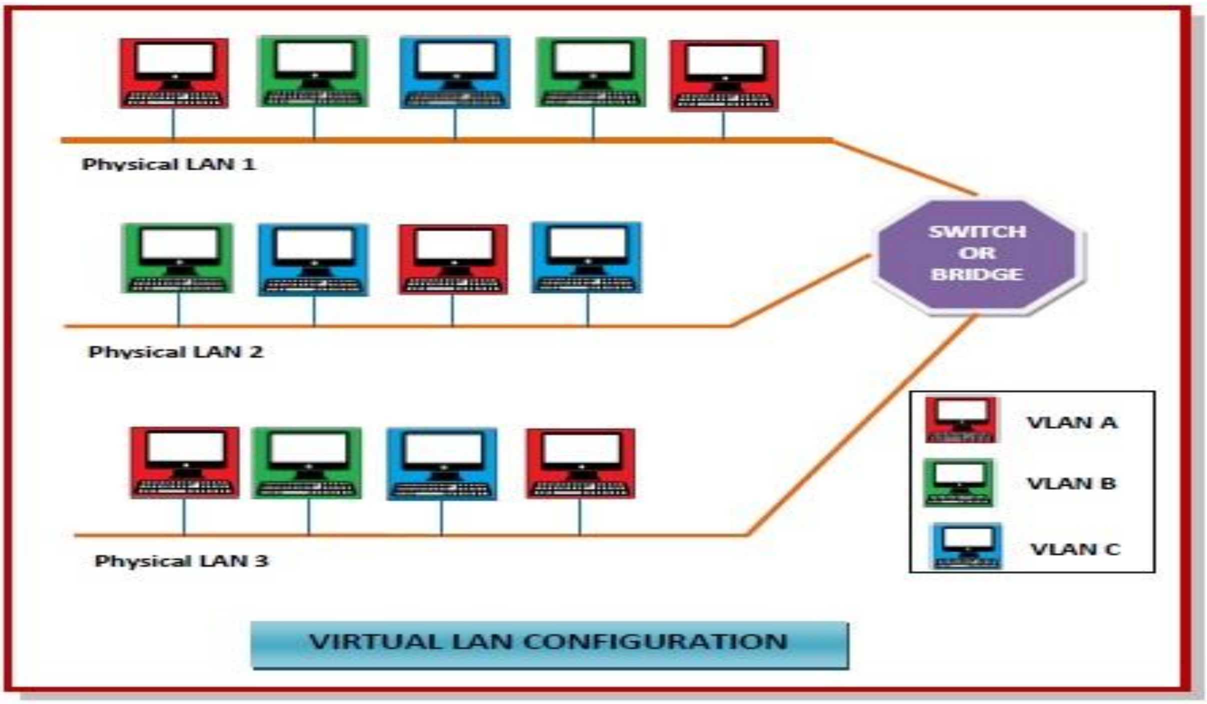
This media access control method uses free token passing to prevent a collision. Only a computer that possesses a free token, which is a small data frame, is authorized to transmit. Transmission occurs from a network terminal that has a higher priority than one with a low priority.

Token passing flourishes in an environment where a large number of short data frames are transmitted. This media access control policy is highly efficient in avoiding a collision. Possession of the free token is the only key to transmitting data by a network node. Each terminal holds this free token for a specific amount of time if the network with the high priority does not have data to transmit, the token is passed to the adjoining station in the network.

Media access control regulates how a network is accessed by computer terminals and transmits from one terminal to the other without collision. This is achieved through CSMA/CD, CSMA/CA, demand priority, or Token passing.

11. VIRTUAL LAN

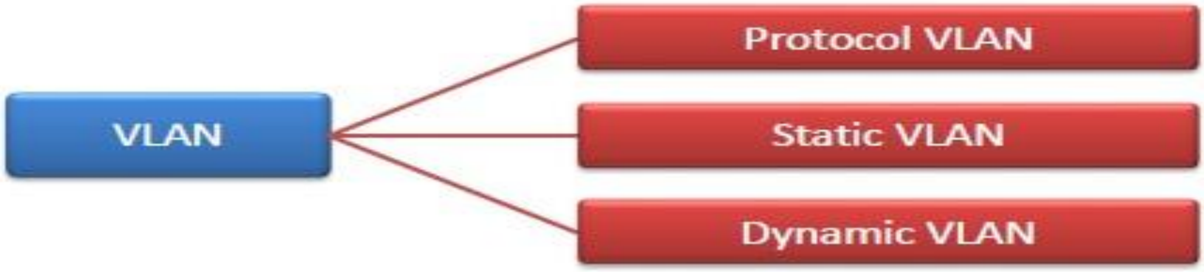
Virtual Local Area Networks or Virtual LANs (VLANs) are a logical group of computers that appear to be on the same LAN irrespective of the configuration of the underlying physical network. Network administrators partition the networks to match the functional requirements of the VLANs so that each VLAN comprise of a subset of ports on a single or multiple switches or bridges. This allows computers and devices in a VLAN to communicate in the simulated environment as if it is a separate LAN.



Features of VLANs

- A VLAN forms sub-network grouping together devices on separate physical LANs.
- VLAN's help the network manager to segment LANs logically into different broadcast domains.
- VLANs function at layer 2, i.e. Data Link Layer of the OSI model.
- There may be one or more network bridges or switches to form multiple, independent VLANs.
- Using VLANs, network administrators can easily partition a single switched network into multiple networks depending upon the functional and security requirements of their systems.
- VLANs eliminate the requirement to run new cables or reconfiguring physical connections in the present network infrastructure.
- VLANs help large organizations to re-partition devices aiming improved traffic management.
- VLANs also provide better security management allowing partitioning of devices according to their security criteria and also by ensuring a higher degree of control connected devices.
- VLANs are more flexible than physical LANs since they are formed by logical connections. This aids is quicker and cheaper reconfiguration of devices when the logical partitioning needs to be changed.

Types of VLANs



- Protocol VLAN – Here, the traffic is handled based on the protocol used. A switch or bridge segregates, forwards or discards frames the come to it based upon the traffics protocol.
- Port-based VLAN – This is also called static VLAN. Here, the network administrator assigns the ports on the switch / bridge to form a virtual network.
- Dynamic VLAN – Here, the network administrator simply defines network membership according to device characteristics.

12.Wireless LAN (802.11)

Wireless LANs are those Local Area Networks that use high frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage. Most WLANs are based upon the standard IEEE 802.11 or WiFi.

IEEE 802.11 Architecture

The components of an IEEE 802.11 architecture are as follows

1) Stations (STA) − Stations comprise all devices and equipments that are connected to the wireless LAN. A station can be of two types:

- Wireless Access Pointz (WAP) − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
- Client. − Clients are workstations, computers, laptops, printers, smartphones, etc.

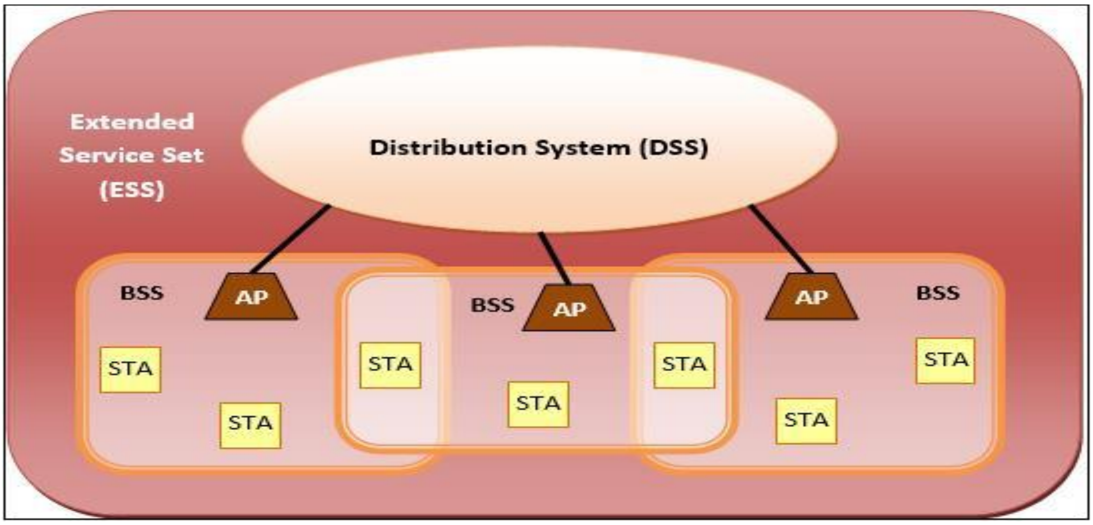
Each station has a wireless network interface controller.

2) Basic Service Set (BSS) −A basic service set is a group of stations communicating at physical layer level. BSS can be of two categories depending upon mode of operation:

- Infrastructure BSS − Here, the devices communicate with other devices through access points.
- Independent BSS − Here, the devices communicate in peer-to-peer basis in an ad hoc manner.

3) Extended Service Set (ESS) − It is a set of all connected BSS.

4) Distribution System (DS) − It connects access points in ESS.



Advantages of WLANs

- They provide clutter free homes, offices and other networked places.
- The LANs are scalable in nature, i.e. devices may be added or removed from the network at a greater ease than wired LANs.

- The system is portable within the network coverage and access to the network is not bounded by the length of the cables.
- Installation and setup is much easier than wired counterparts.
- The equipment and setup costs are reduced.

Disadvantages of WLANs

- Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.
- Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.
- WLANs are slower than wired LANs.

13.PHYSICAL LAYER: DATA AND SIGNALS

Physical Layer

 The main functionality of the physical layer is to transmit the individual bits from one node to another node.

 It is the lowest layer of the OSI model.

 It establishes, maintains and deactivates the physical connection.

 It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

 Line Configuration: It defines the way how two or more devices can be connected physically.

 Data Transmission: It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on thenetwork.

 Topology: It defines the way how network devices are arranged.

 Signals: It determines the type of the signal used for transmitting the information.

Data-Link Layer

 This layer is responsible for the error-free transfer of data frames.

 It defines the format of the data on the network.

 It provides a reliable and efficient communication between two or more devices.

 It is mainly responsible for the unique identification of each device that resides on a local network.

*List out the functions of the Data Link Layer(Apr/May 2021)(2)

Functions of the Data-link layer

 Physical Addressing: The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.

 Flow Control: Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
Error Control: Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.

 Access Control: When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

Network Layer

 It is a layer 3 that manages device addressing, tracks the location of devices on the network.

 It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.

 The Data link layer is responsible for routing and forwarding the packets.

 Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.

 The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

 Addressing: A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.

 Routing: Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.

Transport Layer

 The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.

 The main responsibility of the transport layer is to transfer the data completely.

 It receives the data from the upper layer and converts them into smaller units known assignments.

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

Functions of Transport Layer:

 Service-point addressing: Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.

 Segmentation and reassembly: When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

 Connection control: Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.

 Flow control: The transport layer also responsible for flow control but it is performed end-to- end rather than across a single link.

 Error control: The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

Session Layer

 It is a layer 3 in the OSI model.

 The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

 Dialog control: Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.

 Synchronization: Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

Presentation Layer

 A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.

 It acts as a data translator for a network.

 This layer is a part of the operating system that converts the data from one presentation format to another format.

 The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

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

 Encryption: Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.

 Compression: Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

Application Layer

 An application layer serves as a window for users and application processes to access network service.

 It handles issues such as network transparency, resource allocation, etc.

 An application layer is not an application, but it performs the application layer functions.

 This layer provides the network services to the end-users.

Functions of Application layer:

 File transfer, access, and management (FTAM): An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.

 Mail services: An application layer provides the facility for email forwarding and storage.

 Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

15.TRANSMISSION MEDIA

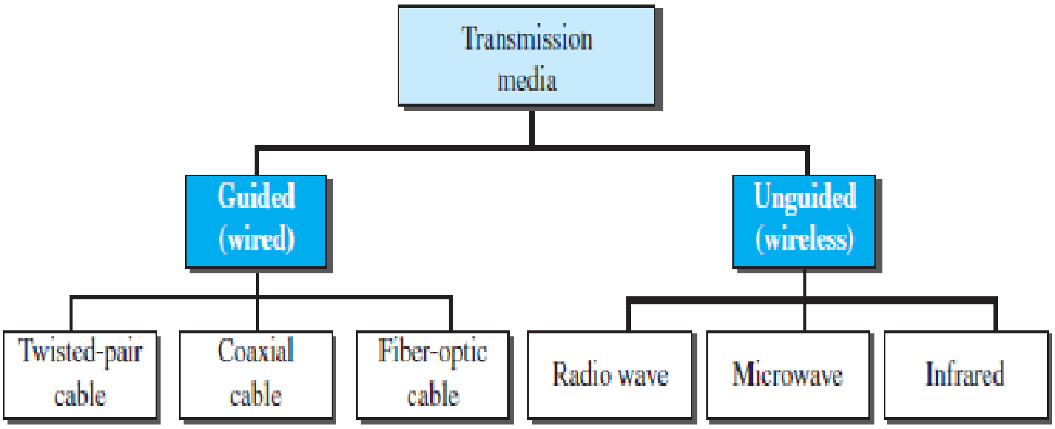
Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.

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

 It is a physical path between transmitter and receiver in data communication.

 In a copper-based network, the bits in the form of electrical signals.

 In a fiber based network, the bits in the form of light pulses.



1. Guided Media:

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

 High Speed

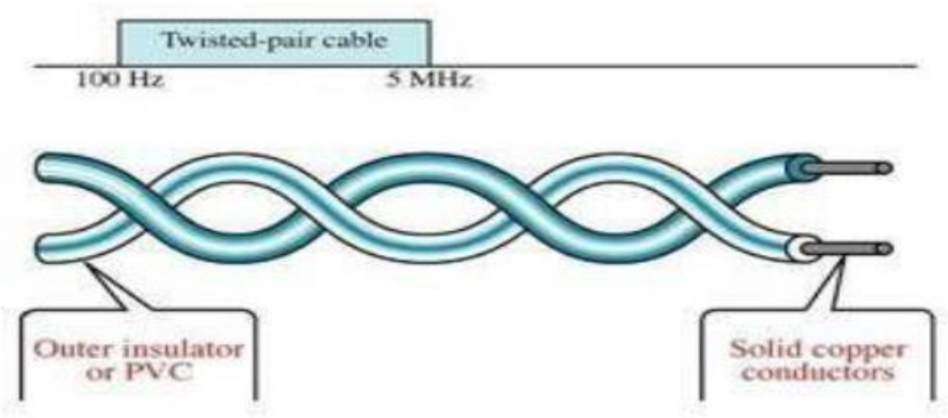
 Secure

 Used for comparatively shorter distances

There are 3 major types of Guided Media

(i) Twisted Pair Cable –

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types



1. Unshielded Twisted Pair(UTP):

This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

Advantages:

- Least expensive
- Easy to install
- High speed
- capacity

Disadvantages:

- Susceptible to external interference
- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation

2. Shielded Twisted Pair (STP):

This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

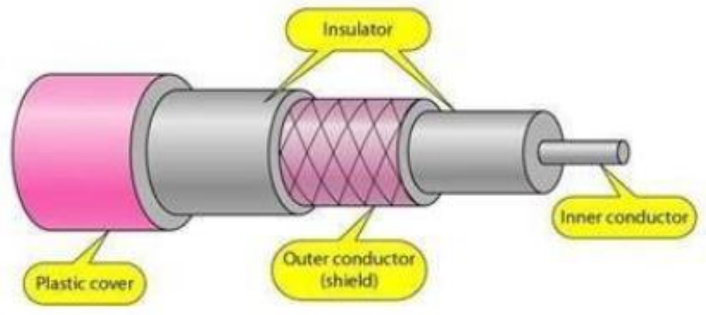
Advantages:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparatively faster Disadvantages:
- Comparatively difficult to install and manufacture
- More expensive
- Bulky

(ii) Coaxial Cable –

It has an outer plastic covering containing 2 parallel conductors each having a separate insulated protection cover. Coaxial cable transmits information in two modes:

- Baseband mode(dedicated cable bandwidth)
- Broadband mode(cable bandwidth is split into separate ranges).
- Cable TVs and analog television networks widely use Coaxial cables.



Advantages

 High Bandwidth

 Better noise Immunity

 Easy to install and expand

 Inexpensive

Disadvantages:

 Single cable failure can disrupt the entire network

(iii) Optical Fiber Cable –

It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for transmission of large volumes of data.

Advantages:

 Increased capacity and bandwidth

 Light weight

 Less signal attenuation

 Resistance to corrosive materials

Disadvantages:

 Difficult to install and maintain

 High cost

 Fragile

 unidirectional, i.e., will need another fiber, if we need bidirectional communication

2. Unguided Media:

It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

Features:

 Signal is broadcasted through air

 Less Secure

 Used for larger distances

There are 3 major types of Unguided Media:

(i) Radiowaves –

These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios
andcordless phones use Radio waves for transmission.
Further Categorized as (i) Terrestrial and (ii) Satellite.

(ii) Microwaves –

It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

(iii) Infrared –

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It isused in TV remotes, wireless mouse, keyboard, printer, etc.

16.SWITCHING -CIRCUIT SWITCHING.

*distinguish between packet switching and circuit switching. (apr/may 2017)(2)

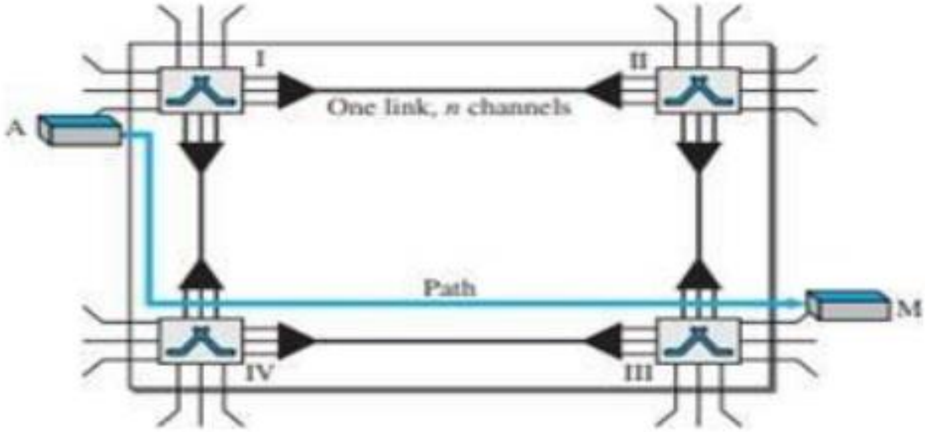
*describe circuit switching and packet switching with examples.(nov/dec 2019)(13)

*differentiate circuit switching and packet switching with suitable application example (nov/dec 2021)(2)

*differentiate circuit switching networks and packet switching networks (nov/dec2020) (2)

A circuit-switched network consists of a set of switches connected by physical links. A

connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link. Each link is normally divided into n channels by using FDM or TDM. Figure shows a trivial circuit-switched network with four switches and four links. Each link is divided into n (n is 3 in the figure) channels by using FDM or TDM.



Circuit switching takes place at the physical layer.

 Before starting communication, the stations must make a reservation for the resources to be used during the communication. These resources, such as channels (bandwidth in FDM and time slots in TDM), switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the teardown phase.

 Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and received by the destination station, although there may be periods of silence.

 There is no addressing involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM). Of course, there is end-to end addressing used during the setup phase, as we will see shortly

Three Phases:

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

connection setup, data transfer, and connection teardown.

Setup Phase :

Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches.

Data-Transfer Phase :l

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase:

When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

Delay

Although a circuit-switched network normally has low efficiency, the delay in this type of network is minimal. During data transfer the data are not delayed at each switch; the resources are allocated for the duration of the connection. Figure shows the idea of delay in a circuit-switched network when only two switches are involved.

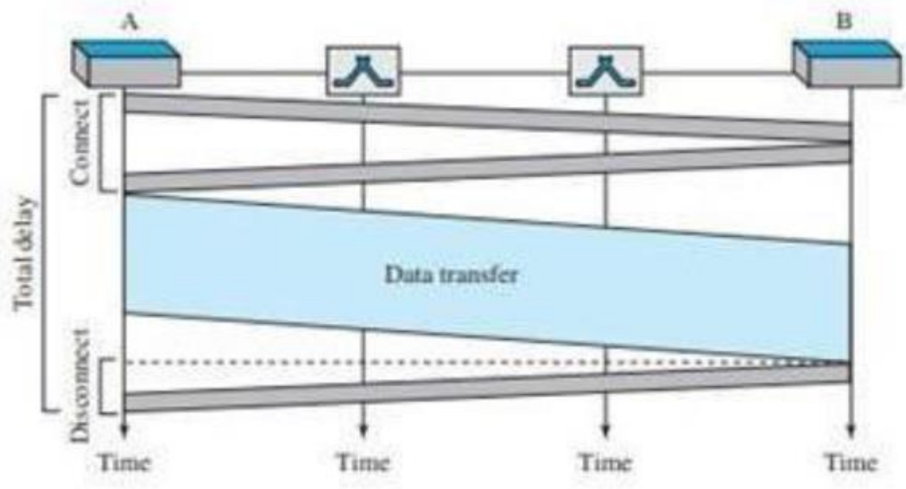


Figure shows, there is no waiting time at each switch. The total delay is due to the time needed to create the connection, transfer data, and disconnect the circuit. The delay caused by the setup is the sum of four parts: the propagation time of the source computer request (slope of the first gray box), the request signal transfer time (height of the first gray box), the propagation time of the acknowledgment from the destination computer (slope of the second gray box), and the signal transfer time of the acknowledgment (height of the second gray box). The delay due to data transfer is the sum of two parts: the propagation time (slope of the colored box) and data transfer time (height of the colored box), which can be very long.

The third box shows the time needed to tear down the circuit. We have shown the case in which the receiver requests disconnection, which creates the maximum delay.