Unit-3 Data Link Layer (DLL)

-Ankit Pangeni

DATE

* Introduction

→ Data link layer is the second layer of OSI model. It hides the details of underlying hardware and represents itself to upper layer as a medium to communicate.

→ It is responsible for node to node delivery of message.

→ The main function of this layer is to define the format of data on the network.

→ Some specific responsibilities of dll include framing addressing, flow control, error control and media access control.

* Functions of DLL

i) Framing → The DLL receives the stream of bits from the network layer & divides into to manageable 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 DLL 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 dll deals with the flow control mechanism to prevent overrun the receiver.

classmate

PAGE

DATE

iv) Error control:- The DLL also deals with damaged or lost frames by adding various mechanisms to detect and retransmit lost frames which increases reliability.

v) Access control:- When two or more devices are connected to the common link, dll ~~provides~~ protocols are necessary to determine which device has control over the link at any point of time.

* Overview of Logical Link Control & Media Access Control.

Data link layer has two sub-layers:

- Logical Link Control: It deals with protocols, flow-control, and error control
- Media Access Control: It deals with actual control of media.

Logical Link Control (LLC)

LLC Sublayer provides the logic for the data link. Thus it controls protocols, synchronization, flow control and error checking functions of the data link layer. It provides accessing and control of the data link. It specifies which mechanisms are to be used for addressing stations over the transmission

medium & for controlling the data exchanged betwe
the originator and recipient machines. LLC provide
node-to-node flow & error control. Frame sequence numbers ar
assigned by LLC.

Media Access Control (MAC)

→ This sublayer is sometimes referred to as the sublayer that determines who is allowed to acce the media at any one time. Other times it refers to a frame structure with mac address inside.
→ This sublayer controls the hardware responsible for interaction with the wired, optical or wireless transmission medium. It provides flow control and multiplexing for transmission medium.
→ It also determines where one frame of data ends & the next one starts. It encapsulates higher-level frame into frames appropriate for the transmission medium
→ It provides a control abstraction of physical link control such that complexities of physical link control are invisible to LLC & upper layers of network stack.

* Framing and Flow Control Mechanisms

- Stop-and-wait ARQ
- Piggybacking
- Go-back-N ARQ
- Selective Repeat ARQ

DATE

* Framing: Frames are the units of digital transmission, particularly in computer networks and telecommunications.
→ 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. However, these bits must be framed.
→ Framing is the function of data link layer which provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Frames have headers that contain information such as error checking codes.

Two types of framing:-
o Fixed size: The frame is of fixed size & there is no need to provide boundaries to the frame, length of the frame itself acts as delimiter.
o Variable size: In this type, there is a need to define the end of the frame as well as the beginning of the next frame to distinguish.

* Flow control: It is a technique that generally observe proper flow of data from sender to receiver. It is very essential because it is possible for a sender to transmit data or information at very fast rate and hence receiver can receive this information and process it.
→ It is basically a technique that gives permission to two of stations that are working & 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.

classmate PAGE

DATE

Flowcontrol Mechanisms :-

i) 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 (or data packet) at a time. After sending each frame, the sender doesn't send any frames until it receives an acknowledgement (ACK) signal from the receiver. After receiving a good error free frame, the receiver sends an ACK of next expected frame.
→ If the ACK does not reach the sender before a certain time, known as the time out, the sender sends the frame again. (Note: time out = 2 * round trip time)
→ Stop and wait for ARQ mainly implements the sliding window protocol concept with window size 1.
→ It offers error & flow control.
→ It uses sequence number for frames so that the ACK of different frames aren't mixed together.

Disadvantages/problems

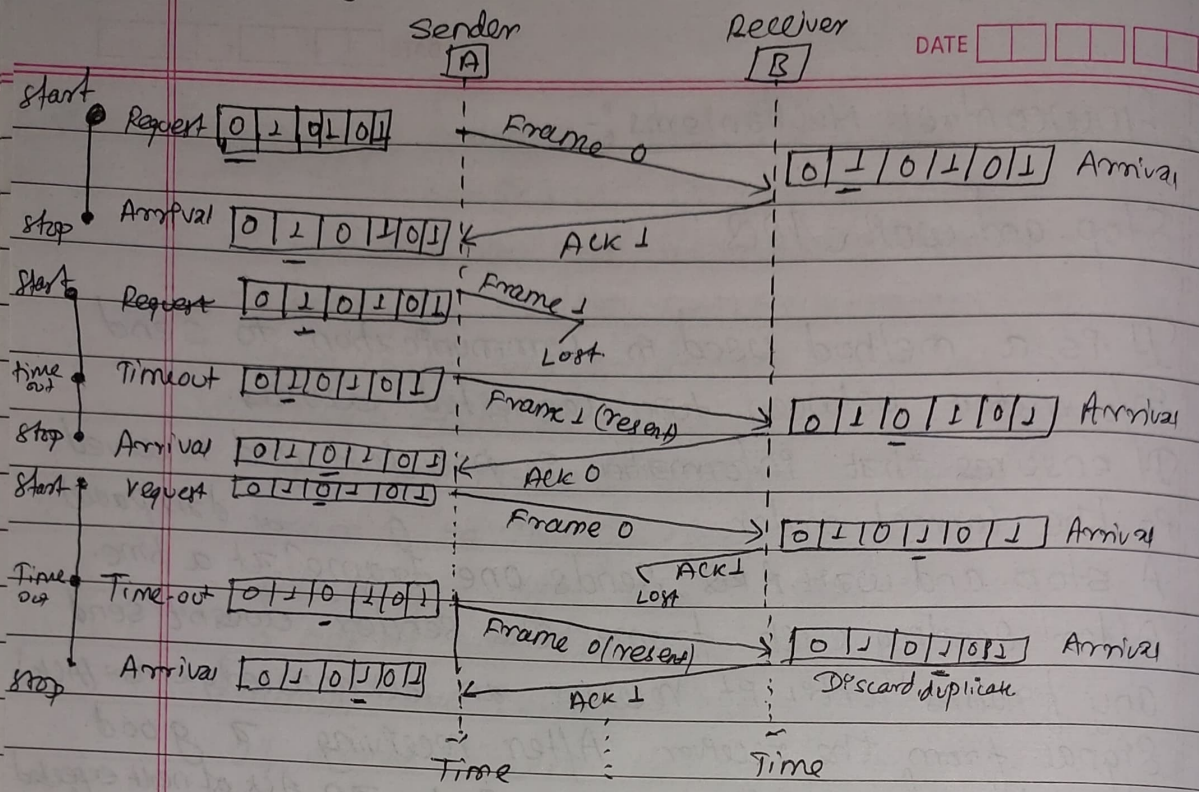
o Problem occur due to loss of data :
Suppose sender sends data & data is lost. The receiver is waiting data for a long time. Since data is not received by receiver so it doesn't send any acknowledgement since, sender doesn't receive any acknowledgement so it won't send next packet. It occurs due to loss of data.

o Problem occur due to lost acknowledgement :
Suppose receiver receives data & sends acknowledgement & ACK is lost in a network, so the sender doesn't receive any ACK. Then sender won't send next packet until ACK is received.

o Problem due to delayed data or ack.

CLASSMATE PAGE

Working: Suppose we want to send frame 01 0101 from A to B



→ Sender A sends frame 0
→ Once receiver B receives frame 0. It sends acknowledgement of next frame 1
→ Once Sender receives ACK 1, it sends frame 1 but it is lost in the network. So, ~~sender~~ receiver doesn't send any ACK. And sender waits until time out
→ Once time out is reached, Sender A resents frame 1.
→ Once receiver B receives the frame, it sends Ack for next frame 0.
→ Once Sender A receives Ack 0, It sends frame 0
→ Once receiver receives frame 0. It sends ack 1
→ The ack 1 is lost in the network.
→ Sender waits until time out and resends frame 0. But, the receiver wants the frame 1. So, it discards the frame and again sends the ack 1.
→ Once Sender receives Ack 1, it sends frame 1
and so on.

DATE

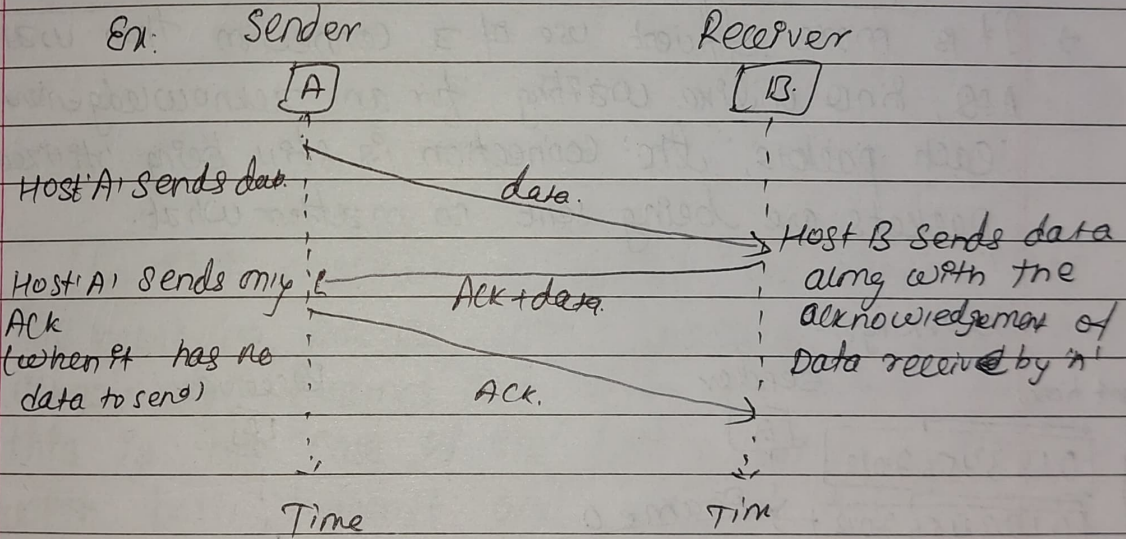
ii) Piggybacking

→ Piggybacking is a technique that controls the flow of information in both direction thereby improving the efficiency of the bidirectional protocals.

→ When a frame is carraying 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 into into the same frame.

→ In this technique, the outgoing acknowledgement is delayed temporarily



As we can see in the figure, we can see with piggybanking, a single message (Ack + data) over the wire in place of two separate messages. Piggybanking improves the efficiency of the bidirectional protocals.

Advantages:

- Makes better use of available bandwidth.
- Usage cost reduction
- Improves efficiency of data transfer.

Disadvantage: More complex.

PAGE

DATE

Go-back-N ARQ (Sliding window)

→ 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.

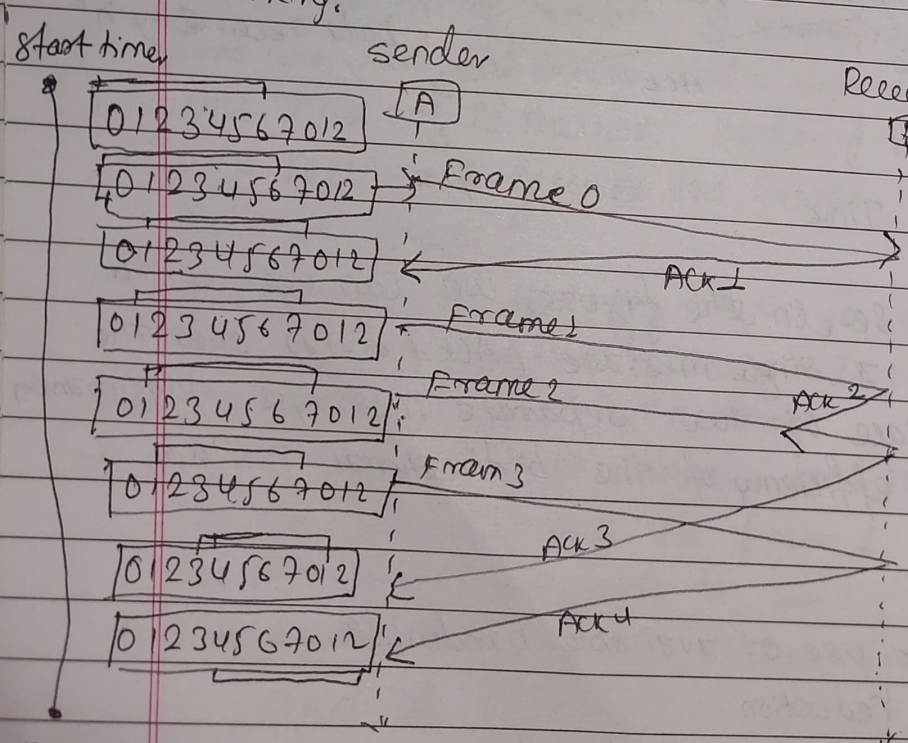
→ The receiver process keeps track of the sequence number of the next expected frame and sends that number with every ACK it sends.

→ The receiver will discard any frame that does not have the exact sequence number it expects and will resend an ACK for last correct in-order frame.

→ Note: Sender's window size is $2^m - 1$ & receiver is 1 (m: bits to represent seq. no.)

→ It is more efficient use of a connection than wait & stop ARQ, since unlike waiting for an acknowledgement for each packets, the connection is still being utilized as packets are being sent no matter what.

working:



DATE

Here, m=3 and sender's window size is $2^m - 1 = 2^3 - 1 = 7$ ie 0 to 6

→ Sender sends Frame 0, Frame 1, Frame 2, Frame 3 - - - - .

→ Receiver receives 0 & sends ack for 1.

→ Receiver receives 1 & sends ack for 2.

→ Ack 2 is lost

→ ~~Still receiver receives 2~~ sender has already sent 2

→ Receiver sends ack for 3

→ Sender sends 3

→ Here, there is no ~~acknowledgement~~ time out event because all outstanding frames are acknowledged before the timer expires. Note that although Ack 2 is lost, Ack 3 serves as both Ack 2 & Ack 3

iv) Selective 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 protocol with both transmit and 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 the frame from the sender does not reach the receiver, the sender continues to send subsequent frames until it has emptied its window.

DATE

-> 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

DATE

Error detection and correction Techniques

Network must be able to transfer data from one device to another with acceptable accuracy. For most applications, a system must guarantee that the data received are identical to the data sent. Data can be corrupted during transmission. Some applications can tolerate a small level of error. Eg: random errors in audio or video transmissions may be tolerated, but when we transfer text, we expect a very high level of accuracy.

In a single-bit error 0 is changed to 1 and vice-versa. In a burst error, multiple bits are changed. A burst error means that 2 or more bits in the data unit have changed from 1 to 0 and 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. Their presence allows the receiver to detect or correct corrupted bits. Here, a shorter group of bits may be appended to the end of each unit. This technique is called redundancy because the extra bits are redundant to the information; they are discarded as soon as the accuracy of the transmission has been determined.

CLASSMATE Draw back
- Sends n-redundant bits for n-bit message.
- Many errors are undected if both the copies are corrupted.

PAGE

DATE

Error detecting codes

It is implemented either at Data Link Layer or Transport Layer of OSI Model. Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error detecting codes which are additional data added to the given digital message to help us detect if any error has occured during transmission of the message.

Some popular techniques for error detection are:

1) Parity checks.

A parity bit is an error detection mechanism

* Single Parity Check.

SPC is a basic form of channel coding in which one extra bit is sent along with the original bits to make the number of 1s either even in case of even parity, or odd in case of odd parity.

The sender while transmitting a frame counts the number of 1s in it. If even parity is used, and no. of 1's is even, then one bit with value 0 is added. This way number of 1's remain even. If the no. of 1s is odd, to make it even, a bit with value 1 is added. The receiver simply counts the number of 1's in a frame. If count is even & even parity is used,

DATE

The frame is considered to be not-corrupted and is accepted. If the count of 1's is odd & odd parity is used, the frame is still not corrupted.

Ex: Original data	Even parity	Odd parity
00000000	0	1
10001001	1	0
01010101	0	1
11010110	1	0

* Two dimensional parity check.

Performance can be improved by using 2D parity check which organizes the data in the form of a table. Parity check bits are computed for each row, which is equivalent to the single parity check. In 2D parity check, a block of bits is divided into row, & the redundant row of bits is added to the whole block. At the receiving end, the parity bits are compared with the parity bits computed from the received data. Ex:

Original data: 11001110 10111010 01110010 01100110

11001110	1	Parity
10111010	1	
01110010	0	Row
01001010	1	
01010100	1	Column parity.

DATE

2) Checksumming methods

A checksum is an error detection technique based on the concept of redundancy. It is divided into two parts: Checksum generator & Checksum

→ **Checksum generator (Sender's side)**

A checksum is generated at the sending side. It subdivides the data into equal segments of n bits each, and all these segments are added together by using one's complement arithmetic. The sum is complemented and appended to the original data known as checksum field. The extended data is transmitted across the network

→ **Checksum Checker (Receiver's side)**

A checksum is verified at the receiving side. The receiver subdivides data into equal segments of n bits each & all these segments are added together & then this sum is complemented. If complement of sum is zero, then data is accepted otherwise rejected

Ex: Suppose the block of 16 bits is to be sent using the checksum of 8 bits [10101001 00111001]

⇒

10101001	00111001

Here, Segments (k) = 2

no. of bits in each segment (n) = 8

DATE

Now, at Sender's side

```
 1 0 1 0 1 0 0 1
+ 0 0 1 1 1 0 0 1
-----------------
 1 1 1 0 0 0 1 0
```

Now, 1's complement of
000 111 01 which is
the Checksum.

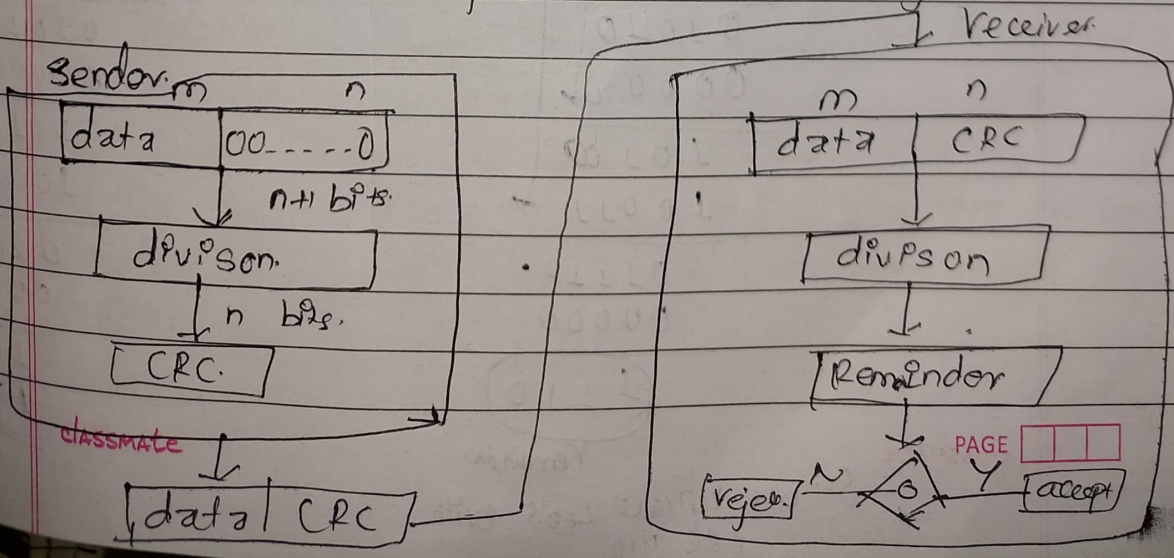
at Receiver's side

```
 1 0 1 0 1 0 0 1
+ 0 0 1 1 1 0 0 1
-----------------
 1 1 1 0 0 0 1 0
+ 0 0 0 1 1 1 0 1   (Checksum)
-----------------
 1 1 1 1 1 1 1 1
```

Now, compute 1's comp
00000000.
So, it is accepted. No error
in the transmission.

3) Cyclic Redundancy Check (CRC)

CRC is an error detection method based on binary division. In CRC, a sequence of redundant bits called cyclic redundancy check bits are appended to the end of the data, so that the resulting data unit becomes exactly divisible by second, predetermined binary number.
At the destination, the incoming data is divided by the same number. If the remainder is '0', then data is accepted, otherwise rejected.



DATE

Eg: Suppose the block of data 1101011011 is to be sent and the polynomial is x^4+x+1

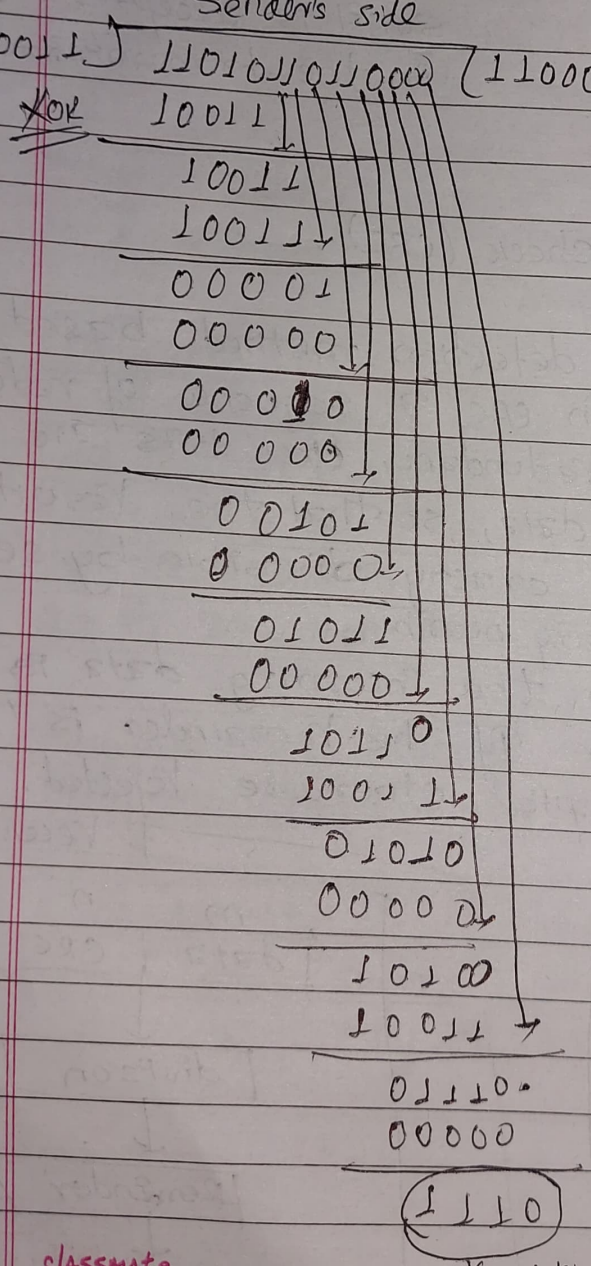
:) Given polynomial

$x^4+x+1 \Rightarrow 1\cdot x^4+0\cdot x^3+0\cdot x^2+1\cdot x+1\cdot x^0$

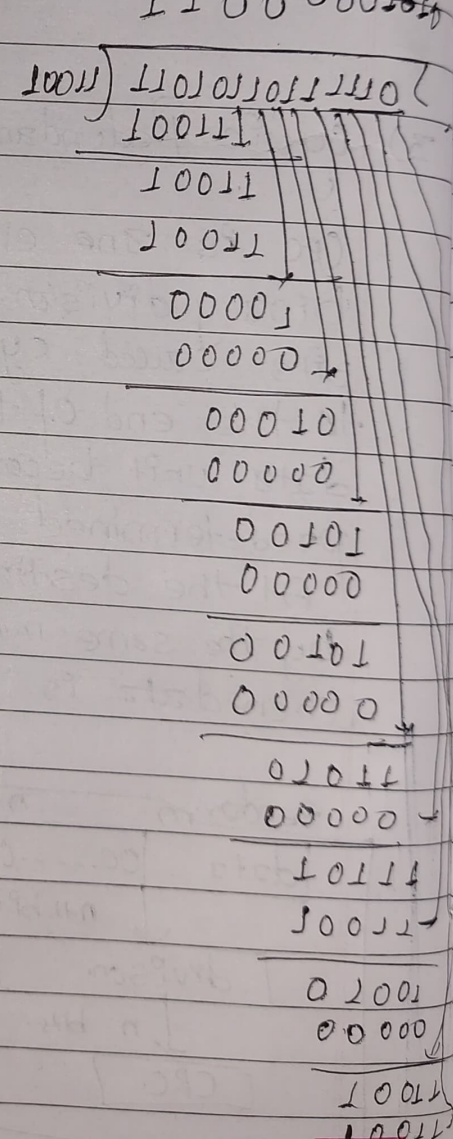
∴ Divisor = 10011 i.e. 5 bits.

Hence, the divisor is 10011 so, CRC should be n-1 bits i.e. 4 bits so, CRC = 0000 is appended to the original bit stream.

Sender's side



Receiver's side



So, we replace 4 0's with CRC 1110

classmate

PAGE

DATE

Since, remainder is 0, so the data is accepted and there is no error.

Error correction code.

* Hamming code: Error correction codes are used to detect and correct the errors when data is transmitted from sender to the receiver. Error correction is the additional ability to reconstruct the original, error-free data.

* Hamming code.

To determine the position of the bit which is in error, a technique developed by R.W Hamming is Hamming code which can be applied to data unit of any length and uses the relationship between data units and redundant units. It is used to detect and correct single bit errors.

Steps.

→ 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

DATE

Ex: 2 A 7 bit Hamming Code is received as 1011011. Assume even parity and state whether the received code is correct or wrong, If wrong, locate the bit in error.

⇒ Received H.C :

D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	1	1	0	1	1

1st lets check for P_1: $D_3\ D_5\ D_7$: 1011

It has odd no of 1's. so, there is an error. So we put P_1 as 1

2nd lets check, $P_2\ D_3\ D_6\ D_7$: 1001

It has even no. of 1's: so, there is no error. So we put P_2 as 0

3rd lets check, $P_4\ D_5 D_6\ D_7$: 1101

It has odd no. of 1's, so there is error. So we put P_4 as 1

Error word: E => | P_4 | P_2 | P_1 |

E => | 1 | 0 | 1 |

which is 5 in ~~binary~~, decimal

So, there is error in the 5th bit

And, the corrected code is [change 1 to 0]

1 0 0 1 0 1 1

Note: bit = 1011 ∴ d = 4

No of redundant bit $r = 2^r > d + r + 1$

$\Rightarrow 2^r > 4 + r + 1$

$2^r > 5 + r$

when r = 3, $8 > 8$

Ex: Encode the data 1101 with even parity using Hamming code.

=> The 7 bit hamming code structure is.

D7	D6	D5	P4	D3	P2	P1
1	1	0		1		

First we calculate p1:-

Check 1 bit, skip 1 bit, check 1 bit, skip 1 bit,----

∴ (1, 3, 5, 7, ----)

For p2 : Check 2 bit, skip 2 bit, Check 2 bit, skip 2 bit,---

∴ (2, 3, 6, 7, 10, 11, ----)

For p4: Check 4 bit, skip 4 bits, check 4 bits, skip 4 bits,---

(4, 5, 6, 7, 12, 13, 14, 15, ----)

∴ or

p_1: D_3 D_5 D_7	p_2: D_3 D_6 D_7	P_4: D_5 D_6 D_7
1 0 1	1 1 1	0 1 1
∴ p1 = 0 (even parity)	∴ p_2 = 1	∴ p4 = 0.

Hence, Encoded hamming code structure is.

D7	D6	D5	P4	D3	P2	P1
1	1	0	0	1	1	0

DATE

* 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.

a) 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 portions each user being assigned one portion. Since, each user has a private frequency band, there is no interface between user.

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

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

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 divison multiplexing time

b) Dynamic Channel Allocation:

When nodes are connected & use a common link

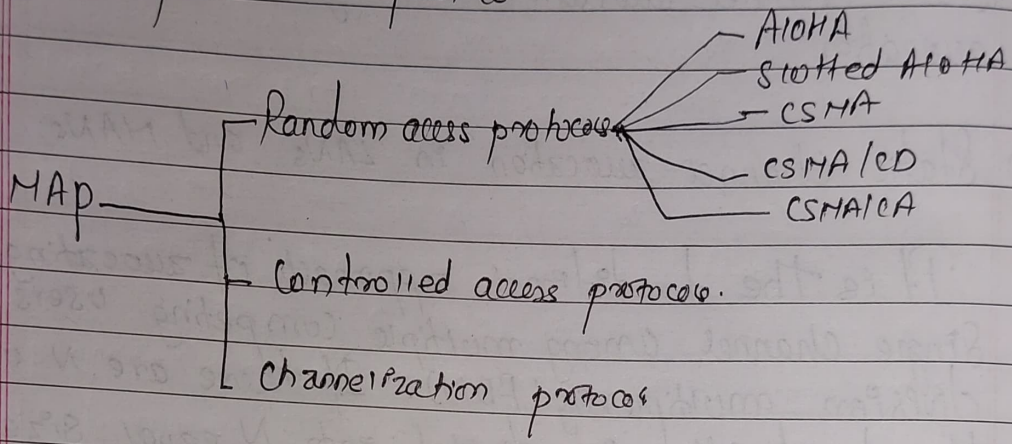
PAGE

classmate

DATE

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 & Channelization protocols.

* Multiple Access protocol.



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: RAP, CAP, CP.

1) Random access protocols.

In this method, no node is superior to another node and none is assigned the control over another. Any node can send data depending upon 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:

DATE

a) ALOHA

- The ALOHA was designed as 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
- It is a multiple access protocol at the data link layer & proposes how multiple terminal access the medium without interference or collision. There are two different versions of ALOHA:

* Pure Aloha.

- The pure ALOHA allows every station to transmit the data whenever they have data to be sent.
- When every station transmits the data without checking whether the channel is free or not, there is always the possibility of collision of data frame
- If the acknowledgement arrived for the received frame, then it is OK or else if the two frames collide, they are damaged.
- The throughput of pure ALOHA is maximized when the frames are of uniform length.

* Slotted Aloha

- This is quite similar to Pure Aloha, differing only in the way transmissions take place.
- Instead of transmitting right at the demand time, the sender waits for some time. The timeline is divided into equal slots & then it is required that the transmission should take place only at slot boundaries.

CLASSMATE

PAGE

DATE

In slotted ALOHA

-> It requires all nodes synchronize their transmissions to start at the beginning of a slot.
-> It makes the nodes to wait till next time slot begins & allow each data frame to be transmitted in the new time slot.
-> It divides the time into equal time slots of length greater than the packet duration.
-> Each time slot corresponds to the length of the frame

If two or more frames collide in a slot, then all the nodes detect the collision event before the slot ends. In this way, the no. of collisions that can possibly take place is reduced by a huge margin. And hence, the performance become much better compared to pure Aloha

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.

There are three modes of CSMA:

o Non-persistent: First the node checks the channel, if the channel is idle then the node or station

DATE

transmits data, otherwise it keeps on waiting and whenever the channel is idle, the stations transmit the data-frame.

- P-Persistent
  The station checks the channel similarly as 1-persistent mode, but the only difference is that when the channel is busy it checks it again after a random amount of time, unlike the 1-persistent where the stations keep on checking continuously.

- 1-persistent
  The station checks the channel & if found idle then it transmits the data frame with the probability of p and if the data is not transmitted. (1-p) then the station waits for a random amount of time & again transmits the data with probability p. & this cycle goes on continuously until the data-frame is successfully sent

C) CSMA 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 delay must be at least two times the maximum propagation delay. If any collision is detected in the CSMA/CD, the station sends a jam/stop signal to the shared channel to terminate data transmission.

DATE

d) CSMA with Collision Avoidance. (CSMA/CA)

It is a protocol that works with a medium access control layer. It was invented for wireless networks. The process of detection of collisions 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 then it means a collision has occured. 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:

- Interface 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 called interframe space or IFS. After this time it again checks medium for being idle.

- Contention window → It is the amount of time divided into slots. If the sender is ready to send data, it choses a random number of slots as wait time which doubles every time medium not found idle.

- Acknowledgement → The sender retransmits the data if acknowledgement is not received before time-out.

DATE

Ethernet Standards

In 1985, the Computer Society of the IEEE started a project, project called 802, to set standards to enable intercommunication along/among equipment from a variety of manufacturers. Project 802 is a way of specifying functions of the physical layer and the data link layer of major LAN protocols

Generally used IEEE 802 specifications are:

	IEEE 802.3	IEEE 802.4	IEE 802.5
i)	The IEEE 802.3 Standard determines the CSMA/CD access Control protocol.	i) It describes a token bus LAN Standards.	i) It describes token ring standards.
ii)	Topology used is Bus topology.	ii) Topology used is Bus topology.	ii) Topology used 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 byte	iv) Size of data field is 0 to 8182 bytes	iv) No limit in size of data field.
v)	Maximum frame required is 64 bytes	v) It can handle short minimum frames.	v) Supports both short and large frames
vi)	Modems not required	vi) Required	vi) Required
vii)	Protocol is very simple.	vii) Extremely complex	vii) Moderately complex

PAGE

DATE

Wireless LAN: Spread spectrum, Bluetooth, Wi-Fi

Spread Spectrum

- In Spread spectrum, signals are combined from different sources to fit into a larger bandwidth.
- It is an increasingly important form of encoding for wireless communications. It can be used to transmit either analog or digital data, using an analog signal. The basic idea is to modulate a signal so as to increase significantly the bandwidth of signal to be transmitted.
- It was initially developed for military & intelligence requirements. The use of spread spectrum makes jamming & interception more difficult & provides improved reception.
- ~~Cross~~ Advantages
- Cross-talk elimination, better output with data integrity, Better security, reduction in noise, not easy to demodulate/modulate(decode), difficult to jam the signals.

Bluetooth

- Bluetooth is a wireless technology for exchanging data over short distances (using short wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building PAN.

DATE

- It can connect several devices, overcoming 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 20,000 member companies in the areas of telecommunications, computing, networking & consumer electronics.

WI-FI

- Wireless Fidility (Wi-Fi) is a family of wireless network protocols, based on IEEE 802.11 family of standards, which are commonly used for local area networking of devices & 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.
- It is one of the fastest growing technology these days.

DATE

Overview of Virtual circuit switching, Frame Relay & ATM.

o Virtual circuit switching.

-> It is a packet switching methodology whereby a path is established between the source and the final destination through which all the packets will be routed during a call.

-> The path is called virtual circuit because, to the user, the connection appears to be a dedicated physical circuit. However, other communications may also be sharing the parts of the same path.

-> Before the data transfer begins, the source and the 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.

o Frame Relay.

-> Frame Relay is also a packet switching methodology that uses virtual circuits.

-> These virtual circuits can be used/setup for each session and set up permanently.

-> Frame relay is designed for fiber optic cables with a very low bit error rate.

DATE

- It has no error recovery and no flow control.
- Whenever a Frame relay switch detects an error in a packet, it just discard the data.
- This results in network with low processing overhead and high transmission rates.
- Frame relay is extensively used today in large corporations to interconnect the LANs between buildings.
- It was developed for taking the advantage of the high data rates & low error rate in the modern communication system. It operates at a high speed (1.54 Mbps to 44.38 Mbps) and allows the bursty data.

Asynchronous Transfer Mode (ATM)

- ATM, also known as cell relay, is a streamlined packet transfer interface which takes advantage of the reliability and fidelity of modern digital facilities to provide faster packet switching than X.2.
- Like packet switching and frame relay, ATM involves the transfer of data in discrete chunks, & allows multiple logical connections to be multiplexed over a single physical interface.
- In the case of ATM, the information flow on each logical connection is organized into fixed-size packets, called cells.
- It is a streamlined protocol with minimal error & flow control capabilities.
- This reduces the overhead of processing ATM cells and reduces the number of overhead bits required with each cell, thus enabling ATM to operate at high data rates.

DATE

DLL protocol: HDLC, PPP.

HDLC.

-> HDLC stands for high-level data link control.
-> It is a bit oriented protocol that is implemented by point-to-point configuration and also multipoint configurations.
-> Dynamic addressing is not offered by HDLC and it is not compatible with non-cisco devices.
-> HDLC is used in synchronous media. It does not provide link authentication & 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) is a communication protocol of the data link layer that is used to transmit multiprotocal data between two directly connected (point-to-point) computer.
-> It is a byte-oriented protocol that is widely used in broadband communications having heavy loads and high speeds.
-> Since it is data link layer protocol, data is transmitted in frame.

PAGE

DATE

Services provided by PPP

- Defining the frame format of data to be transmitted
- Defining the procedure for establishing link between two points & exchange of data
- Stating authentication rules of the communicating devices.
- Stating the method of encapsulation of network layer data in the frame.

Questions asked from this chapter

DATE

Q. What is flow control? Explain stop-and-wait ARQ with suitable example. How is it different from Go-Back-N-ARQ? (2078 - 10 marks) (2076 - 10 marks)

Q. What is CSMA/CD? Why there is no need of CSMA/CD on a full-duplex ethernet LAN? (2078 - 5 marks)

Q. Short Notes :- ALOHA (2078 - 2.5 marks)

Q. Why do we need wireless LAN? Explain the architecture of IEEE 802.11 in detail. (2076 - 5 marks)

Q. Short notes: Hamming distance (2076 - 2.5 marks)

Q. Differentiate between ATM and frame relay (2074 & (2070 - 6 marks) marks)

Q Explain how slotted ALOHA improves the performance of the system over pure ALOHA? (2070 - 6 marks)

Q. Explain ppp with example. (2073 - 6 marks, 2068 - 6 marks)

Q What is random access protocol? Discuss ALOHA in detail. (2076 - 6 marks)