Unit-3

Data link Layer (DLL)

The data link layer (dll) transforms the physical layer, a raw transmission facility, to a link responsible for node-to-node communication. Specific responsibilities of the data link layer include framing, addressing, flow control, error control and media access control. The data link layer divides the stream of bits received from the network layer into managable data units called frames.

The data link layer adds a header to the frame to define the address of the sender and receiver of the frame. When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

⊛ Functions:

i) Framing → The data link layer receives the stream of bits from the network layer divides into managable data units called frames.

ii) Physical addressing → If frames are to be distributed to different stations on the network. To define the physical address of the sender and/or receiver of the frame, the DDL adds a header to the frame.

iii) Flow Control → If the rate at which the data are consumed by the receiver is less than the rate produced by the sender, the data link layer deals with a flow control mechanism to prevent overrun the receiver.

iv) Error Control → The data link layer also deals with damaged or lost frames. By adding mechanisms to detect and retransmit lost frames increases reliability.

v) Access Control → When more than two or two devices are connected to the common link, data link layer protocals are necessary to determine which device has contol over the link at any point of time.

The data link layer (dll) is divided into two sub layers as follows:

ⓐ. Logical Link Control (LLC):- It is the upper sublayer of the data link layer of the open system interconnections (OSI) refrence model for data transmission. It acts as an interface between the network layer and the medium access control (MAC) sublayer of the data link layer. It is mainly used for its multiplexing property. It allows several network protocols to operate simultaneously within a multipoint network over the same network medium. LLC provides node-to-node flow and error control. Frame Sequence Numbers are assigned by LLC.

ⓑ Media Access Control (MAC):- It is the sublayer that controls the hardware responsible for interaction with the wired, optical or wireless transmission medium. It provides flow control and multiplexing for the transmission medium. It provides a control abstraction of the physical layer such that the complexities of physical link control are invisible to the LLC and upper layers of network stack. It encapsulates higher-level frames into frames appropriate for the transmission medium.

⊛ Framing and Flow Control Mechanisms:-

Framing → Frames are the units of digital transmission particularly in computer networks and telecommunications. Frame is continuously used in time division multiplexing process. Framing is the point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits. framing is a function of the data link layer. Frames have headers that contain information such as error-checking codes. There are two types of framing:

i) Fixed size → The frame is of fixed size and there is no need to provide boundaries to the frame, length of the frame itself acts as delimiter.

ii) Variable size → In this there is need to define end of frame as well as beginning of next frame to distinguish.

Flow Control: It is a design issue at data link layer. It is technique that generally observes 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.

Flow control is basically technique that gives permission to two of stations that are working and processing at different speeds to just communicate with one another. It is actually set of procedures that explains sender about how much data or frames it can transfer before data overwhelms receiver.

Flow Control Mechanisms:

1) **Stop-and-wait ARQ:** It is a method used in communication to send information between two connected devices. It ensures that information is not lost and received in the correct order. A stop-and-wait ARQ sends one frame at a time. After sending each frame, the sender doesn't send any frames until it receives an acknowledgement (ACK) signal. After receiving a good frame, the receiver sends an ACK. If the ACK does not reach the sender before a certain time, known as the timeout, the sender sends the same frame again.

In this case, the sender resends the same packet. The sender, waiting for a single ACK, receives two ACKs, which may cause problems if it assumes that the second ACK is for the next frame in the sequence. To avoid these problems, the most common solution is to define a 1 bit sequence number in the header of the frame. This sequence number alternates (from 0 to 1) in subsequent frames.

Stop-and-wait ARQ is inefficient compared to other ARQs, because the time between packets is twice the transit time. The throughput on the channel is a fraction of what it could be. To solve this problem, one can send more than one packet at a time. This is what is done in GO-BACK-N ARQ and the Selective Repeat mechanisms.

9) Piggybacking → Piggybacking is a technique that controls the flow of information in both direction thereby improving the efficiency of the bidirectional protocols. When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B and vice-versa. Piggybacking combines the data frames and control info into the same frames.

Merit → It can save bandwidth since the data frame and ACK frame can be combined into just one frame.

Demerit → The algorithm is complicated because it needs to combine two arrival events into one.

10) Go-Back-N ARQ → It is an specific technique of the ARQ protocol, in which the sending process continues to send a number of frames specified by a window size even without receiving an ACK packet from the receiver. The receiver process keeps track of the sequence number of the next frame it expects to receive, and sends that number with every ACK it sends. The receiver will discard any frame that does not have the exact sequence number it expects and will resend an ACK for the last correct in-order frame.

Once the sender has sent all of the frames in its window, it will detect that all of the frames since the first lost frame are outstanding and will go back to sequence number of the last ACK it received from the receiver process and fill its window starting with that frame and continue the process over again.

Go-Back-N ARQ is a more efficient use of a connection than stop and wait ARQ since unlike waiting for an acknowledgement for each packets, the connection is still being utilized as packets are being sent.

Selective Repeat ARQ → In this mechanism unlike Go Back N ARQ, the receiving process will continue to accept and acknowledge frames sent after an initial error; this is the case of the sliding window protocal with both transmit and receive window sizes greater than 1.

The receiver process keeps track of the sequence number of the earliest frame it has not received, and sends that number with every ACK it sends. If a frame from the sender does not reach the receiver, the sender continues to send subsequent frames until it has emptied its window.

The receiver continues to fill its receiving window with the subsequent frames, replying each time with an ACK containing the sequence number of the earliest missing frames. Once the sender has sent all the frames in its window, it re-sends the frame number given by the ACKs, and then continues where it left off.

Maximum Window Size = Sequence Number Space / 2

⊛. Error Detection and Correlation Techniques:-

Data can be corrupted during transmission. Some applications require that errors be detected and corrected. Some applications can tolerate a small level of error. For example, random errors in audio or video transmissions may be tolerable, but when we transfer text, we expect a very high level of accuracy.

In a single-bit error, a 0 is changed 1 or a 1 to a 0. In a brust error, multiple bits are changed. For example, a 11100 s brust of impulse noise on a transmission with a data rate of 1200 bps might change all or some of the 12 bits of information. In a single-bit error, only 1 bit in the data unit has changed. A brust error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

Redundancy → The central concept in detecting or correcting errors is redundancy. To be able to detect or correct errors, we need to send some extra bits with our data. These redundant bits are added by the sender and removed by the receiver.

@. Error Detection:-

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver end fails, the bits are considered corrupted.

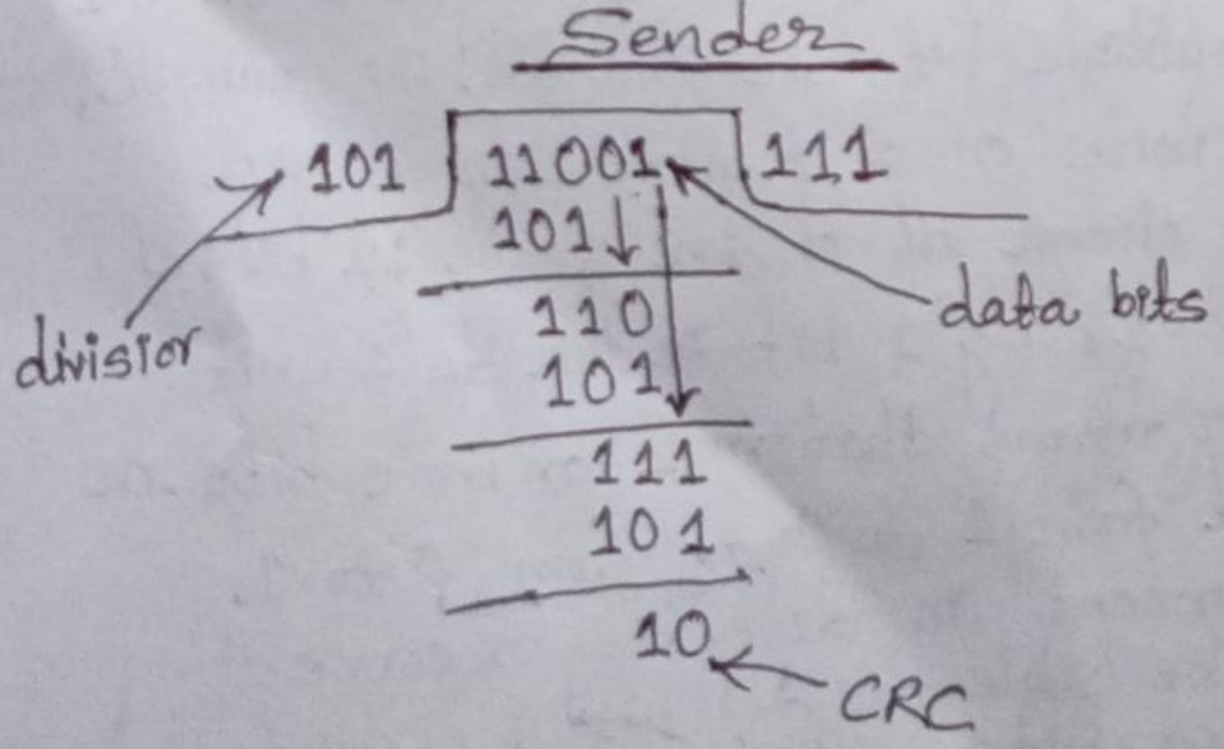
1) **Parity Check:** One extra bit is sent along with the original bits to make number of 1s either ever in case of even parity, or odd in case of odd parity.

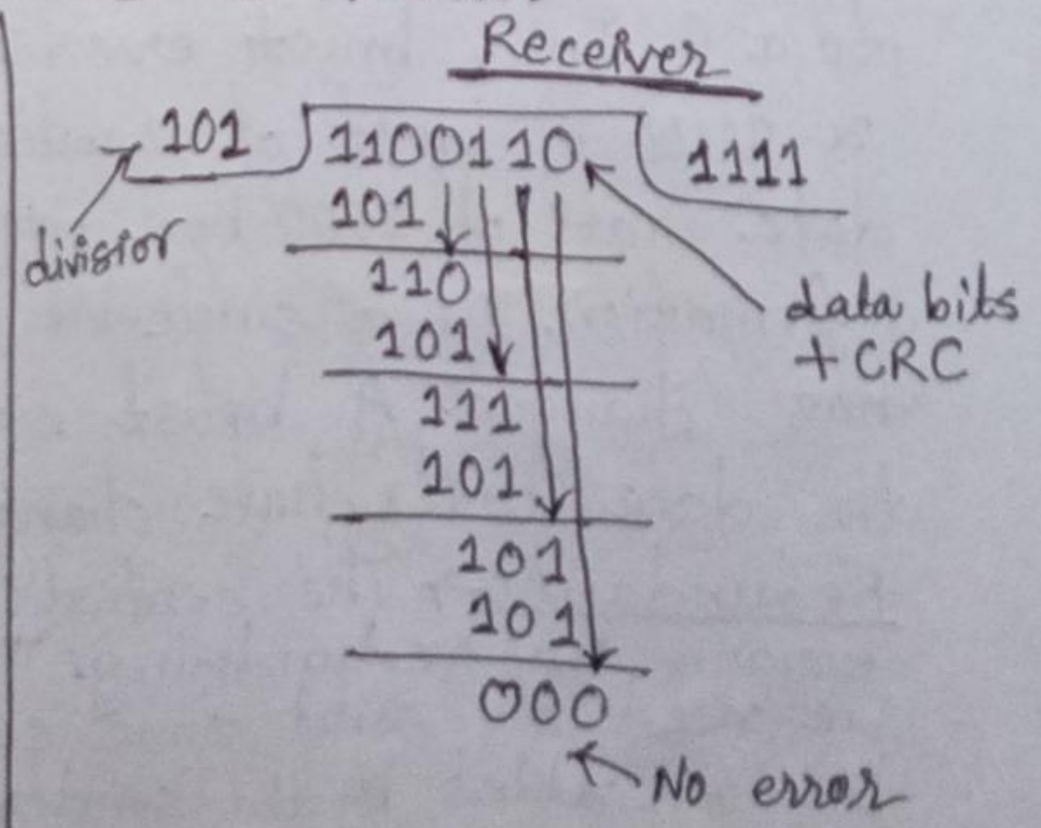
The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even. If the number of 1s is odd, to make it even a bit with value 1 is added.

The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

2) **Cyclic Redundancy Check (CRC):-**

CRC technique involves binary division of the data being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.





At the other end, the receiver performs division operation ~~one~~ on codewords using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occured in transit.

(b). Error Correction :-

In digital world, error correction can be done in two ways:

→ Backward error correction: When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.

→ Forward error correction: When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

For correcting the errors, one has to know the exact position of the error. To achieve this, we have to add some additional redundant bits. Suppose r is the number of redundant bits and d is the total number of the data bits. The number of redundant bits r can be calculated by using formula: $2^r >= d+r+1$

For example:- If the value of d is 4, then the possible smallest value that satisfies the above relation would be 3.

Hamming Code :- To determine the position of the bit which is in error, a technique developed by R.W Haming is the Haming code which can be applied to any length of the data unit and uses the relationship between data units and redundant units.

Steps for Hamming code

→ An information of d bits are added to the redundant bits r to form d+r.

→ The location of each of the (d+r) digits is assigned a decimal value.

→ The r-bits are placed in the positions $2^0, 2^1, \ldots, 2^{k-1}$.

→ At the receiving end, the parity bits are recalculated. The decimal value of the parity bits determines the position of an error.

For example:- Suppose the original data is 1010 which is to be sent. Then,

Total number of data bits 'd' = 4

Number of redundant bits $r = 2^r >= d+r+1$

i.e, $2^r >= 4+r+1$

Therefore, the value of r is 3 that satisfies the above relation.

Total number of bits = d+r = 4+3 = 7.

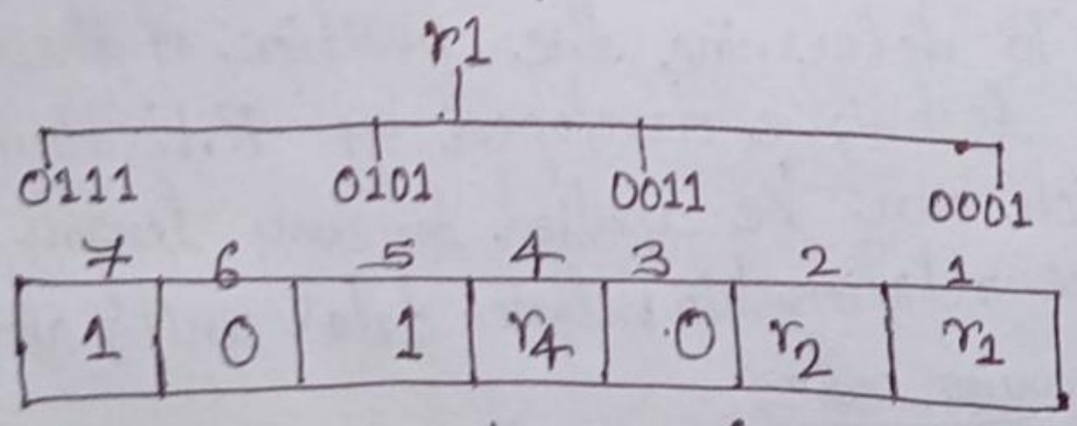
Determining the position of redundant bits:

The number of redundant bits is 3. The three bits are represented by r1, r2, r4. The position of the redundant bits are calculated with corresponds to the raised power of 2. Therefore, their corresponding positions are. 2^0, 2^1 and 2^2.

The position of r1 = 1
The position of r2 = 2
The position of r4 = 4.

Determining the parity bits:

For r1 bit → The r1 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the first position.



We observe from above figure that the bit positions that includes 1 in the first position are 1,3,5,7. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r1 is even, therefore the value of the r1 bit is 0.

⇒ Similarly for determining r2 bit we perform a parity check on the bit positions whose binary representation includes 1 in the second position. Similarly for r4 bit.

⊛ Checksumming Method: It is a error detection scheme, where data is divided into k segments each of m bits. In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum. The checksum segment is sent along with the data segments.

At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented. If the result is zero, the received data is accepted; otherwise discarded.

Example:

Original data

10011001	11100010	00100100	10000100
1	2	3	4

k=4, m=8

Sender

1→ 10011001
2→ 11100010
(1)01111011
↳ 1
01111100
3→ 00100100
10100000
4→ 10000100
(1)00100100
↳ 1
Sum: 00100101
CheckSum: 11011010

Receiver

1→ 10011001
2→ 11100010
(1)01111011
↳ 1
01111100
3→ 00100100
10100000
4→ 10000100
(1)00100100
↳ 1
00100101
1101 1010
Sum: 1111 1111
Complement: 0000 0000

Conclusion: Accept Data

⊛ Channel Allocation Techniques:-

Channel allocation is a process in which a single channel is divided and alloted to multiple users in order to carry user specific tasks. Channel allocation problem can be solved by two schemes: static channel allocation and dynamic channel allocation.

ⓐ Static Channel allocation in LANs and MANs:

It is the traditional approach of allocating a single channel among multiple competing users frequency division multiplexing (FDM). If there are N users, the bandwidth is divided into N equal ~~sized pro~~ portions each user being assigned one portion. Since each user has a private frequency band, there is no interface between users.

$$T = 1/(U*C-L)$$

$$T(FDM) = N*T(1/U(C/N)-L/N)$$

where, T = mean time delay,
C = capacity of channel,
L = arrival rate of frames,
1/U = bits/frame,
N = number of sub channels,
T(FDM) = Frequency Division Multiplexing Time.

ⓑ Dynamic ~~Chall~~ Channel Allocation:

Dynamic channel allocation is a strategy in which channels are not permanently allocated to the cells. When a user makes a call request then Base Station (BS) send that request to the Mobile Station Center (MSC) for the allocation of channels or voice channels. This way the likelihood of blocking calls is reduced. As traffic increases more channels are assigned and vice-versa.

ⓐ Multiple Access Protocal:

When nodes are connected and use a common link called a multipoint we need multiple access protocol to coordinate access to the link. It is of three types: Random access protocols, controlled access protocols and Channelization protocols.

1) Random Access Protocol:-

In this method no node is superior to another node and none is assigned the control over another. Any node can send data depending on medium's state (idle or busy). It has two features:-

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

The random access protocols are further subdivided as;

a) **ALOHA:-** The aloha protocol was designed as a part of a project at the University of Hawaii. It provided data transmission between computers on several of the Hawaiian Islands involving packet radio networks. Aloha is a multiple access protocol at the data link layer and proposes how multiple terminals access the medium without interference or collision. There are two different versions of ALOHA as follows:-

i) **Pure ALOHA** → Pure Aloha is an un-slotted, decentralized and simple to implement protocol. In pure ALOHA, the stations simply transmit frames whenever they want data to send. It does not check whether channel is busy or not before transmitting. In case, two or more stations transmit simultaneously, collision occurs and frames are destroyed.

Whenever any station transmits frame, it expects acknowledgement from the receiver. If it is not received within specified time, the station (i.e, node) assumes that frame has been destroyed. Then, the station waits for random amount of time and sends frame again. This randomness helps in avoiding more collisions. This scheme works well in small networks where the load is not much. But it is not suitable for largely loaded networks. This led to the development of Slotted Aloha.

Pure ALOHA vunerable Time = 2 × Frame Transmission Time (T_{fr}).

Throughput for pure ALOHA (S_{pure}) = $G \times e^{-2G}$

where G is no. of stations wants to transmit in T_{fr}.

Maximum throughput $(S_{pure})_{max} = 0.184$ for $G = 0.5$

Which means, in Pure ALOHA, only about 18.4% of time is used for successfull transmissions.

ii) **Slotted ALOHA** → In slotted ALOHA, the time of shared channel is divided into discrete intervals called slots. The stations are eligible to send a frame only at the beginning of the slot and only one frame per slot is sent. If any station is not able to place the frame onto the channel at the beginning of the slot, it has to wait until the beginning of the next time slot.

Slotted ALOHA vulnerable Time = Frame Transmission Time (T_{fr}).
Throughput for slotted ALOHA ($S_{slotted}$) = $G \times e^{-2G}$
where G is no. of stations wants to transmit in T_{fr} slot.
Maximum throughput $(S_{slotted})_{max} = 0.368$ for $G = 1$.
Which means, in slotted ALOHA, about 36.8% of the time is used for successful transmissions.

(b) Carrier Sense Multiple Access (CSMA):

It 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.

CSMA access modes:-

1) 1-persistent → The node senses the channel, if idle sends the data, otherwise it continiously keeps on checking the medium for being idle and transmits unconditionally as soon as the channel gets idle.

2) Non-persistent → The node senses the medium, if idle sends the data with p probability. If the data is not transmitted then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. It is used in WiFi and packet radio systems.

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

This method adds on to the CSMA algorithm to deal with collision. In CSMA/CD, the size of a frame must be large enough so that collision can be detected by sender while sending the frame. So, the frame transmission dealy must be at least two times the maximum propagation delay.

④ Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA):

It was invented for wireless networks. The process of collission detection involves sender receiving acknowledgement signals. If there is just one signal then the data is successfully sent but if there are two signals then it means a collision has occured. To distinguish between these two cases, collision must have a lot of impact on received signal.

CSMA/CA avoids collision by:

i) Interframe space → Station waits for medium to become idle and if found idle does not immediately send data rather it waits for a period of time called interframe space or IFS. After this time it again checks medium for being idle.

ii) 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 not found idle.

iii) Acknowledgement → The sender re-transmits the data if acknowledgement is not received before time-out.

⑤. Ethernet Standards:

(802 denotes ethernet standard)

IEEE 802 specifies to a group of IEE standards. IEEE standards 802 are used for controlling the Local Area Network and Metropolitan Area Network. The user layer in IEEE 802 is serviced by the two layers: data link layer and physical layer. Generally used IEEE 802 specifications are as follows:-

IEEE 802.3	IEEE 802.4	IEEE 802.5
i) The IEEE 802.3 standard determines the CSMA/CD access control protocol.	i) IEEE 802.4 describes a token bus LAN standards.	i) IEEE 802.5 describes token ring standards.
ii) ~~Topoly~~ Topology used in IEEE 802.3 is Bus Topology.	ii) Topology used in IEEE 802.4 is Bus Topology.	ii) Topology used in IEEE 802.5 is Ring Topology.
iii) It has frame format size of 1572 bytes.	iii) It has frame format size of 8202 bytes.	iii) It has frame format size equal to variable size.

iv) Size of data field is 0 to 1500 bytes. v) Minimum frame required is 64 bytes. vi) Modems are not required. vii) Protocol is very simple.	iv) Size of data field is 0 to 8182 bytes. v) It can handle short minimum frames. vi) Modems are required. vii) Protocol is extremely complex.	iv) No limit is of the size of the data field. v) It supports both short and large frames. vi) Modems are required. vii) Protocol is moderately complex.

⊛. Wireless LAN:

@ Spread Spectrum → Spread Spectrum techniques are methods by which a signal (e.g. electrical, electromagnetic etc.) are generated with a particular bandwidth which spread in frequency domain resulting a signal with wider bandwidth. These techniques are used for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference, noise, and jamming, to prevent detection and to enable multiple-access communications.

ⓑ Bluetooth → It is a wireless technology standard for exchanging data over short distances. It can connect several devices overcomming problems of synchronization. Bluetooth was standardized as IEEE 802.15.1 but the standard is no longer maintained. It is managed by the Bluetooth Special Interest Group (SIG), which has more than 35,000 member companies in the areas of telecommunication, computing, networking and consumer electronics.

© Wi-Fi → Wireless-Fredility (Wi-Fi) is a family of wireless network protocols, based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet access, allowing nearby devices to exchange data by radio waves. These are the most widely used computer networks in the world used globally in laptop, tablets, mobiles, smart TVs etc.

⊛. Overview of Virtual Circuit Switching, Frame Relay & ATM:

Virtual Circuit Switching → It is a packet switching method where a path is established between the source and destination through which all packets will be routed during a call. The path is called virtual circuit because the connection appears to be a dedicated physical circuit.

Before the data transfer begins, the source and destination identify a suitable path for the virtual circuit. Additional parameters such as maximum packet size are also exchanged between the source and destination during call setup. The virtual circuit is cleared after the data transfer is completed.

Frame Relay → It is also a packet switching method that uses virtual circuits. These virtual circuits can be set up for each session or can be set up permanently. Frame Relay is designed for fiber optic cables with a very low bit error rate. Frame Relay has no error recovery and no flow control.

It is extensively used today in large corporations to interconnect the LANs between buildings. Frame relay operates at high speed (1.544 Mbps to 44.376 Mbps). It has large frame size of 9000 bytes. The damaged frame is simply dropped, there is no retransmission.

Asychronous Transfer Mode (ATM) → It is a switching technique used by telecommunication networks that ~~used~~ uses asychronous time-division multiplexing to encode data into small, fixed-sized cells. This is different from Ethernet or internet which use variables packet sizes for data or frames.

The ATM provides data link layer services that run on the OSIs layer 1 physical links. It functions much like small-packet switched and circuit-switched networks, which makes it idle. ATM services have four different bit rate choices:

- → Available bit rate
- → Constant bit rate
- → Unspecified bit rate
- → Variable bit rate.

⊛. DLL Protocol: HDLC, PPP

(read comparing each points of both as differences, so will be easier to read)

(HDLC) High-Level Data Link Control → HLDC stands for high-level data link control. HDLC is a bit oriented protocol. HDLC is implemented by point-to-point configuration and also multi-point configurations. Dynamic addressing is not offered by HDLC. HDLC is used in synchronous media. HDLC is not compatible with non-Cisco devices. HDLC does not provide link authentication. HDLC is more costly comparatively.

8	8	8	>=0	16	8
Flag	Address	Control	Data	Checksum	Flag

Frame Format for HDLC Protocol.

(PPP) Point-to-Point Protocol → PPP stands for Point-to-Point Protocol. PPP is a byte oriented protocol. PPP is implemented by Point-to Point configuration only. Dynamic addressing is offered by PPP. PPP is used in synchronous media as well as asynchronous media. PPP is compatible with non-Cisco devices. PPP provides link authentication using various protocols. PPP is comparatively less costly.

1	1	1	1 or 2	Variable	2 or 4	1
Flag	Address	Control	Protocol	Payload	Checksum	Flag

Frame Format for PPP Protocol.