Total No. of Pages 01 Roll No. .....

SIXTH SEMESTER B.Tech. (CO)

MID SEMESTER EXAMINATION MARCH-2020

CO-306 COMPUTER NETWORKS

Time: 1:30 Hours Max. Marks: 30

Note: Answer ALL FIVE questions. All questions carry equal marks.
Assume suitable missing data, if any.

Date	Grade/ Marks	Signature

Total No. of Pages:1 —119— Roll No.....

SIXTH SEMESTER B. Tech.(CO)

MID SEMESTER EXAMINATION MAR-2019

CO-306 COMPUTER NETWORKS

Time: 1:30 Hours Max. Marks: 30

Note: All questions are compulsory. Assume suitable missing data, if any.
All questions carry equal marks.

Total no. of Pages: 01 Roll no.....

B.Tech.(CO) Sixth Semester

Mid-Term Examination Mar-2023

CO306 Computer Networks

Time: 01:30 Hours Max. Marks: 30

Note: Answer all Questions.
Assume suitable missing data, if any.

Total No. of Pages: 2 Roll No. .....

SIXTH SEMESTER B.TECH (COE)

MID SEMESTER EXAMINATION (MARCH 2018)

CO-306 COMPUTER NETWORKS

Time:1.5 hours Max. Marks: 30

Note:Attempt all questions.
Assume suitable missing data, if any.

Total no. of Pages: 2 Roll no.....

B.Tech. _____ SEMESTER

END TERM EXAMINATION May-2023

COURSE CODE (CO306) COURSE TITLE COMPUTER NETWORKS

Time: 03:00 Hours Max. Marks: 40

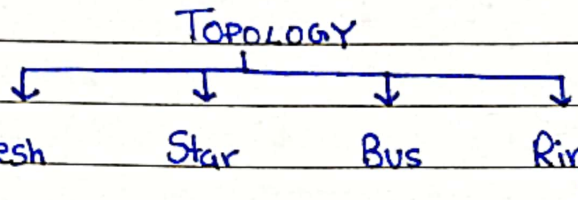
Note : Attempt any five questions
All questions carry equal marks.
Assume suitable missing data, if any.

UNIT-1 : INTRODUCTION CONCEPTS

Page No. | Date

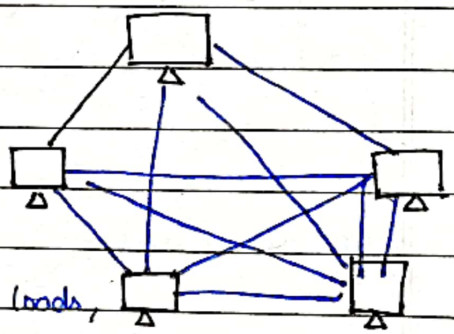
B) Explain the Bus, Star, Ring, Hybrid and Tree network topologies giving their advantages and disadvantages. 2019S

(b) Categorize three basic topologies and give an advantage and disadvantage of each type. 2019M



MESH TOPOLOGY

In mesh topology, every device has a dedicated point to point link to every other device



cables = $^nC_2$

ports = n (n-1)

Advantages:

→ Dedicated links ensure individual data loads, eleminating traffic problems.

→ Robustness: System remains functional even if a link is usable

→ Enhance privacy and security due to dedicated links

→ Easy fault identification and isolation through point-to-point links.

Disadvantages:

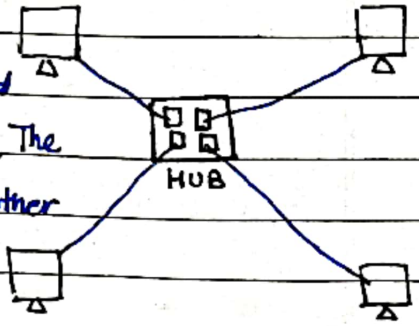
→ Increased installation complexities due to the need for every device to connect to every other.

→ Increased amount of cabling and potentially exceeding available space.

→ High cost associated with the h/w reqd. for connecting each link.

STAR TOPOLOGY

In star topology, each device has a dedicated p-t-p link only to a central controller (hub). The devices are not connected directly to each other



Page No.
Date

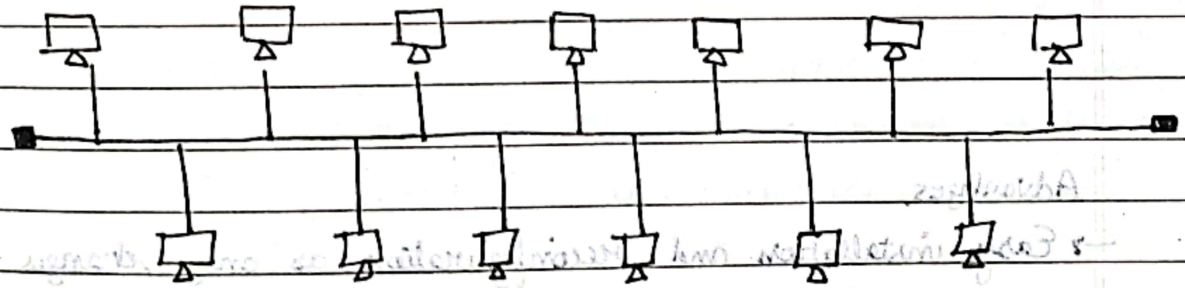
cables = n
ports = n

Advantages:
→ Cost effective compared to mesh topology.
→ Simple installation as each device needs one link and I/O ports.
→ Robust as there is no one point failure.
→ The hub enables monitoring and bypassing defective links.

Disadvantages:
→ If the hub fails, the entire system is affected.
→ Cable dependency.

BUS TOPOLOGY

Bus topology, is a multipoint topology where one long cable acts as a backbone to link all devices in network.



cables = n+1
ports = n

Advantages:
→ Easy installation of nodes connected to nodes by droplines.
→ Reduced Cabling compared to mesh and star.
→ Elemination of redndant cabling.

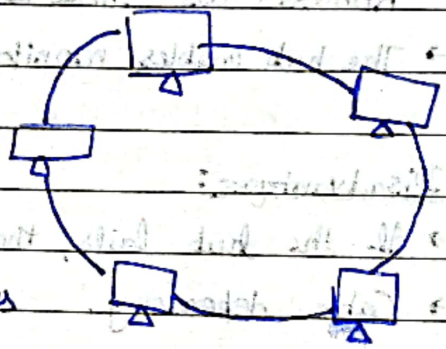
Page No.
Date

Disadvantages

→ adding new devices is challenging → limited scalability
→ Fault in the bus cable halts all transmission → degradation.
→ Degradation in quality due to signal reflection at taps.

RING TOPOLOGY

In a ring topology, each device has a dedicated point to point connection with only two devices on either side of it. A signal is passed along the ring in one dirⁿ from device to device, until it reaches destination.



cables = n
ports = 2×n

Advantages

→ Easy installation and reconfiguration as only changes to two connection for addition / removal of devices are required.
→ Simplified fault isolation through circulating signals to issue alarms if no signal is received.
→ Constraints on max. length allow to manage media and traffic

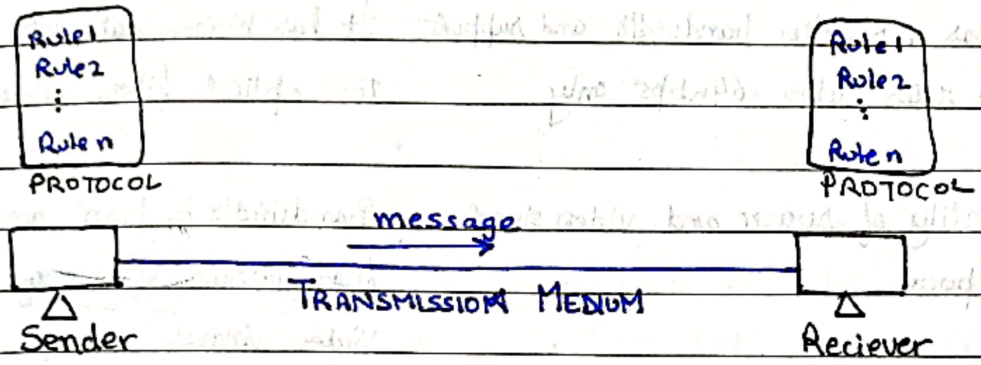
Disadvantages

→ Break in ring can disable entire network in simple unidir ring.
→ Vulnerability ~~in ring~~ due to d/o disruption
→ not pvt.

Page No.
Date

1[a] Explain the five components of a data communication system. 2020M

Data communication is the process of transferring data electronically from one plate to other



The components are:-

1.) Message: It is the data or information to be communicated. It may consist of text, number, picture, sound, video etc.

2.) Sender: It is the device that sends the message. It is also called source or transmitter which can be a computer, fax machine or mobile phone etc.

3.) Reciever: It is the device that recieves the message. It is called sink which must be capable to accept the message. It can be a computer, printer, fax machine, mobile phone etc..

(communication media)

4.) Transmission Medium: It is the path through which messages are transferred from one place to another. It is also called communication channel. It is a physical cable or a wireless medium.

(PROTOCOL)

5.) Encoder and Decoder: Encoder is a device that converts digital signals in a form that can pass through a transmission medium. Decoder converts the encoded signal into digital form. using protocol which is a set of rules

c) Differentiate Narrow band and broad band ISDN. 2023M [3] [CO1]

	NARROW BAND ISDN	BROAD BAND ISDN
→	It has a smaller bandwidth and support data rates upto 64kbps only	It has higher data rates upto 1Gbps due to optical fibre cable use
→	Quality of service and video signals is poor	Bandwidth is high and can allow transmission of very high quality video images through it.
→	N-ISDN is divided into two 2B + 1D	B-ISDN is divided into several B channels (30 or 23) along a D channel.
Application:	Small businesses for voice calls, basic internet, faxing etc.	Large Businesses and institutions requiring high speeds for video conferencing, multimedia sharing, internet access with higher bandwidth needs.

Q.5 [a] How do guided media differ from unguided media? Explain with suitable examples. 2019S

Q.5 [a] How do guided media differ from unguided media? Explain with suitable examples. 2019S

[a] How do guided media differ from unguided media? Explain with suitable examples. 2018S

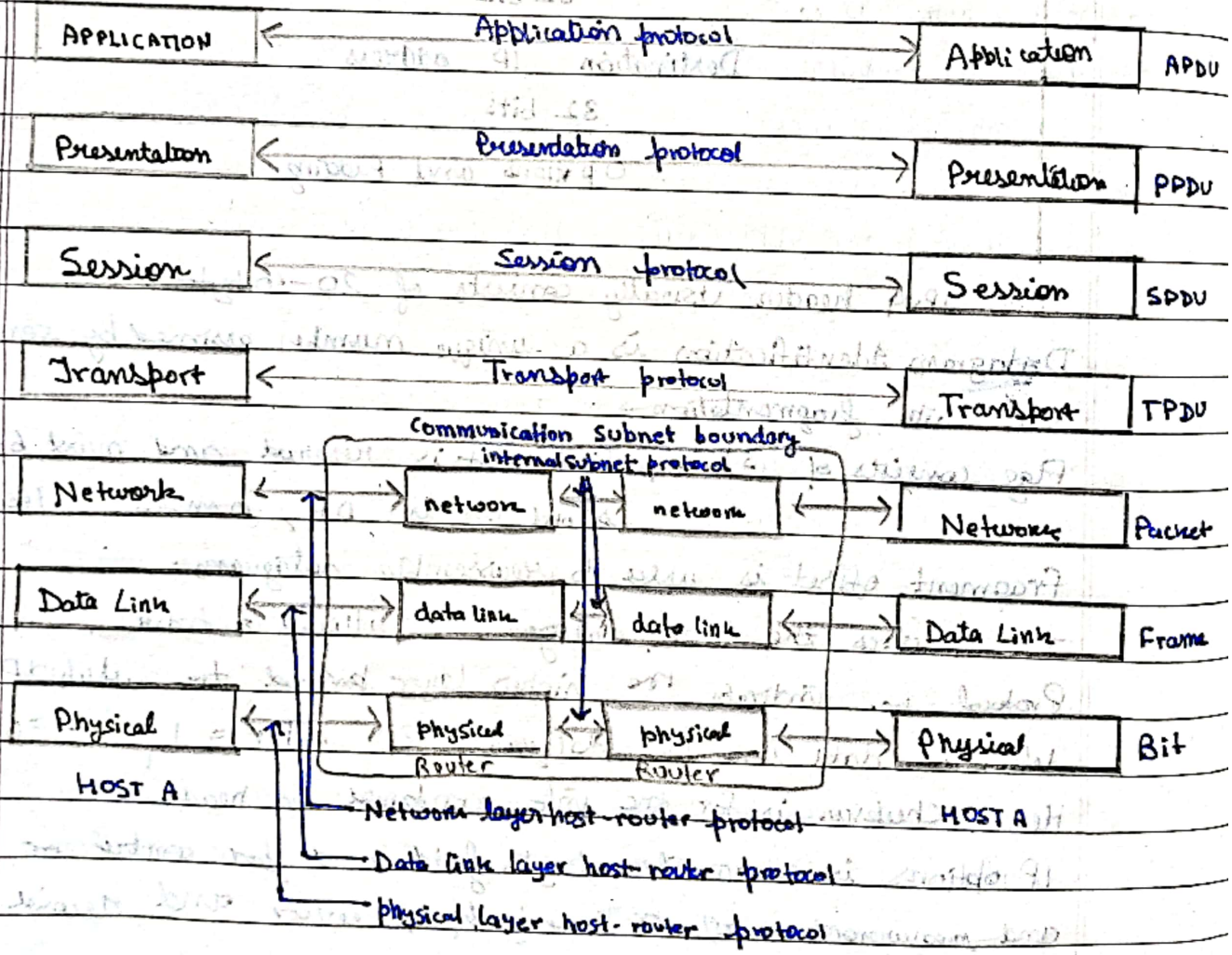
	GUIDED MEDIA	UNGUIDED MEDIA
	Wired communication occurs through bounded transmission media.	Wireless communication occurs through unbounded transmission media.
	Signal propagates through wires.	Signal propagates through air
	Its used for point to point commⁿ.	It is suited for radio broadcast in all dirⁿ.
	Signals are in form of voltage, current, photons	Signals are in form of Electromagnetic waves.
	cost effective	expensive
Eg)	Twisted Pair Wires, Coaxial Cables, Optical fibre cable	Microwave, Radio links / IR light

Page No.
Date

Q.1
[a] What is OSI reference model? Explain responsibilities of various layers of OSI model. And also Compare and contrast OSI model with TCP/IP model. 2019S

Q.1
[a] What is OSI reference model? Explain responsibilities of various layers of OSI model. And also Compare and contrast OSI model with TCP/IP model. 2018S

The OSI (Open Systems Interconnection) Reference Model, developed by ISO, is a conceptual framework with seven layers, each serving a distinct communication function. It aims for international standardization, providing a structured approach for network protocol and design



The responsibilities of various layers of OSI reference model are:

Q.1
A) What are the various layers of OSI model? Compare and contrast OSI model with TCP/IP model 2019S

1. a. Explain OSI layers in Computer Networking? 2018S

1. Physical layer :
- Transmit raw bits over a communication channel.
- Addres electrical signals, timing and physical transmission medium.

2. Data link layer :
- Transform raw transmission into a reliable line.
- Break data into frames for transmission.
- Control access to shared channels in broadcast networks.
- Manage error and flow control

3. Network layer :
- Control subnet operation.
- Determine routing paths from source to destination.
- Handle congestion and ensure quality of service.
- Overcome problems when packets travel across different networks.

4. Transport layer :
- Accept and split data into smaller units.
- Ensure correct delivery of data at the destination.
- Provide end-to-end communication and isolation from h/w changes.
- Determine type of service (point-to-point, order of delivery) etc.

5. Session layer :
- Establish sessions between users on different machines.
- Manage Dialogue control, token management and synchronization.

6. Presentation layer :
- Manage syntax and semantics of transmitted info.
- Define abstract data structures and standard encodings for communication

7. Application layer :
- Host various application protocols (HTTP, FTP, SMTP etc)
- Facilitate common user needs - such as web browsing and communication -

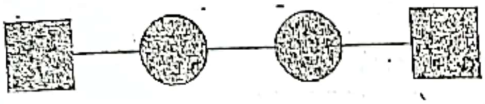
Page No.
Date

Q1 a) Differentiate OSI reference model with the TCP/IP reference model.
2023M .[4] [CO1]

	OSI Model	TCP/IP Model
1.)	OSI stands for open system interconnection.	TCP/IP implies Transmission Control Protocol / Internet Protocol.
2.)	It was developed by ISO in 1984	It was developed by ARPANET in 1982
3.)	It consists of 7 layer : starting from bottom Physical, data-link, network, transport, session, presentation and application.	It consists of 4 layers from bottom: Network interface, internet, transport and application layer.
4.)	The OSI model follows a vertical approach	The TCP/IP model follows a horizontal approach.
5.)	In the OSI model, the transport layer provides a guarantee for delivery of the packets.	In TCP/IP model, it doesn't provide such guarantee, but still we can say its a reliable model.
6.)	here, physical and data-link layers are separate layers	here, physical and data link layers are merged as a single network layer.
7.)	here, the session and presentation layers are separated such as both are different.	here, both these layers are included in the application layer.

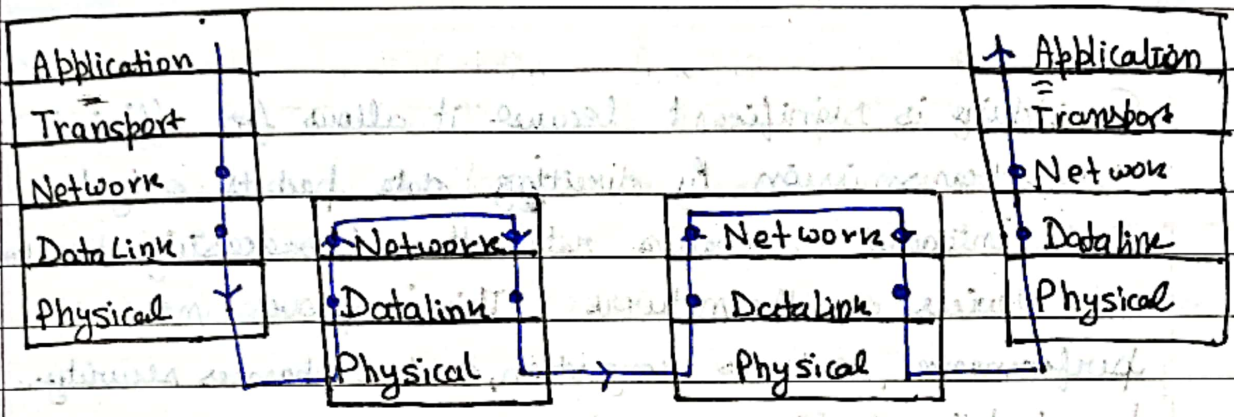
diagram

1. Explain OSI layers and with the help of diagram show the interaction among different layers of OSI. 2018 M
Assume that source S and destination D are connected through two intermediate routers labeled R. Determine how many times each packet has to visit the network layer and the data link layer during a transmission from S to D. 7 marks



GATE 2013

Page No. | Date



Clearly the packet visits :

i.) Data link Layer – 1(S) + 2(R) + 2(R) + 1(D) = 6 times

ii.) Network layer - 1(S) + 1(R) + 1(R) + 1(D) = 4 times.

[b] What are the responsibilities of Presentation layer and Session layer of OSI model? 2020M

PRESENTATION LAYER

→ It translates data b/w the formats the network requires and the format the computer expects (Eg ASCII or EBCDIC)

→ It does the protocol conversion.

→ For security, it carries out encryption at transmitter and decryption at receiver.

→ It carries out data compression to reduce the bandwidth of the data to be transmitted.

SESSION LAYER

→ It allows two systems to start a dialogue with each other. The communication initiated b/w two processes can be either in half / full duplex.

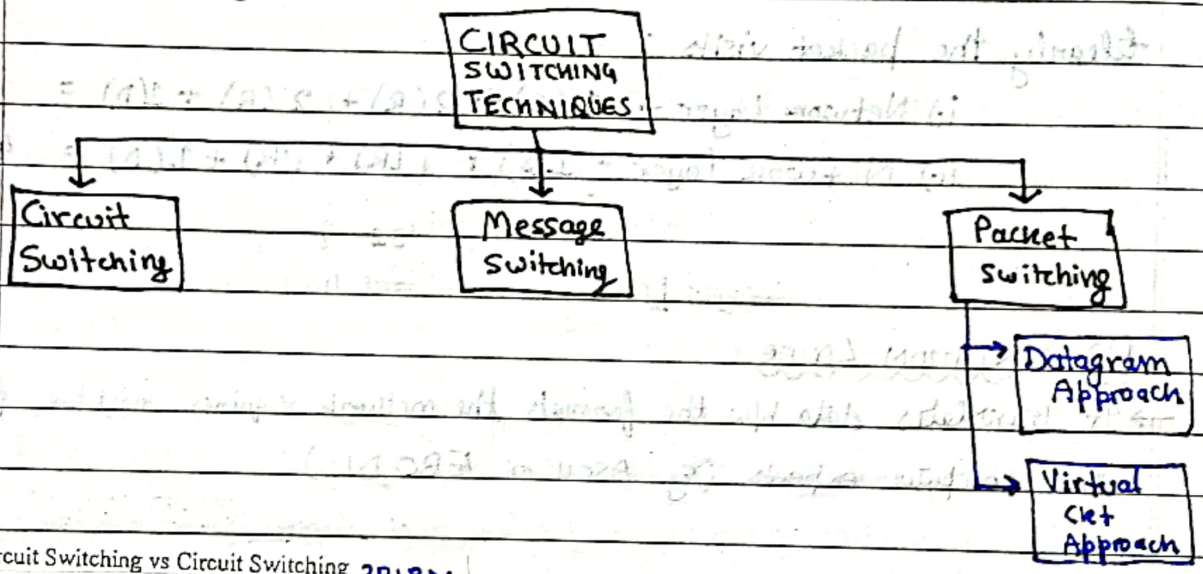
→ It allows addition of check points (i.e. synchronization points) into a stream of data. Incase of crash, retransmission can start from checkpoint instead of start.

Page No.
Date

b) Explain the significance of Switching? What are different switching techniques used in computer networks? Discuss. 2023M [3] [CO1]

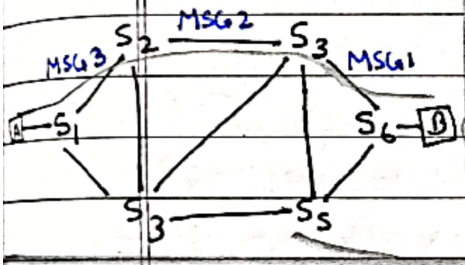
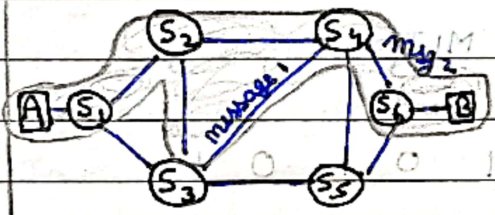
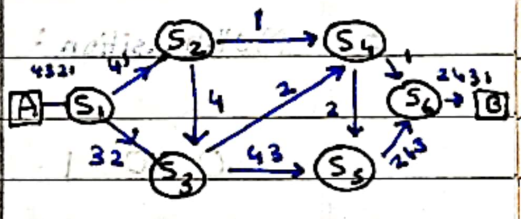
b. What is the difference between circuit switching and packet switching? What is Virtual Circuit Network? 2018S (10 marks)

Switching is significant because it allows for efficient data transmission by directing data packets only to their intended destination rather than broadcasting them to all devices on the network. This improves network performance, reduces congestion, and enhances security by isolating traffic.



b. Virtual Circuit Switching vs Circuit Switching 2018M

CIRCUIT SWITCHING	MESSAGE SWITCHING	PACKET SWITCHING
There is physical connection b/w transmitter and receiver.	No physical path is set b/w transmitter and reciever in advance	No path physically is established b/w transmitter and receiver.
All the packets uses same path	Packets are stored and forward.	Packets travel independently.
Need an end to end path before data transmission.	No need of end to end path before data transmission	
There is one big entire data stream called a message.	There is one big entire data stream called message.	The big message is divided into a smaller number of packets.

Message arrives in sequence.	Message arrives in sequence	Packets do not arrive in sequence at the destination.
Low transmission Capacity	Max transmission capacity	Max Transmission Cap.
Waste of bandwidth is possible	No wastage of Bandwidth	No waste of bandwidth.
Not suitable for handling interactive traffic	Suitable for handling interactive traffic	Suitable for handling interactive traffic.
		

Write short notes: -
[a] Virtual circuit switching 2020M

VIRTUAL CIRCUIT NETWORK

It is a category of packet switching network where a virtual path is established between the source and destination systems for communications. It is not really a dedicated physical path but a logical circuit allocated from a managed pool of ckt resources as per traffic requirements.

Its phases are :

→ Set-Up Phase

→ Data Transfer

→ Tear Down Phase

UNIT-2 : DATA LINK LAYER

Page No. | Date

c) What is the significance of data link layer? Explain the design issues of data link layer. 2023M [3] [CO2]

DLL is the second layer of OSI model of CN. It is responsible for node to node delivery of data between a network segment. Its significance is made clear by its functionalities :

1. FRAMING: divides stream of bits into managable units called frames.
2. PHYSICAL ADDRESSING: Adds header to frame to define physical address of sender/receiver.
3. FLOW CONTROL: mechanism to avoid a fast transmitter from overrunning a slow receiver by buffering extra bits.
4. ERROR CONTROL: Achieved by adding a trailer at the end of frame. It uses a mechanism to avoid duplication of frames.
5. ACCESS CONTROL : It determines which of the devices has control over the link at any given time, when two or more devices are connected to the same link.

DESIGN ISSUES

1.) Services provided to n/w layer :
   a.) Unacknowledged and connectionless services : Sender sent frame W/O Ack or conn
   b.) Acknowledged and connectionless services : frame Ack but no logical connection.
   c.) Acknowledged and connection oriented services : Logical connection established before data transfer, frames numbered for reliability.

2.) Frame Synchronization : Ensuring standard of each frame for proper recognition by devices

3.) FLOW CONTROL : Regulating data flow to prevent overwhelming the recievers.

4.) Error Control : Detecting and correcting transmission error to prevent frame duplication

(B) What are the different types of error detection methods? Write the steps to compute the Checksum in CRC code. if the frame is 11010101 and generator is x4 + x+1 what would be the transmitted frame? 2018S

Page No.
Date

Q.2
[a] What are the different types of error detection methods? Write the steps to compute the Checksum in CRC code. If the frame is 110101011 and generator is x4 + x+1 what would be the transmitted frame? 2018S

Some types of error detection methods are

1. Vertical Redundancy Check (VRC) } Parity
2. Longitudinal Redundancy Check (LRC) }
3. CheckSum
4. Cyclic Redundancy Check (CRC)

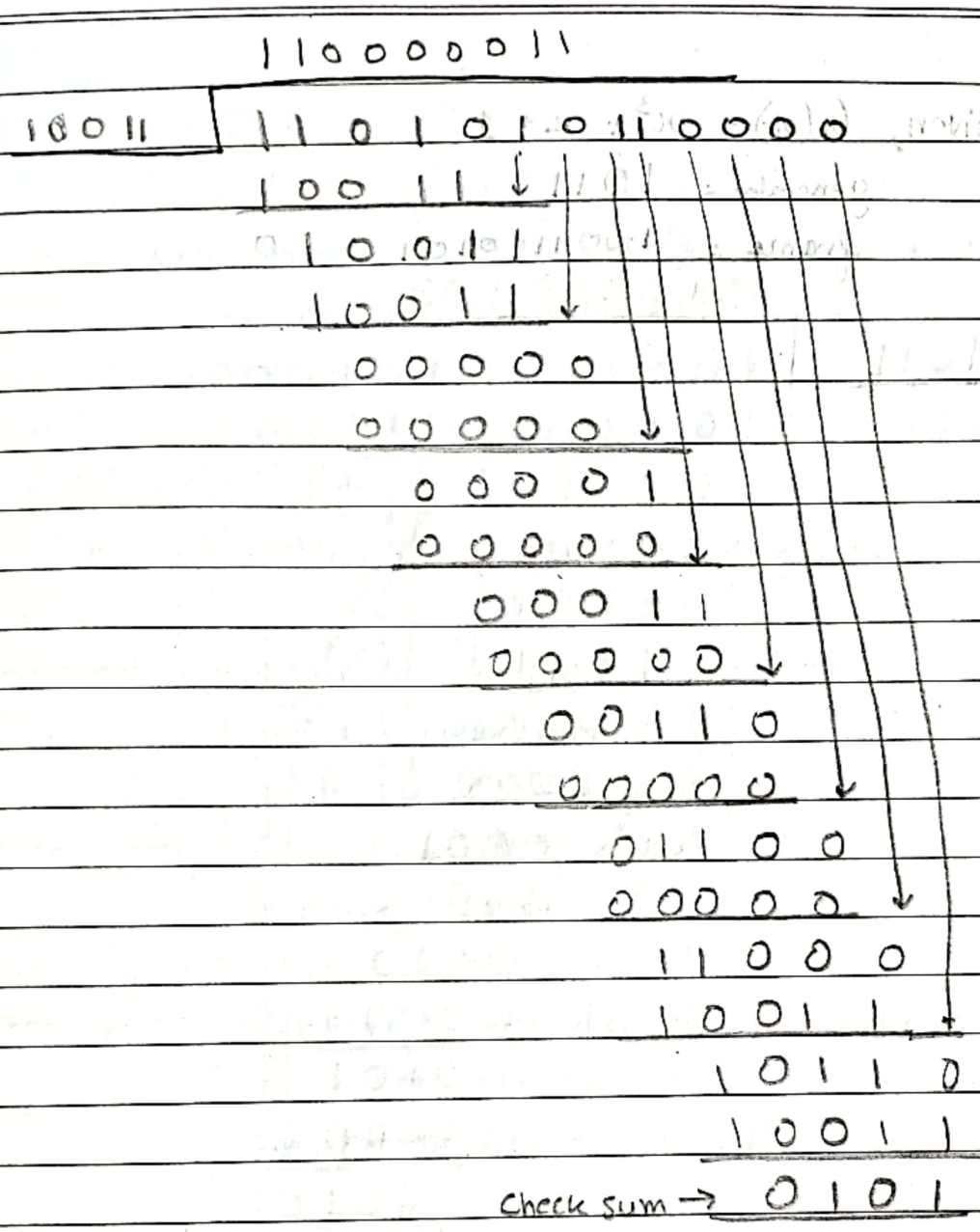
Steps to compute checksum in CRC code.
Let $G(x)$ be the generator polynomial
$M(x)$ be the polynomial corresponding to frame bits.

1. Let r be the degree of $G(x)$. Append r zero bits to the low-order end of the frame so it now contains $m+r$ bits and corresponds to polynomial $x^r M(x)$.

2. Divide the bit string corresponding to $G(x)$ into bit string corresponding to $x^r M(x)$, using modulo 2 division.

3. Subtract the remainder ($< r$ bits) from the bit string corresponding to $x^r M(x)$ using modulo-2 subtraction. The resultant is the checksummed frame to be transmitted, call it $T(x)$.

Given,
$G(x) = x^4 + x + 1$
$\therefore$ Generator = 10011
Frame = 11010 1011



∴ Transmitted frame = 1 1 0 1 0 1 0 1 1 0 1 0 1

2[a] Define CRC. A bit stream 1001110101 is transmitted using the standard CRC method described in the text. The generator polynomial is $x^3 + x + 1$. Show the actual bit string transmitted. Suppose the fourth bit from the left is inverted during transmission. Show that this error is detected at the receiver's end. 20 2M

CRC (Cyclic Redundancy Check) is an error-detection method in digital communication. It involves creating a checksum based on data content, which is then compared at the receiving end. A match indicates error-free transmission, while a mismatch signals potential errors, prompting corrective actions.

Given, $G(x) = x^3 + x + 1$

generator = 1011

frame = 1001110101

Sender Side

```
                1010000100
        ---------------------
1011  | 1001110101000
        1011
        ----
         0101
         0000
         ----
          1011
          1011
          ----
             0000
             0000
             ----
                0010
                0000
                ----
                  1010
                  1011
                  ----
                    0010
                    0000
                    ----
                     0100
                     0000
                     ----
                      100
```

∴ transmitted bit string : 1001110101100

Corrupt bit : 1000110101100

Page No. | Date

Reciever side

```
             1
1011 ) 1000110101100
       1011
       0111
       0000
        1111
        1011
         1000
         1011
          0111
          0000
           1110
           1011
            1011
            1011
             0001
             0000
              0010
              0000
               0100
               0000
                100 ≠ 000
```

Thus error is detected

P.T.O.

Q.4(a) A bit stream 10011101 is transmitted using the standard CRC method. The generator polynomial is $x^3 + 1$. Show the actual bit string transmitted. Suppose the third bit from the left is inverted during transmission. 2019M

Generator : 1001

Frame : 10011101

Sender side

```
1001 | 10011101000
       1001
       ----
        0001
        0000
        ----
         0011
         0000
         ----
          0110
          0000
          ----
           1101
           1001
           ----
            1000
            1001
            ----
             0010
             0000
             ----
              0100
              0000
              ----
               100
```

transmitted frame = 10011101100

Reciever side with error

```
1001 | 10011110100
       1001
       ----
        0111
        0000
        ----
         1111
         1001
         ----
          1100
          1001
          ----
           1011
           1001
           ----
            0101
            0000
            ----
             1010
             1001
             ----
              0110
              0000
              ----
               110
               000
               ---
                110
```

Hence error detected.

Page No.
Date

Q1. a) Suppose a data link layer uses CRC (Cyclic Redundancy Check) to detect errors in transmitted data. If the data word is 101001 and the generator polynomial is x^3 + x + 1, what is the remainder obtained after performing CRC and Code word received at the receiver side? [3] [CO2]

dataword : 101001

generator : 1011

```
1011 | 1010001000
       1011
       ----
        0010
        0000
        ----
         0101
         0000
         ----
          1010
          1011
          ----
           0010
           0000
           ----
            0100
            0000
            ----
             100
```

Remainder = 100

Code word = 101001100

Q.6.

[a] Describe the following: 2018

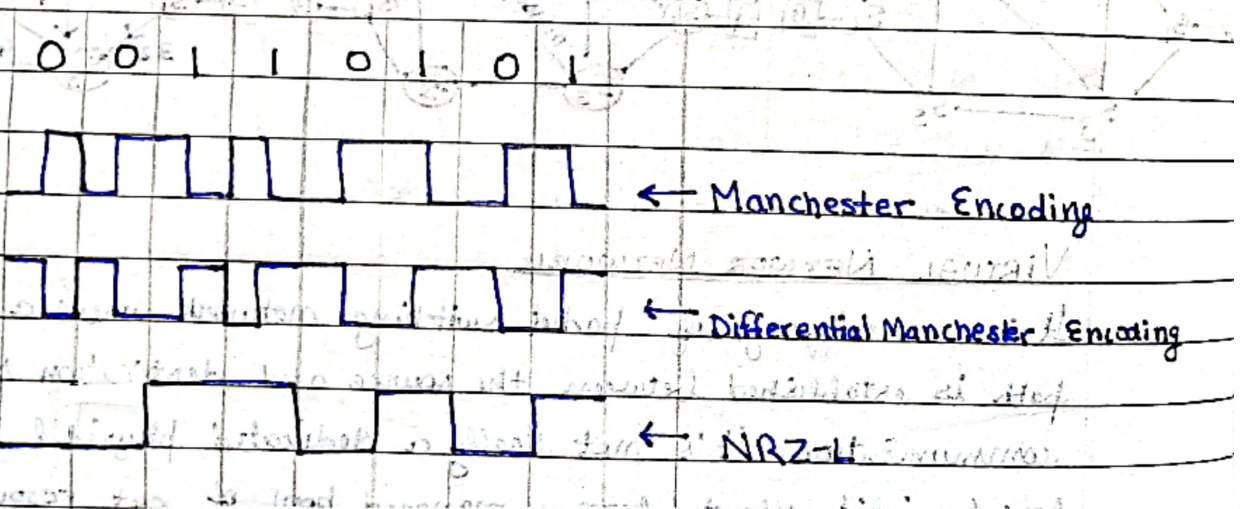
(i) Hamming Codes

Page No.
Date

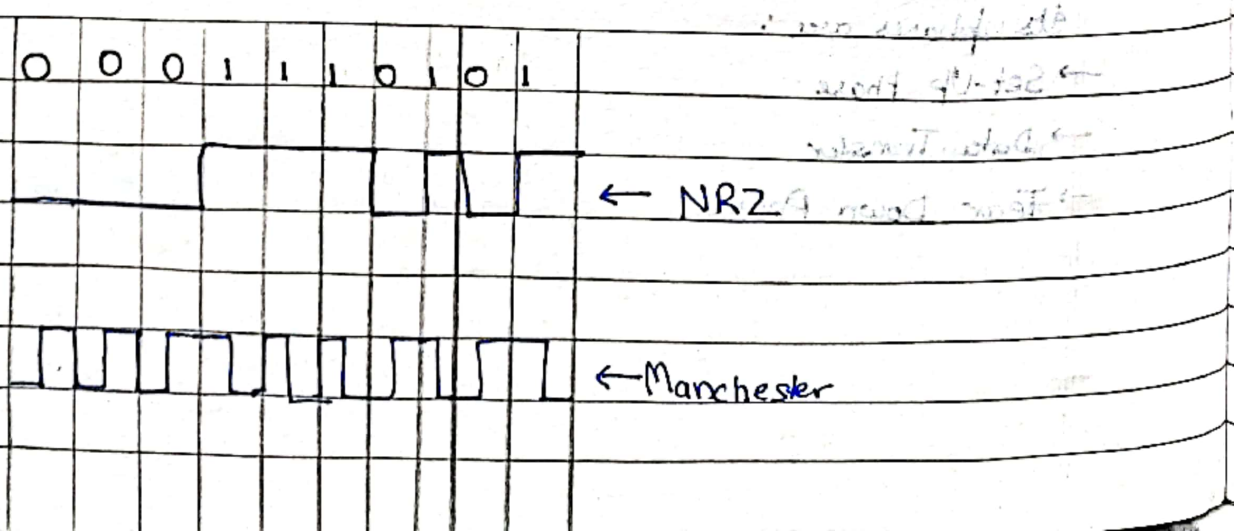
[b] What are different data encoding techniques? Explain and Encode data stream 00110101 by using Manchester, Differential Manchester and NRZ-L encoding methods. 2019S

Different data encoding techniques are:

1. Unipolar : Non-Return-to-Zero (NRZ)
2. Polar: NRZ-L, NRZ-I, NRZ-J.
   Biphase : Manchester, Differential Manchester
3. Bipolar : AMI, pseudoternary
4. Multilever : 2B/1Q, 8B/6T, 4D-PAM5
5. Multitransition : MLT-3



4[a] Draw the following encoding scheme for the bit stream: 0001110101
I. NRZ II. Manchester coding 2020M



Page No.
Date

(b) Sketch the waveform for the bit steam 10110010 in differential Manchester encoding scheme. 2019M

1 0 1 1 0 0 1 0

← Differential Manchester Encoding.

(ii) Burst of error

A burst error refers to a cluster of errors that occur closely together in signal.
So, two or more bits in the data have changed from (1 to 0) or (0 to 1).

Length of Burst Error (8 bits).

Sent: 0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 1

Recive: 0 1 0 1 1 1 0 1 0 1 1 0 0 0 1 1

Burst errors are common in data transmission and more likely to occur than single-bit-errors.

(iii) Parity check

Parity checking is an error detecting method to ensure integrity of data. It is a simple technique when an extra bit called parity bit is added to each word being transmitted. It can detect single bit errors.

odd parity: if # 1s in code is odd then parity bit is set, otherwise unset
even " : ——— even ——— set ——— unset

1 1 0 0 0 0 1	1
original data	parity bit (odd)

Page No.
Date

Q.1 (a) Write the difference between bit stuffing and character stuffing.
2019M

BIT STUFFING	CHARACTER STUFFING
It is known as bit oriented stuffing.	It is known as byte oriented stuffing.
The flag pattern of '01111110' (8-bit) is mostly used for starting and end of flag. But the data may contain this pattern. So, we stuff an extra 0 in data whenever there is a ZERO followed by 5 consecutive 1s in the data. ∴ Single bit stuffed	Escape Character of 1-byte (ESC) which was the predefined pattern of the bit is stuffed in the data frame when there is the same pattern as in the data. ∴ Single byte stuffed.
When receiver receives, they remove the extra bit for de-stuffing the data.	When receiver receives, they removes ESC for destuffing of the data.
Disadvantage: code sets unpredictable as its dependent on transmitted data	Disadvantage: only applied to 8 bit char and 8-bit char code is not used by all.

Q.2 a) Q1. The following character encoding is used in a data link protocol:
A: 11010101; B: 10101001; FLAG: 01111110; ESC: 10100011
Show the bit sequence transmitted (in binary) for the character frame: A B ESC C ESC FLAG FLAG D F each of the following framing methods are used:
2023M

(i) Flag bytes with byte stuffing.
(ii) Starting and ending flag bytes, with bit stuffing. [4] [CO2]

Date

let C = C
D = D
F = F

i.) The modified character frame is:

FLAG A B ESC ESC C ESC ESC ESC FLAG ESC FLAG D F FLAG

∴ = 01111110 11010101 10101001 10100011 10100011 C 10100011 10100011 10100011 10100011 01111110 10100011 01111110 DF 01111110

ii.) We will stuff content bytes with 0 after 5 consecutive 1s

01111110 11010101 10101001 10100011 D1111101010 01111101010 DF 01111110

Page No.
Date

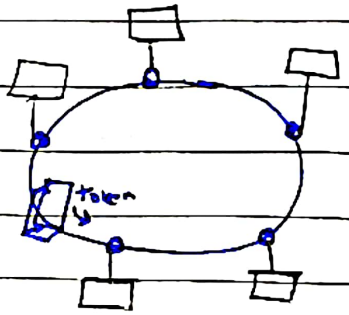
[b] If we want to detect two-bit errors, then what should be the minimum Hamming distance? 2020M

$t = 2$

$\therefore d_{min} = t+1 = 2+1 = 3$

(d) IEEE 802.5 2019M

Token Ring is a LAN protocol where nodes are connected in ring topology.



In this, data is transmitted sequentially from one node to another in a unidirectional manner, i.e. access control method is token passing. Each node must wait for token before transmitting, ensuring orderly data flow and collision avoidance. The node may transmit one or more data frames but before the expiry of token holding time (THT)

→ Data transfer rate is 4 Mbps – 16 Mbps.
→ piggybacking acknowledgement is used.
→ Differential manchester encoding is used

Frame Format.

Data

SD(1)	AC(1)	FC(1)	DA(6)	SA(6)	DATA	CRC(4)	END	FS

Token

SD(1)	AC(1)	ED(1)

Page No.
Date

[b] Explain the IEEE 802 standard. How does Fast Ethernet and Gigabit Ethernet differ from standard Ethernet 2018S

The IEEE 802 is a collection of networking standards and layered architectures that covers the physical and DLL of tech. such as Ethernet and wireless. It is set up in 1980. These specifications apply to LANs & MANs.

These are:

IEEE 802.1	Architecture, Management, Networking	802.9	IDVN
802.2	Logical Link Control (LLC)	802.10	SWG
802.3	CSMA/CD	802.11	WLAN working Group
802.4	Token Bus	802.12	DPWG
802.5	Token Ring	802.13	—
802.6	MANs	802.14	CMWG
802.7	BTAG	802.15	WPAN working group
802.8	FOTAG	802.16	BWA SG.

	STANDARD (10 Base-T) ETHERNET	FAST ETHERNET (100 BASE-T)	GIGABIT ETHERNET (1000 BASE-X)
Year	10 Mbps	100 Mbps	1 Gbps
Types	10 Base-T	100 Base T4, 100 Base TX, 100 Base FX	1000 Base -SX, —LX, —CX, — T
IEEE	802.3	802.3u	802.3z, 802.3ab, 802.3ah
Delay	Most delay	More Delay →	← Less Delay
Coverage	100m	10km	< 70 km
	Cheap	Cost = x	cost = 2x

Page No.
Date

(B) What is Ethernet 802.3 standard? Discuss in detail the frame format and the channel access method used. 2019S

[c] IEEE 802.3 2020M

The IEEE 802.3 standard is a set of constantly evolving set of specifications which form the foundation of wired Ethernet networks.

→ It is constantly evolving offering speeds like 2.94Mbps, 10Mbps, 100Mbps, 1Gbps, 40Gbps, 400Gbps and so on.

→ It uses Bus topology

→ It uses manchester coding and uses coaxial Cable, Twisted Cable and Optical Cable as channel.

FRAME FORMAT

PREAMBLE	SOF	MAC-D	MAC-S	Length	DATA + PAD	CHECKSUM
7B	1B	6B	6B	2B	46B - 1500B	4B

→ Preamble + SOF : It is added by physical layer and sent technically in frame. It is a series of bits as per 1010 1010 ... 101011, last 11 bits → SOF These 7+8 bits are used for clock synchronization.

→ Source/Dest. Address : It is a MAC address of src and destination node. Size of MAC is 6B = 48 bits = 12 digit Hex address.

→ Length : It gives the length of frame.

→ Data + Pad : If the data size is smaller than min size associated with every frame (46B) then padding bits will be added ∴ Min size = 46B | Max size = 1500B.

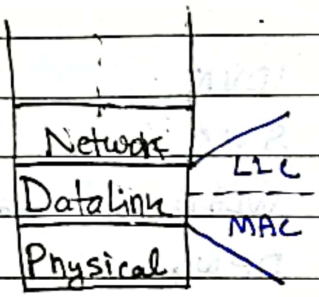
→ CRC : 4Byte CRC is used to detect errors in a given frame.

Media Access control used is CDMA/CD (no acknowledgement), back off method with CSMA/CD for random wait time

Page No.
Date

[b] The data link layer in IEEE standard is divided into sub layers LLC and MAC. Justify statement with example. 2019 S

The data link layer in IEEE standard is divided into two sublayers, LLC (Logical Link Control) and MAC (Media Access Control).



LLC manages communications between devices over a single link of network. It controls data flow among various applications and services, as well as provides acknowledgement and error checking mechanisms.

MAC manages the transmission of data between two devices. It controls the hardware responsible for interaction with the media of the It is also responsible for the physical addressing of frames.

GPT Ex.) Scenario: printing two documents (data packets) on a shared network (printer).

MAC Sublayer: Acts as a queue manager by assigning unique number to each document and ensure only one doc is printed at a time to avoid collisions.

LLC Sublayer: Like a document handler, takes each document and adds information like name (src addrss) and printer's name (dest address) to doc header (frame). It may add error corr codes for reliable printing

Page No.
Date

[b]Explain the dynamic channel allocation model in details. And also explain pure and slotted aloha

2018S

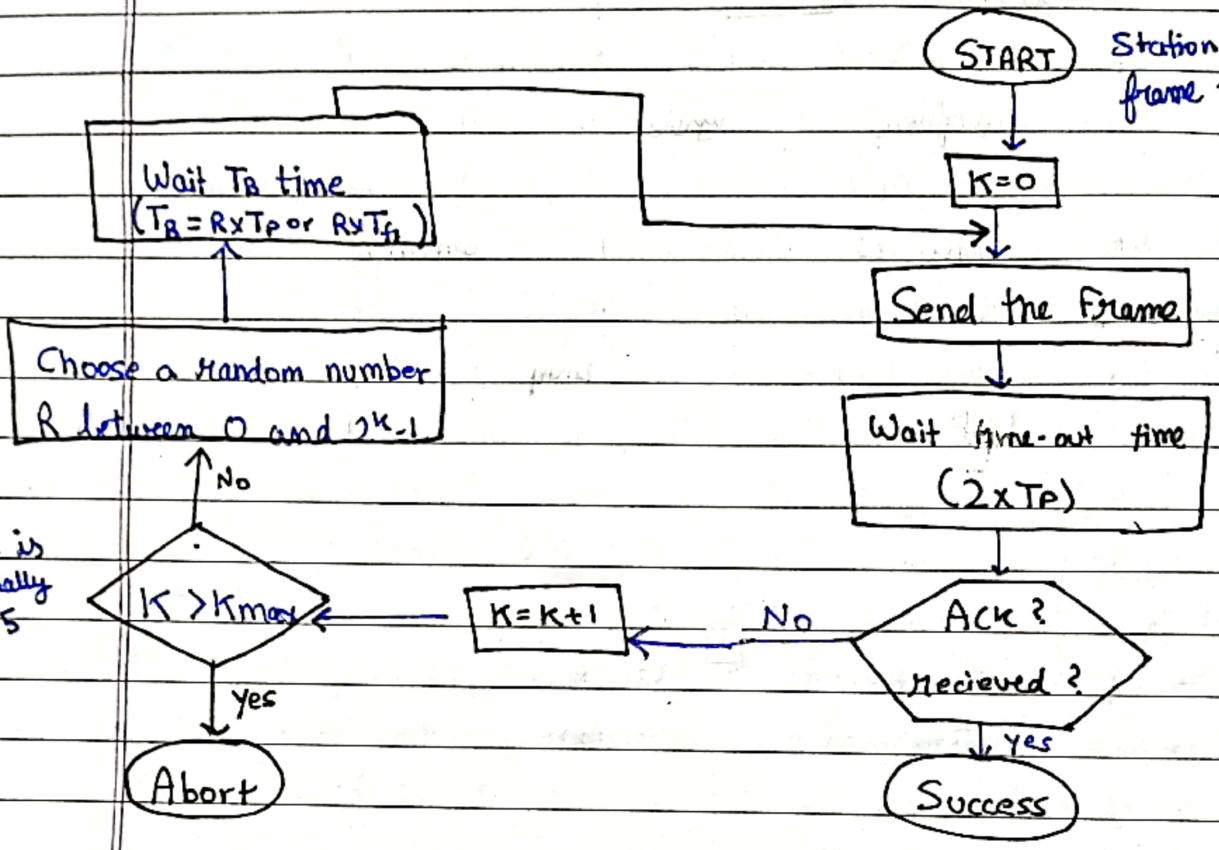
out of syllabus

UNIT 2.1 : Medium Access Control Sublayer

Page No. | Date

Q.3
(A) Explain pure and slotted aloha in detail. 2019

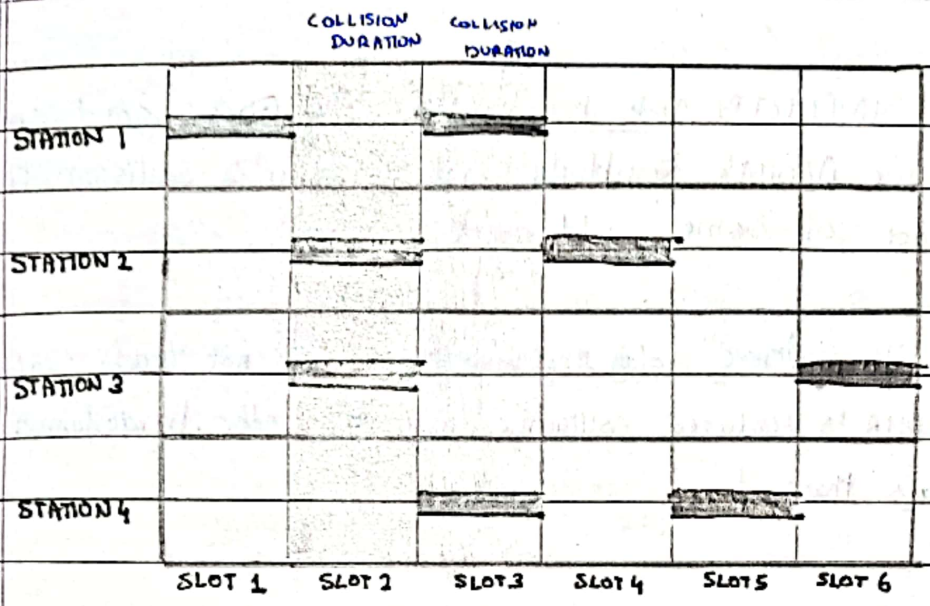
5. Write Short notes on any two: 3.5x 2 = 7 marks
a. Flow diagram of Pure Aloha 2018M



Pure Aloha is a simple random access protocol in data communication. It allows stations to transmit data whenever they have it, without checking for collisions. However collisions are likely, leading to high retransmissions and decreased efficiency. It served as a foundation for more sophisticated protocols like slotted aloha and CSMA

[b] Slotted ALOHA. 2019S

Slotted ALOHA is a random access protocol invented to improve the efficiency of pure ALOHA (pure ALOHA has vulnerable time of 2xTfr as there is no rule that defines when a station can sent).
In slotted ALOHA, we divide the time into slots of Tfr seconds and force the Station only to send at the beginning the time slot. If a station misses this moment, it must wait until the beginning of next time slot. This reduces collisions compared to ALOHA.



Frames in Slotted ALOHA network.

There can still be collisions if multiple nodes transmit in the same slot.

∴ Throughput, $S = G \times e^{-G}$.

Vulnerable time, $T = T_{fr}$

b) List out the situations in which pure ALOHA and slotted ALOHA performs better. Justify your answer. 2023M [3] [CO2]

PURE ALOHA performs better in the case of:

- Light traffic: When few devices are communicating, the chance of collisions is low, and pure ALOHA offers decent efficiency.
- SIMPLE IMPLEMENTATION: Requires minimal synchronization and coordination amongst devices, making it easy to set up and use.
- COST-SENSITIVE APPLICATION: Due to its simple nature, pure ALOHA can be implemented with less complex and h/w making it budget-conscious.

SLOTTED ALOHA performs better in case of:

- Moderate Traffic: The use of time slots reduces collisions as compared to pure upstream ... in scenarios with more active devices

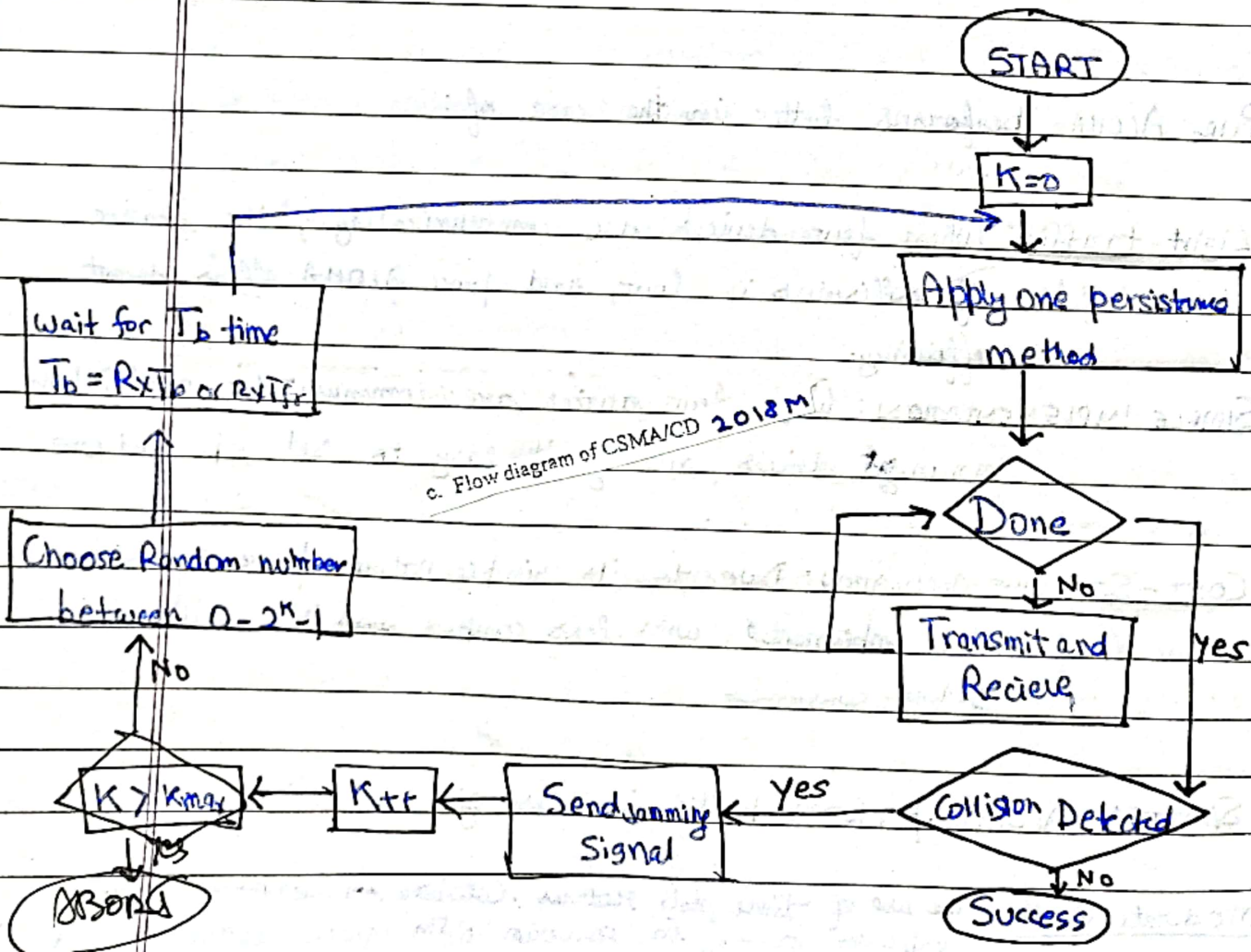
- **BALANCING SIMPLICITY AND PERFORMANCE:** Offers a good compromise between pure ALOHA's simplicity and CSMA's collision avoidance at the cost of some additional complexity.

- **Applications with moderate delay requirements:** While not truely real-time, slotted ALOHA's reduced collisions lead to better predictability and lower delays than pure.

(b) How is CSMA a clear improvement over ALOHA? How is it further improved by implementing CSMA/CD? 2019M

Carrier Sense Multiple Access (CSMA) is an improvement over ALOHA because it has the mechanism to sense the channel for carrier signal before transmitting, reducing the likelihood of collisions.

c. Flow diagram of CSMA/CD 2018M



Page No.
Date

CSMA/CD (CSMA with collision detection) further improves CSMA by detecting multiple collisions while they are happening and takes steps to resolve them. If a collision is detected, station stops transmitting and waits a random amount of time, and then attempts to retransmit. This helps to minimize the impact of collisions and increase overall efficiency compared to CSMA alone.

[b] Suppose in a CSMA/CD LAN, the maximum end to end propagation delay is 25.6 μsec. If the line is operating in 100MBPS then what will be the minimum frame length (in bytes) of the LAN? 2020M

Given,

Bandwidth, $BW = 100 Mbps$

propagation time, $T_p = 25.6 \mu s = 25.6 \times 10^{-6} s$

Now, for CSMA/CD

transmission time $\geq 2 \times T_p$

$\Rightarrow T_t > 2 \times T_p$ —(1)

and

$T_t = \frac{1}{BW}$ —(2)

from (1), (2)

$\frac{L}{BW} \geq 2T_p \Rightarrow L \geq 2T_p \cdot BW$

$\Rightarrow L \geq 2 \times 25.6 \times 10^{-6} \times 10^8 bps$

$\Rightarrow L \geq 5120 bits$

$\Rightarrow L \geq 640 bytes$ ($\because 8 bits = 1 byte$)

Thus, minimum size of frame for LAN is 640bytes.

c) A CSMA/CD network has a data rate of 100 Mbps and a propagation delay of 5 μs. The minimum frame size is 512 bytes. What is the minimum packet transmission time? 2023E [3][CO2]

Given,

$BW = 100 Mbps = 100 \times 10^6 bps = 10^8 bps$

$T_p = 5 \mu s = 5 \times 10^{-6} s$

$L = 512 bytes$

$\therefore T_t \geq 2 \times T_p \quad \therefore T_{tmin} = 2 \times T_p = \boxed{10^{-5} s}$?

Page No. | Date

(b) A sender transmits 10 packets to a receiver using the Stop-and-Wait protocol. The propagation delay is 100 ms and the transmission time for each packet is 10 ms. If the acknowledgement delay is negligible, what is the time taken to transmit all the packets, Explain steps? [3][CO3] 2023E

$T_p = 100ms$

$T_t = 10ms$

1. Sending packet 1

transmission time = 10ms

2. Wait for ACK

prop delay = 100ms

ACK transmission time = 0 (given)

∴ total time for packet 1 = 10ms + 100ms = 110 ms

3. Similarly for all packets

packets = 10

total trips time = 110ms / packet

∴ Total time = 10 x 110 ms

= 1100 milliseconds

= 1.1s

[b] Why is acknowledgement numbered in Stop-And-Wait protocol? Discuss the situation when unnumbered acknowledgements can create confusion in the sender and receiver end. 2020M

Acknowledgements are numbered in STOP-and-WAIT because they are needed for

→ Detecting Lost Packets: Sender know which packet to resend if the acknowledgement doesn't arrive.

→ Handling out-of-order ack: Numbers prevent misinterpretations and maintain data order.

→ Preventing deadlocks: Numbers distinguish new packets from retransmissions.

Situations with unnumbered ack:

P.T.O.

Page No.
Date

LOST ACK: if ack for packet x is lost, sender won't know if its sent. It might wait indefinately or retransmit unnecessarily, (efficiency)

DELAYED ACK: If ack for x is delayed and ack for y comes first, sender wont understand which one to send next leading to out of order delivery.

4. Explain Go back N protocol. In Stop and wait protocol, derive the relation between the length of the packet (L), bandwidth of the Channel (B) and time of propagation (T_p) to achieve 50% efficiency. 7 marks 2018M

GO BACK-N PROTOCOL

Go Back N is a Sliding window protocol, (N is the window size, i.e the no of frames sender will send before waiting for Ack).

If the acknowledgement of a frame is not recieved within the agreed upon time period, then all the frames in the current window will be retransmitted.

It overcomes the 'inefficiency of 'stop and wait' by allowing the transmitter to continue sending enough frames so the channel is kept busy while transmitter waits for acknowledgement.

Drawbacks:

→ transmit lot of frames even if only 1 is lost
→ error if NAK is lost.

DERIVATION

$$\text{Efficiency} = \frac{\text{Total use-ful time}}{\text{Total cycle time}} = \frac{T_t}{T_t + 2T_p} \quad (1)$$

where T_t = transmission time
T_p = propagation time

also $\text{Bandwidth} = \frac{L}{T_t}$

put in (1)

$$\eta \leq \frac{T_t/T_t}{(T_t + 2T_p)/T_t} \Rightarrow \eta = \frac{1}{1 + \frac{BW\,T_p 2}{L}}$$

Page No.
Date

$$\Rightarrow \eta \leq \frac{1}{1 + \frac{BW.T_p \cdot 2}{L}}$$

for 50% efficiency, $\eta = 1/2$

$\Rightarrow$

$\Rightarrow$ $\boxed{L \geq 2\, T_p\, (B.W)}$

Q.3 (a) A channel has a bit rate of 4kbps and propagation delay of 20ms. What is the minimum size of frame does stop and wait give efficiency of atleast 50% ? 2019M

Given,

propagation time, $T_p = 20 \times 10^{-3}$ s

Bandwidth, $BW = 4$ Kbps

Efficiency, $\eta = 0.5$

$\therefore$ transmission time, $T_t = L/BW$

$\therefore \eta \leq \frac{1}{1 + \frac{BW.T_p \cdot 2}{L}} \Rightarrow 0.5 \leq \frac{1}{1 + \frac{BW.T_p}{L}}$

$\Rightarrow L \geq 2 \times T_p \times BW \Rightarrow \boxed{L \geq 160 \text{ bits}}$

Q.2 A) What are the functions of Data link layer? A channel has a bit rate of 4kbps and a propagation delay of 20 msec. For what range of frame sizes does stop-and-wait give an efficiency of at least 50 percent? 2015

Page No.
Date

Q3. a) Suppose there are 5 stations in a CSMA p-persistent network. The channel is idle with a probability 0.2 and each station has a probability of 0.5 of transmitting in a given time slot. If station 1 is ready to transmit, what is the probability that it will successfully transmit on the first attempt? 2023E [4][CO2]

probability that channel is idle = 0.2 = i

Station transmit = 0.5 = p

∴ probability of successful transmission (no collision)

$= P(\text{channel is idle}) * \prod_{i=2}^{5} P(\text{Station } i \text{ doesnt transmit})$

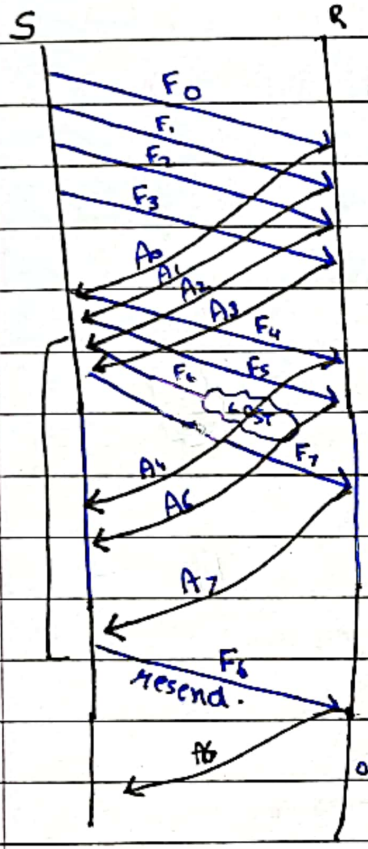
$= 0.2 * (1-0.5)^4$

Prob. = 0.0125

Page No.
Date

Q2. a) In Selective Repeat protocol, the sender's window size is 4 and the receiver's window size is also 4. The sequence numbers range from 0 to 7. The sender sends packets 0, 1, 2, 3 and they are all acknowledged. The sender then sends packets 4, 5, 6, 7, but packet 6 is lost. The sender then sends packet 6 again. What is the minimum number of packets that need to be retransmitted and why? 2023E [2][CO3]

The packets are transferred in the following manner:



In selective repeat ARQ, only the frame which is damaged or lost is retransmitted by transmitter. Hence one packet is needed to be retransmitted.

Or

c) Explain flow control mechanism using Sliding window protocol. [3] [CO1]
2023M

2. a. Explain Selective Repeat Protocol and Go back N protocol with example. 2018S

Page No.
Date

3 [a] Station A needs to send a message consisting of 9 packets to Station B using a sliding window (window size 3) and go-back-n error control strategy. All packets are ready and immediately available for transmission. If every 5th packet that A transmits gets lost (but no acks from B ever get lost), then what is the number of packets that A will transmit for sending the message to B? 2020M

Page No.
Date

[b] Network Routing 2020M

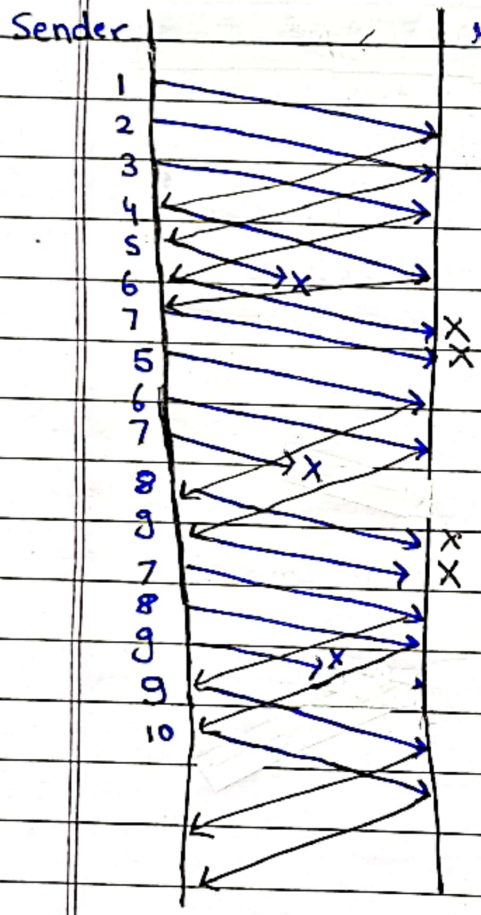
b. Let the system wants to send 10 packets using Go back N protocol with sliding window size (N) as 3. What are the total no of transmissions if every 5th packet is lost. 2018E **(10 marks)**

16

b. Let the system wants to send 10 packets using Go back N protocol with sliding window size (N) as 3. What are the total no of transmissions if every 5th packet is lost. (10 marks)

2018S

They are transmitted as:



∴ total # transmissions = 17

[b] Explain the working of Sliding Window Protocol with suitable example. Explain how ARQ can be used for error correction? How does Go back N ARQ differ from selective repeat ARQ. 2019S

Automatic Repeat Request (ARQ) is an error-control mechanism which uses acknowledgements (or NAK) and timeouts to achieve reliable data transmission over an unreliable link. So retransmission occurs in 3 cases:

→ Damaged frame

→ Lost frame

→ Lost Acknowledgement

Page No. | Date

Anytime error is detected, then NAK is returned and ARQ retransmits specific frames.
If frame is not recognized or damaged by noise then it is considered as lost frame and ARQ performs automatic retransmission.

DIFFERENCE

	GO-BACK N	SELECTIVE REPEAT
i)	Retransmit 'N' no. of frames in case of any error	Retransmit only those frames that have problem.
ii)	If error-rate is high, it wastes a lot of bandwith with redundant t/r.	Less wastage of bandwidth.
iii)	Less complicated	More complicated due to sorting and storage
iv)	It is used most often	It is used less due to high complexity.

1. a. Explain Selective Repeat Protocol with example. Consider a network connecting two systems located 8000 km apart. The bandwidth of the network is 500×10^6 bits per second. The propagation speed of the media is 4×10^6 meters per second. It is needed to design a Go-Back-N sliding window protocol for this network. The average packet size is 10^7 bits. The network is to be used to its full capacity. Assume that processing delays at nodes are negligible. What is the minimum size in bits of the sequence number field? 2018E GATE-2015

Given,
distance = 8000 km
Bandwidth = 500×10^6 bps
Prop. speed = 4×10^6 m/s
Avg packet scene = 10^7 bits

∴ transmission time, T_t = (packet size)/(BW) ⇒ T_t = 0.02 s
propagation time, T_p = Distance/Velocity ⇒ T_p = 2 s
∴ Round trip T_p = 2 × 2 = 4 s

∴ Total packets that can be transferred before an ACK = $\frac{RTP}{T_t} = \frac{4}{0.02} = 200$
So, in Go-Back-N, max sequence no. is one more than window size = 201
It can be represented in $\lceil \log_2(201) \rceil = 8$ bits.

Page No.
Date

Q.7 Write short notes on the following

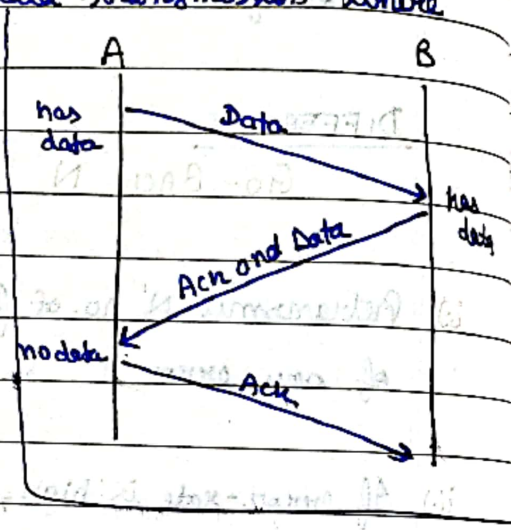
a) Piggy back and Sliding Window Syndrom. 2019S

PIGGY BACK

In all practical situations transmission of data needs to be bi-directional, called full-duplex t/n.

Piggybacking is a technique used in data transmission where acknowledgements are attached to outgoing data frames, optimizing Bandwidth by allowing bidirectional communication without wasting resources on separate acknowledgement channels.

Instead of sending Ack immediately, reciever wait till they have some data to transmit



Disadvantage

→ additional system complexity

→ if DLL takes too long to send ACK, then retransmission takes place.

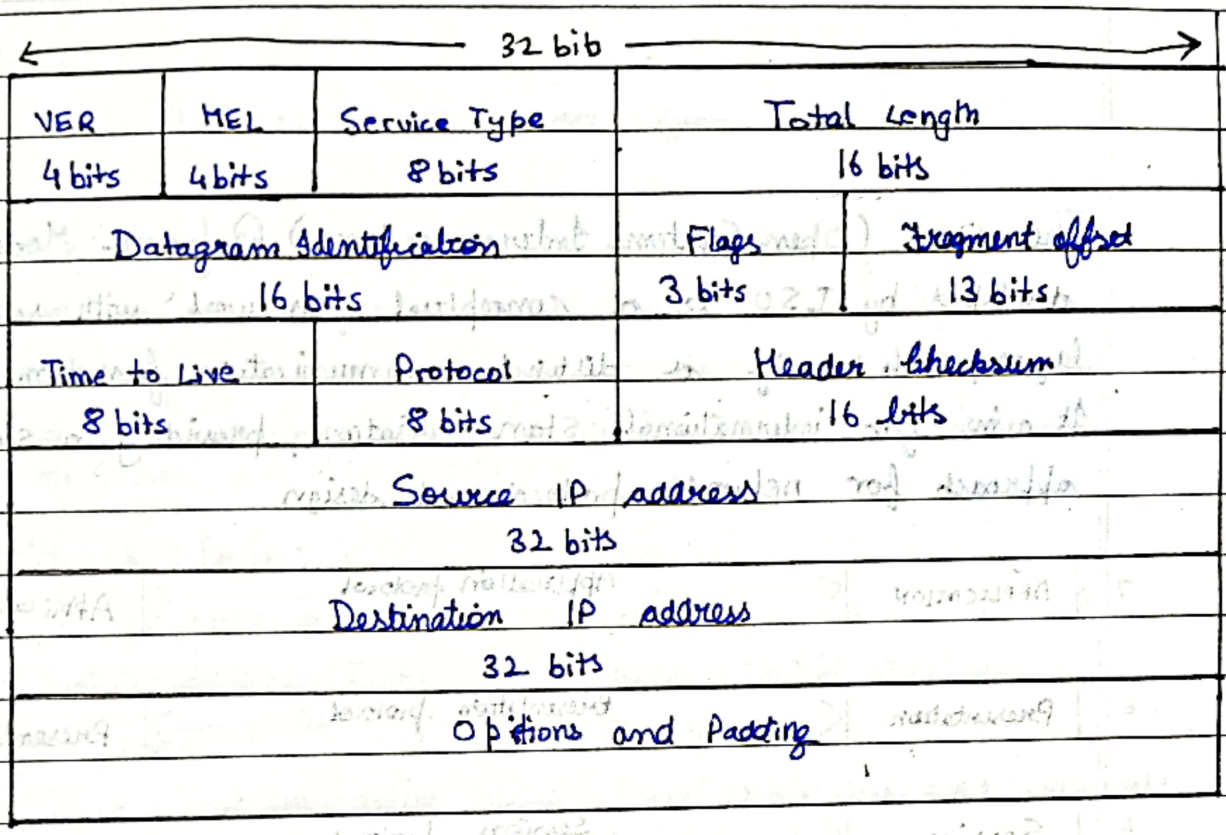
SILLY WINDOW SYNDROME:

out of syllabus

UNIT - 3 : NETWORK LAYER.

Page No. | Date

Q.2(a) Explain the IP header format of IPv4 in detail. 2019M



The IPv4 header usually consists of 20-60 bytes.
Datagram Identification is a unique number assigned by sender used with fragmentation.
Flag consists of 3 bits, first bit is reserved and must be 0
second bit is DF, 0 means allow fragment
Fragment offset is used to reassemble datagrams.
TTL specifies the time, datagram is allowed to travel.
Protocol no. indicates the higher layer protocol to which IP should deliver the data in this datagram. E) ICMP = 1 | TCP = 6 | UDP = 17
Header Checksum is for the info contained in header
IP options is a variable length field used for control or debugging and measurement. E) Timestamp, Record and record route.

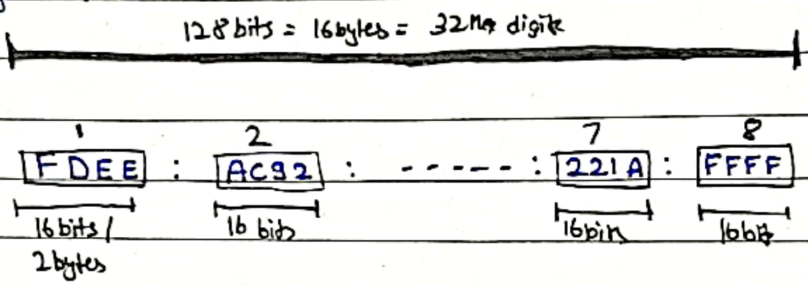
Q4(2.3) Answer IPv4 header questions 2023E [2][CO3]

i. What is the size of the IPv4 header in bytes?
ii. How many bits are used to represent the IPv4 address?
iii. What is the maximum size of an IPv4 datagram?
iv. What is the value of the TTL (Time To Live) field in the IPv4 header for a packet that has to traverse 15 routers?

i) 20 bytes
ii) 32 bits
iii) 65,535 bytes = $2^{16}-1$
iv)

b) IPv6 address structure 2019S

IPv6 addresses are 128-bit hexadecimal numbers, i.e. 16 byte octets, i.e 8 groups of four hexadecimal digits separated by colons:

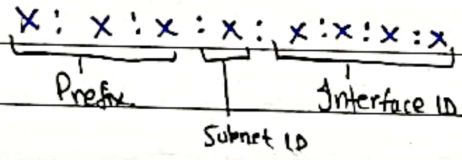


IP addresses can be shortened / abbreviated by omitting leading zeros within each group and collapsing consecutive group of zeros into double colon (::). (only once)

Eg) original ⇒ AC81 : 9840 : 0086 : 0000 : 0000 : BBFF : 000F : FFFF

abb ⇒ AC81 : 9840 : 86 :: BBFF : F : FFFF

They generally have a network prefix, host identifier, interface



Q.5 Write short notes on any two of the following:
(a) IPv6 2019M

IPv6 is the latest generation Internet protocol designed a successor to IPv4. It was designed to enable high performance, scalable internet. It overcame weakness of IPv4 and added several new features.

→ Larger Address Space: IPv6 has 128 bit address space which provides approximately 340 undecillion IP addresses.

→ Buffer Header Format: It has a better header structure where options are separate from base header which are inserted when needed. Speeds up Routing.

→ More Security: IPv6 includes security in basic specification. It includes encryption of packets (ESP) and authentification of sender of packets (AH).

It has better support for resource allocation, includes plug and play and follows good practices of IPv4 and rejects minor flaws / obsolete items of IPv4.

Q.4
(A) Compare different classes of IPv4 in terms of netid and hostid. What are the advantages and disadvantages of classfull addresses? 2018S

CLASSES	NETID (bits)	Host ID (bits)	NETWORK RANGE
A	8	24	1.0.0.0 – 127.255.255.255
B	16	16	128.0.0.0 – 191.255.255.255
C	24	8	192.0.0.0 – 223.255.255.255
D	Reserved	——	224.0.0.0 – 239.255.255.255
E	Reserved	——	240.0.0.0 – 255.255.255.255

ADVANTAGES

→ Classfull addressing is straight forward and easy to understand with clear divisions into classes based on the size of the network.

→ Allows simple expansion as it has fixed no. of network for each class.

→ Its efficient interms of address space as it allocates large blocks to organizations.

DISADVANTAGES

→ LACK OF INTERNAL ADDRESS FLEXIBILITY: Big organizations are assigned large monolithic blocks of addresses that dont match well the structure of underlying internal nfw.

→ INEFFICIENT USE OF ADDRESS SPACE: The existance of only three block sizes (A, B, C) leads to waste of limited IP address space.

→ PROLIFERATION OF ROUTER TABLE ENTRIES: The growth of internet necessitates more router table entries, leading to performance issues, exacerbated by inefficient address space allocation.

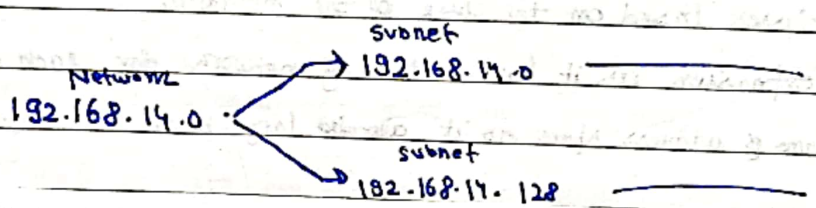
Page No. | Date

a) What is subnetting in IP network? Explain with suitable examples[4] [CO3]
2023M

A subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. By this, an organization (or ISP) that is granted a range of addresses may divide the range into several subranges and assign them to a subnetwork.
Computer that belong to a subnet are addressed with an identical most-significant bit-group in their IP addresses.
By this we can
→ improve security
→ easily administer individual subnetworks

Its done by using these steps:
1. Identify class of IP address and Default Subnet Mask.
2. Convert the default subnet mask into binary.
3. Note #hosts reqd. per subnet and find subnet generator (SG) and octet position.
4. Generate the new subnet mask.
5. Use the SG and generate the network ranges (subnets) in the appropriate octet position.

Ex:



b) i) Given the IP address 10.0.0.0/8, how many subnets and hosts per subnet can be created? [2][CO3]
2023E

IP address belongs to class A ⇒ network bit = 8
Subnet mask : 11111111.00000000.00000000.00000000 = 255.0.0.0
∴ no. of borrowed bits = 8 − 8 = 0 = b (i.e no of subnet bits = 0)
∴ # subnets = $2^b = 2^0 = 1$

∴ no of host bits, h = 32 − 8 = 24
∴ # hosts per subnet = $2^h - 2 = 2^{24} - 2 = 16,777,214$

2. The address of a class B host is to be split into subnets with a 6-bit subnet number. What is the maximum number of subnets and the maximum number of hosts in each subnet? Consider the following routing table at an IP router

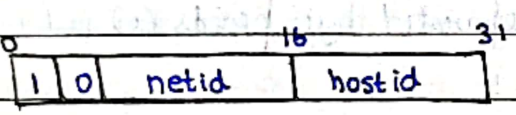
2018 M ↑ UGC NET 2017

GATE 2015

	Network No.	Net Mask	Next Hop	
i	128.96.170.0	255.255.254.0	Interface 0	a
ii	128.96.168.0	255.255.254.0	Interface 1	b
iii	128.96.166.0	255.255.254.0	R2	c
iv	128.96.164.0	255.255.254.0	R3	d
v	0.0.0.0	Default	R4	e

For each IP address in Column I, match the correct entries to Next Hop in Column III. 5 marks

Page No. / Date

a.) 

subnets = $2^6 - 2 = 62$

Total n/w id = 16 + 6 = 22

∵ n/w id + host i/d = Total n/w id

⇒ # host id = 32 − 22 ⇒ h = 10

∴ # hosts = $2^h - 2 = 2^{10} - 2 = 1022$

b.) i.) 128. 96. 171. 92

AND 255. 255. 254. 0

128. 96. 170. 0 (Matched), next hop → I_0

ii.) 128. 96. 168. 151

AND 255. 255. 254. 0

128. 96. 166. 0 (Matched), next hop → R_2

iii.) 128. 96. 163. 151

AND 255. 255. 252. 0

128. 96. 162. 0 (not matched)

try to mask with 2nd longest prefix

128. 96. 163. 151

AND 255. 255. 252. 0

128. 96. 160. 0 (No match) Next hop → R_4 (Default)

iv.) 128. 96. 165. 121

AND 255. 255. 254. 0

128. 96. 164. 0 (Matched), next hop → R_3

∴ i → a | ii → c | iii → e | iv → d

Page No.
Date

[b] What is dotted decimal notation in IPv4 addressing and hexadecimal notation in IPv6 addressing? An organization is granted the block 130.56.0.0/16. The administrator wants to create 1024 subnets. 2018S

a. Find the subnet mask
b. Find the number of addresses in each subnet
c. Find the first and last addresses in subnet 1
d. Find the first and last addresses in subnet 1024

Ans Dotted decimal notation is a way of representing IPv4 addresses using four decimal numbers separated by periods (.).

Eg.) 192.168.1.1

Hexadecimal notation is a way of representing IPv6 addresses where each hexadecimal number represents four bits of IPv6 address. IPv6 addresses are 128 bit long, so they are typically represented as eight groups of four hexadecimal digits separated by colons.

Eg.) 2001 : 0dB8 : 85a3 : 0000 : 0000 : 8a2e : 0370 : 7334.

a.) $n = 10 \quad \because 2^{10} = 1024.$

Its in class B as $128 < 130 < 191$

$\therefore$ Default Mask = /16

Bits for Subnet = /10

$\therefore$ Subnet mask = /26

i.e. 255.255.255.192

b.) Remaining bits = 32 − 26 = 6 bits = b

$\therefore$ we can allocate $2^b - 2$ address

$= 2^6 - 2 = 64 - 2$

$= 62$ addresses

c) First address of subnet 1 = 130.56.0.1

last address of subnet 1 = 130.56.0.62

d.) first address of subnet 1024 = 130.56.255.193

last address of subnet 1024 = 130.56.255.254.

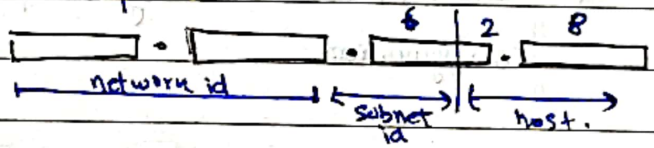
Page No.
Date

3. a. Explain IPv4 Classful IP addressing? The address of a class B host is to be split into subnets with a 6 - bit subnet number. What is the maximum number of subnets and maximum number of hosts in each subnet? 2018 E

IPv4 classfull addressing refers to the original method of allocating IP addresses, which was based on dividing the address space into classes: A, B, C, D, E. Each class had a fix number of network and host bits, which determine the no. of networks and host per network that could be accomodated.

	← 32 bits →			→ Range of host address
A	0	Network	Host	1.0.0.0 – 127.255.255.255
B	10	Network	Host	128.0.0.0 - 191.255.255.255
C	110	Network	Host	192.0.0.0 - 223.255.255.255
D	1110	Multicast address		224.0.0.0 – 239.255.255.255
E	1111	Reserved for future use		240.0.0.0 – 255.255.255.255

This system is rigid and lead to ineffient address allocation with the rapid growth of internet. And was replaced.



Given,

Its in class B, so network bits = 16

Subnet bits, b = 6

Host bits = 32 − 16 − 6 = 10

Subnets = 2^b = 64

hosts = $2^{10} - 2$ = 1022

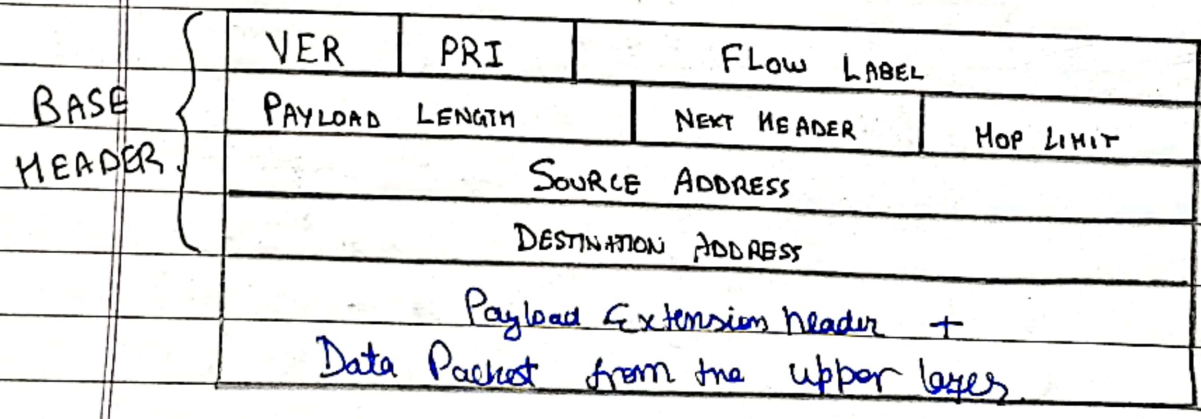
ii) What is the network address and broadcast address for the IP address 10.20.30.40/26? 2023E [2][CO3]

Page No.
Date

[b] What are the major differences between IPv4 and IPv6? Discuss header format and Network addressing with reference to IPv6. 2019S

	IPv4	IPv6.
1.	IPv4 addresses are 32 bits (4bytes) in length and represent 2^{32} (aroamd 4 billion addresses).	IPv6 addresses are 128 bits (16bytes) in length and represent 2^{128} (aroamd 310 undecillion addresses).
2.	Its address is written in dotted decimal notation like 121.8.12.2.	Its address is written in hexadecimal notation like FABC:AC77:7834:2222:FACB:0000:0000:4567
3.	The basic length of IPv4 header comprises a minimum of 20 bytes. The max length of the IPv4 header is 60 bytes, and it uses 13 fields to identify various control settings	The IPv6 header is a static header of 40 bytes in length and has only 8 fields. Optional information is carried by an extension header, placed after IPv6 header.
4.	The IPv4 node has only Stateful auto-configuration.	The IPv6 node contains both a stateful and stateless address auto config mechanism
5.	Security in IPv4 networks is limited to tunneling blw two networks	IPv6 has been designed to satisfy the growing and expanded need for network security.

IPv6 Header



Page No.
Date

The header has eight fields:

1) VERSION (VER): It is a four bit field which defines the version of IP such as IPv4 or IPv6.

2) PRIORITY: It is a 4 bit field which defines the priority of the packet which is important in connection with the traffic congestion.

3) FLOW LABEL: It is a 24 bit (3 byte) field which is designed for providing special handling for a particular flow of data.

4) PAYLOAD LENGTH: This is a 2 byte length field which is used to define the total length of IP datagram excluding the header.

5) NEXT HEADER: It is an 8 bit field which defines the header which follows the base header in the datagram.

6) HOP LIMIT: This is an 8 bit field which has same purpose as time to live in IPv4

7) SRC | DEST Address: 16 byte IP address which identifies original src and final dest of datagram.

Network addressing already discussed.

Page No.
Date

(b) Explain the distance vector routing algorithm and give the limitations of this algorithm. 2019M

Distance vector routing algorithm is one of the most common intradomain routing algorithm. It is used in Routing information protocol where each router maintains a table called vector, such a table gives the best known distance to each destination and the information about next node. It is also known as distributed Bellman Ford routing algo. It follows:

1.) Initialization: Each router initializes its distance vector / vector table by only knowing the cost to directly connected neighbours.

2.) Sharing: Routers periodically share their entire distance vector table with immediate neighbours.

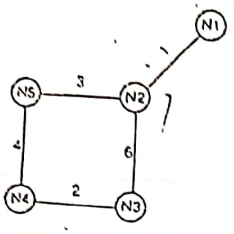
3.) Updating: When router receives a distance vector table from neighbour, it checks for
→ new destination and adds them in its table.
→ Shorter paths and updates their distance.

4.) This process continues till the network stablizes.

LIMITATIONS

→ Count to infinity problem which is solved by split horizon algo.
→ does not take bandwidth into consideration when choosing route which is solved by Link State Routing Algo

3. What will be the the final distance vectors at different nodes for the following given network where N1,N2,N3,N4,N5 represents Nodes of the network? 2018M 4 marks



Page No.
Date

for N_1

Dest	Dist	Next
N_1	0	—
N_2	1	N_2
N_3	7	N_2
N_4	8	N_2
N_5	4	N_2

for N_2

Dest	Dist	Next
N_1	1	N_1
N_2	0	—
N_3	6	N_3
N_4	7	N_5
N_5	3	N_5

for N_3

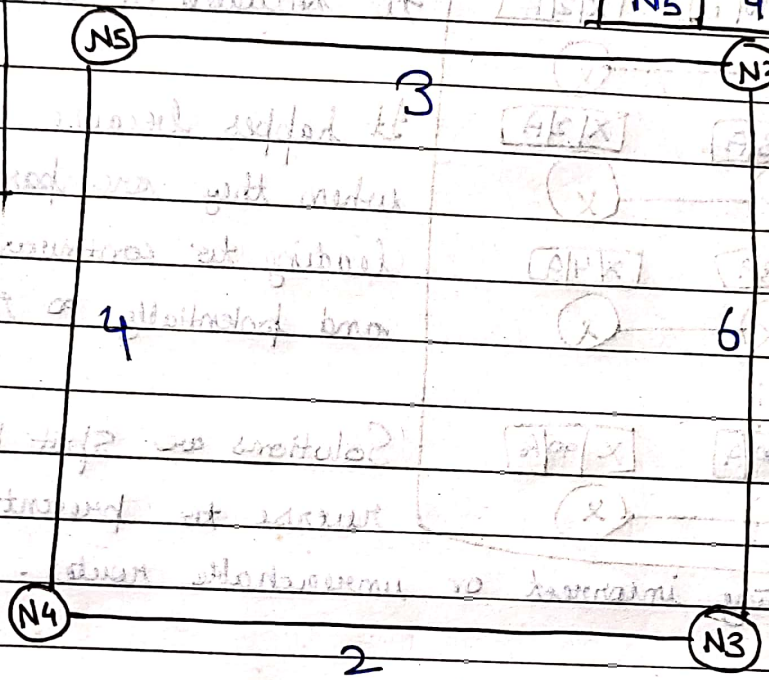
Dest.	Dist	Next
N_1	7	N_2
N_2	6	N_2
N_3	0	—
N_4	2	N_4
N_5	6	N_4

for N_4

Dest	Dist	Next
N_1	8	N_5
N_2	7	N_5
N_3	2	N_3
N_4	0	—
N_5	4	N_5

for N_5

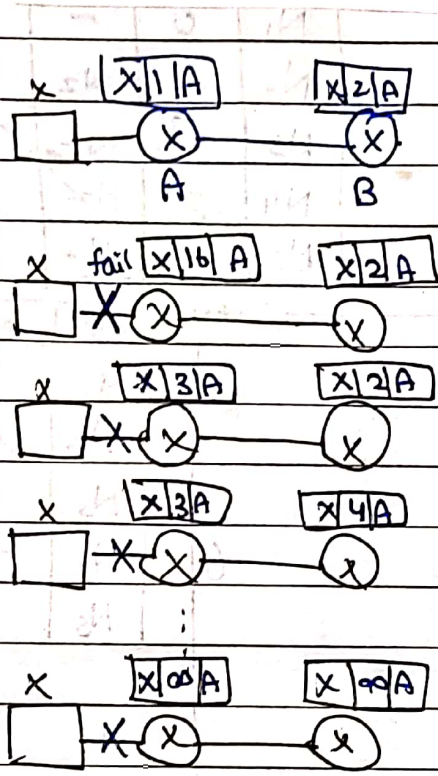
Dest	Dist	Next
N_1	4	N_2
N_2	3	N_2
N_3	6	N_4
N_4	4	N_4
N_5	0	—



Page No.
Date

3. a. Explain Distance Vector Routing (DVR) algorithm. What is count to infinity problem? 2018S
b. What is count to infinity problem in DVR. Explain Link state algorithm with example. How is switch different from router?
2018E (10 marks)

Eg:)



The count to infinity problem occurs in DVR algo when routers inadvertently create routing loops due to outdated or incorrect information.

It happens because routers can't detect when they are part of a looped path, leading to continuously increasing and potentially ∞ routing loops.

Solutions are split horizon and poisoned reverse to prevent routers from propagating incorrect or unreachable routes.

LINK STATE ROUTING ALGO

It is an intradomain routing algo used by OSPF (open shortest path first). Link state is determined by routers using hello packets. All the routers share their link states with each other flooding link state packets. Based on link state information, routers determine the shortest path using dijkstra's algorithm. With the use of a link state routing algo, routers route the frames with a global knowledge of CN.

Ex:)