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.

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.

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

SIXTH SEMESTER B.TECH (COE)

END TERM EXAMINATION (May 2018)

CO306 COMPUTER NETWORKS

Time: 3 hours Max. Marks: 40

Note: Attempt any four questions. Each question is of 10 marks.
Assume suitable missing data, if any.

Total No. of Pages 02 Roll No:

VI SEMESTER B.Tech.(Col

SUPPLIMENTARY EXAMINATION May- 2019

Paper Code: CO-306 Title of Paper: Computer Networks

Time: 3:00 Hours Max. Marks : 40

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

Total No. of Pages 02 Roll No:

VI SEMESTER B.Tech. (CO)

SUPPLIMENTARY EXAMINATION Sept-2019

Paper Code: CO-306 Title of paper: Computer Networks

Time: 3:00 Hours Max. Marks : 40

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

Signature

Total No. of Pages 02

Roll No: 019

V SEMESTER B.Tech. (CO/SE)

SUPPLIMENTARY EXAMINATION FEB-2018

Paper Code:CO/SE 305 Title of paper: Computer Networks

Time: 3:00 Hours Max. Marks :70

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

— 132 —

Total No. of Pages: 1

SIXTH SEMESTER Roll No. .....

B.TECH (COE)

SUPPLEMENTARY EXAMINATION (August 2018)

CO-306 COMPUTER NETWORKS

Time: 3 hours Max. Marks: 40

Note: Attempt any four questions. Each question is of 10 marks.
Assume suitable missing data, if any.

Sub.

Roll No.

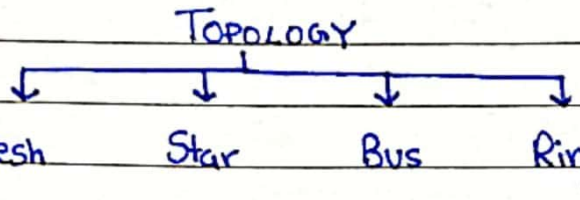
Date	Grade/ Marks	Signature

UNIT-1 : INTRODUCTION CONCEPTS

Page No. | Date

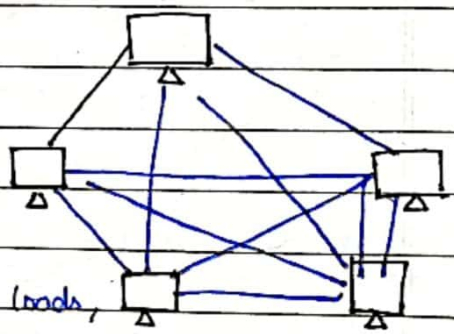
B) Explain the Bus, Star, Ring, Hybrid and Tree network topologies giving their advantages and disadvantages. 2019S

(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:

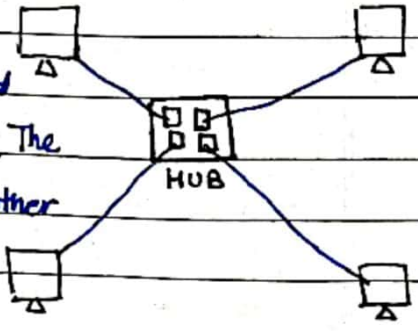
→ Dedicated links ensure individual data loads, eliminating traffic problems.
→ Robustness: System remains functional even if a link is usable
→ Enhance privacy and security due to dedicated links
→ Easy fault identification and isolation through point-to-point links.

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

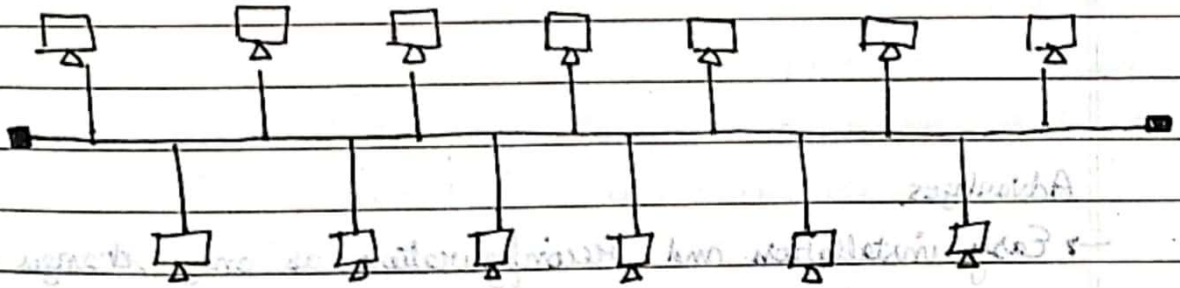
cables = n
ports = n

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 redundant cabling.

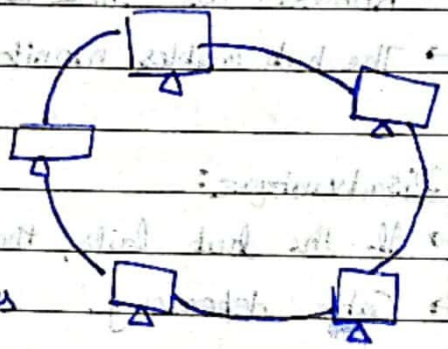
Page No.
Date

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

Q2) Q2) What is the difference between guided and unguided transmission media? Give an example of each. 2023E [2][CO1]

Guided Media is a communication medium which allows the data to get guided along it. For the media mean to have a point to point connection.

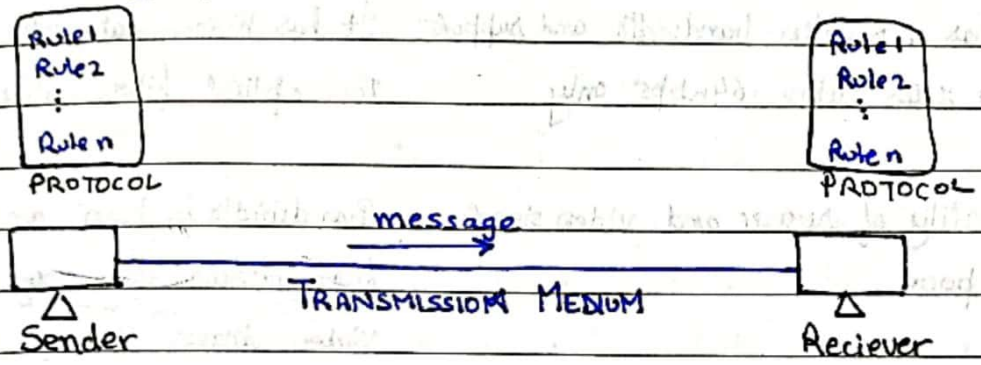
The wireless Media is also called unguided media.

Wired Media	Wireless Media.
1. The signal energy is contained and guided within a solid medium.	The signal energy propagates in the form of unguided EM waves.
2. Used for point to point communication.	Used for radio broadcasting to all.
3. Leads to discrete network topologies	Leads to continuous network topologies
4. Additional Nr capacity can be procured by adding more wires	It is not possible to procure additional capacity
5. Installation is costly, time consuming and complicated.	Installation needs less time and money.
6. Attenuation depends exponentially on the distance	Attenuation is proportional to the square of distance
Eg:) Twisted wire cable, Coaxial cable, Optical fibre cable.	Radio, IR

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. 2018S

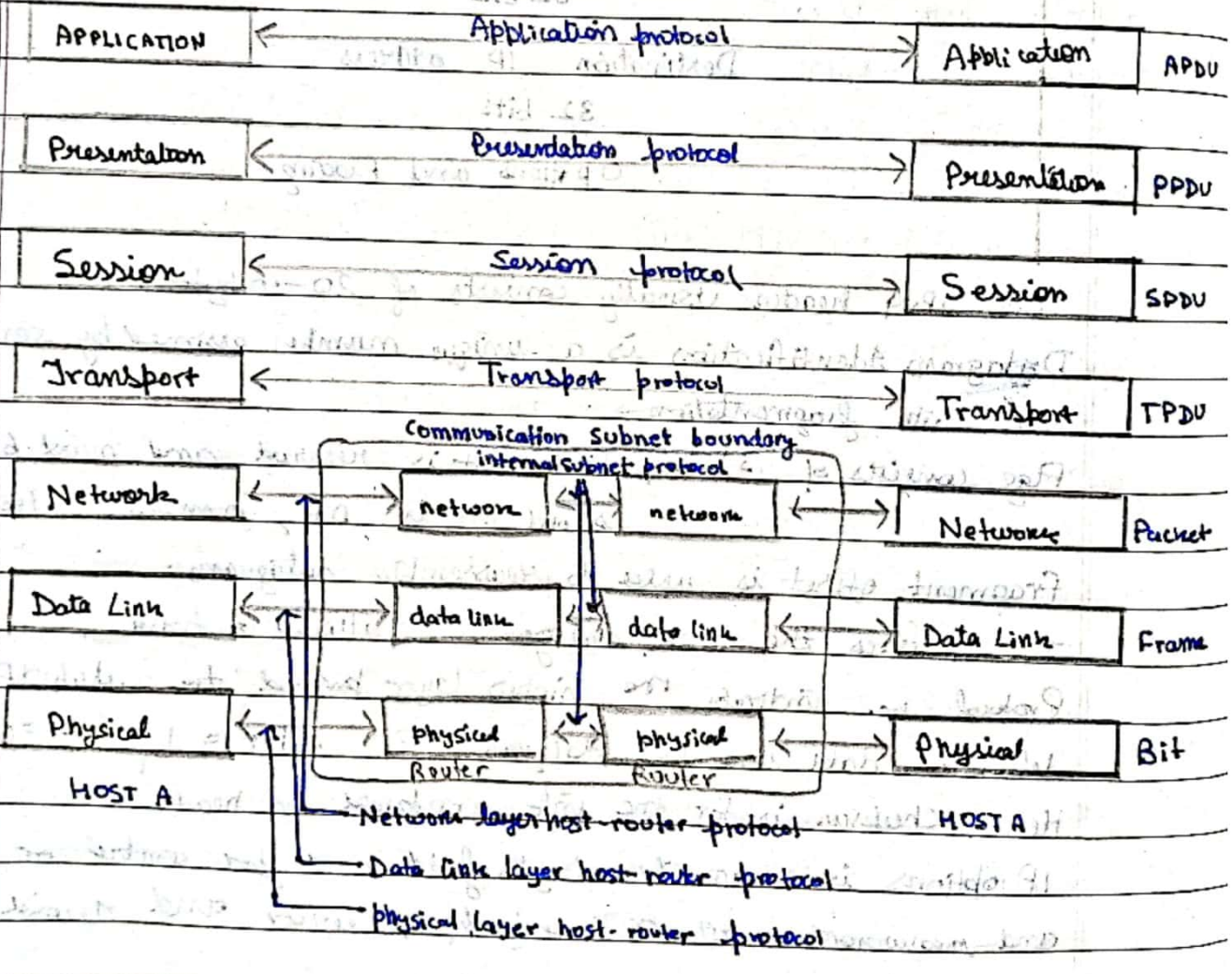
	GUIDED MEDIA	UNGUIDED MEDIA
	Wired communication occurs through bounded transmission media.	Wireless communication occurs through unbounded transmission media.
	Signal propagates through wires.	Signal propagates through air
	Its used for point to point comm^n.	It is suited for radio broadcast in all dir^n.
	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

Page No.
Date

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 -

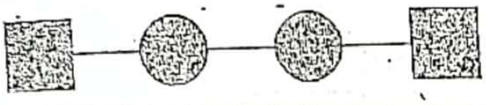
Page No.
Date

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

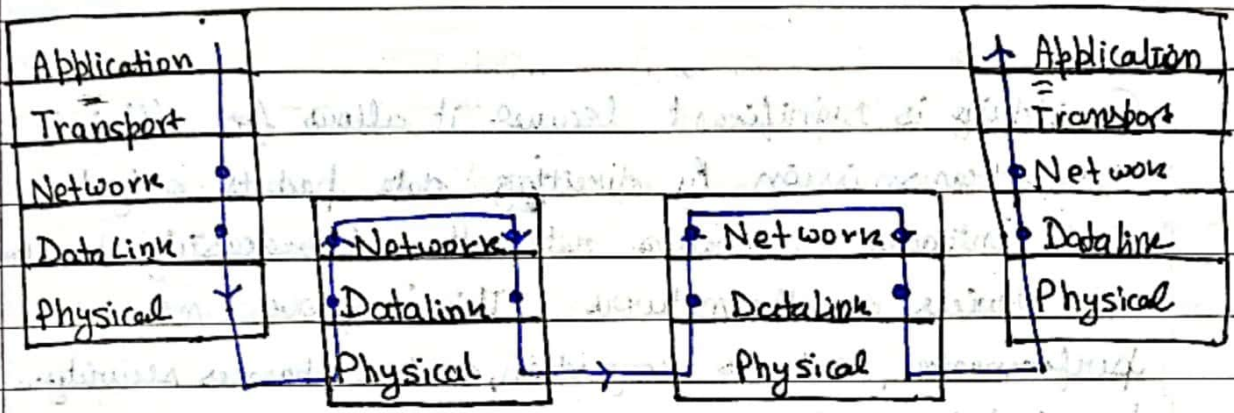
	OSI Model	TCP/IP Model
1.)	OSI stands for open system interconnection.	TCP/IP implies Transmission Control Protocol / Internet Protocol.
2.)	It was developed by ISO in 1984	It was developed by ARPANET in 1982
3.)	It consists of 7 layer : starting from bottom Physical, data-link, network, transport, session, 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



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.

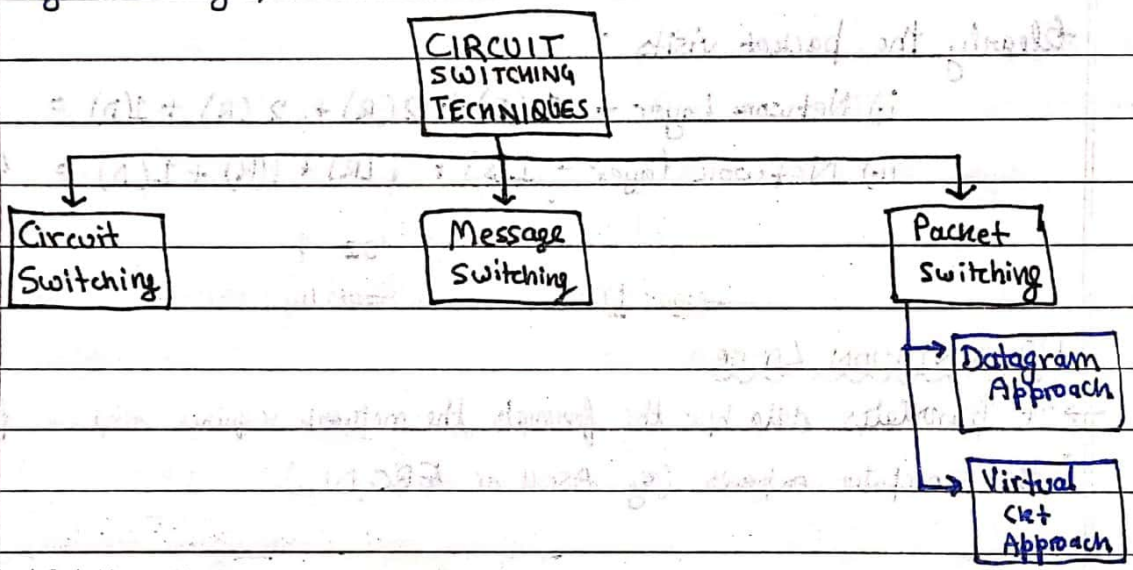
→ It allows addition of check points (i.e. synchronisation points) into a stream of data. Incase of crash, retransmission can start from checkpoint instead of start.

c. Switching/ Multiplexing Techniques 2005

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? 20185 (10 marks)

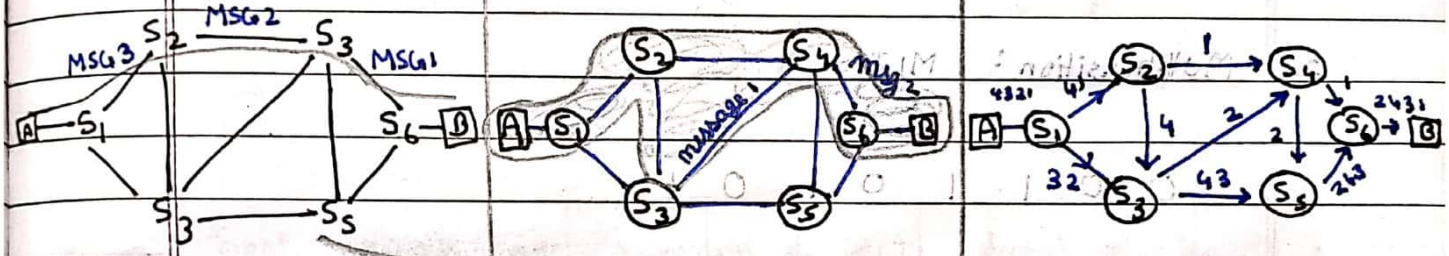
Switching is significant because it allows for efficient data transmission by directing data packets only to their intended destination rather than broadcasting them to all devices on the network. This improves network performance, reduces congestion, and enhances security by isolating traffic.



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 waste of Bandwidth	No waste of bandwidth.
Not suitable for handling interactive traffic	Suitable for handling interactive traffic	Suitable for handling interactive traffic.



c. Virtual Circuit Network 2018E

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 communication. 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 receiver.

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

UNIT 2.2 : LLC

(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 $T(x)$.

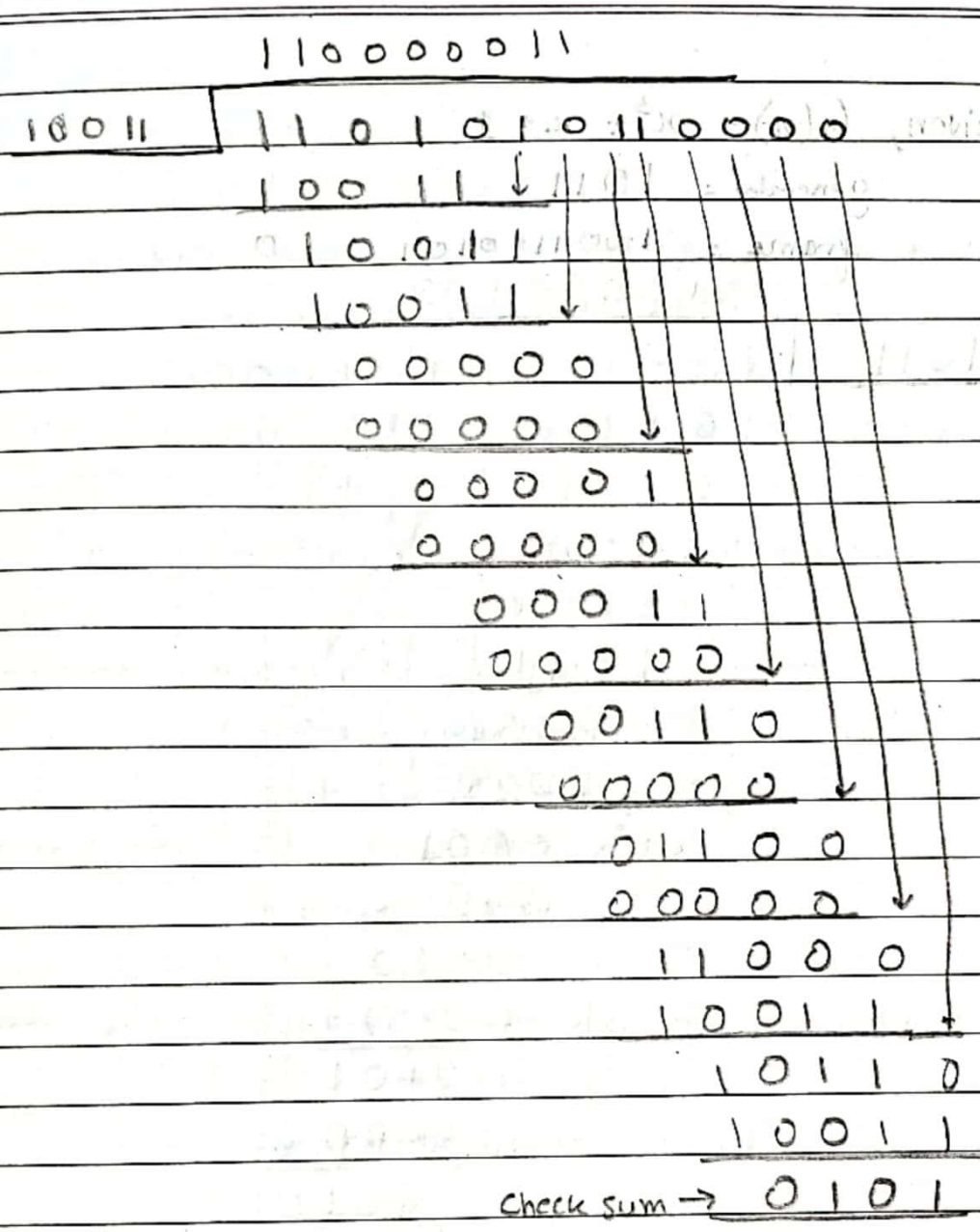
Given,

$G(x) = x^4 + x + 1$

$\therefore$ Generator = 10011

Frame = 110101011

Page No.
Date



∴ 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
                ----
                 0100
                 0000
                 ----
                  100
```

∴ transmitted bit string : 1001110101100

Corrupt bit : 1000110101100

Page No.
Date

Reciever side

```
                                1
          1011 | 1000111010100
                 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. 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

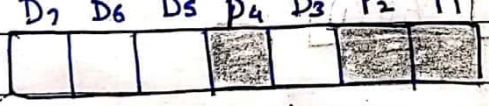
Code word = 101001100

Q.6.

[a] Describe the following: 2018S

(i) Hamming Codes

Hamming code is a linear block code which is used for error detection. The parity bits are inserted in b/w the data. 7 bit hamming code is common



parity bit at position 2^n

$P_1 P_2 P_4$ → parity bits | $D_3 D_5 D_6 D_7$ → data bits.

∴ $P_1 \rightarrow D_3 D_5 D_7$

$P_2 \rightarrow D_3 D_6 D_7$

$P_3 \rightarrow D_5 D_6 D_7$

parity of even is set → so $P_1 P_2 P_3$ is zero

Eg:) Data word = 1011

Code → 1 0 1 0 1 0 1

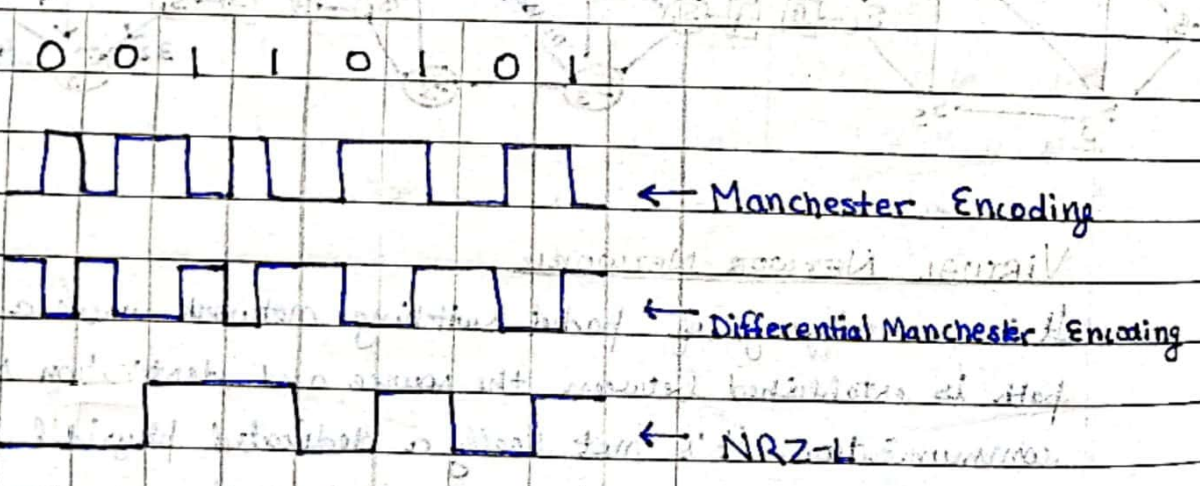
(101) (101) (111)

Page No.
Date

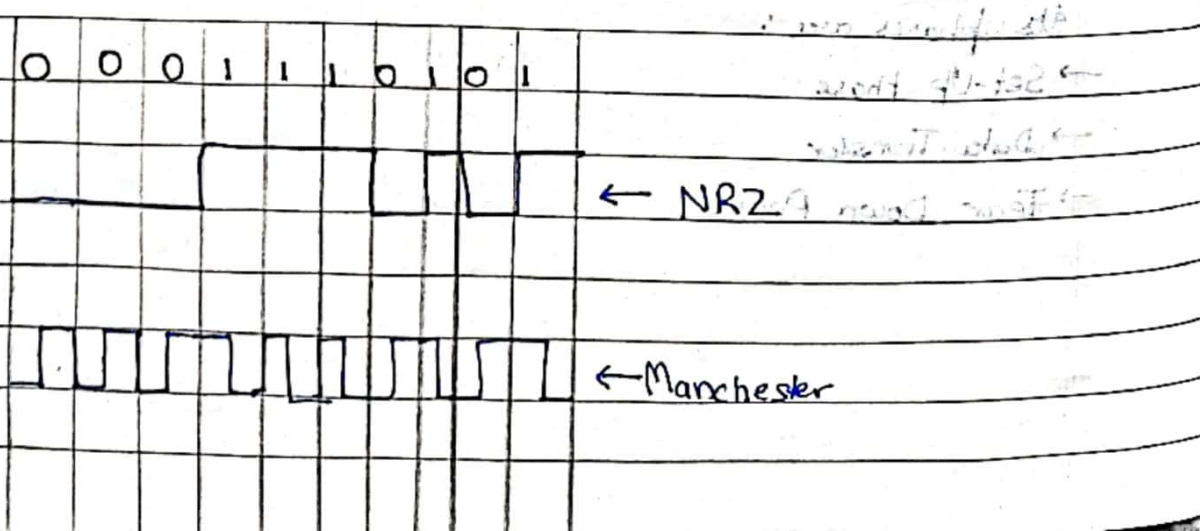
[b] What are different data encoding techniques? Explain and Encode data stream 00110101 by using Manchester, Differential Manchester and NRZ-L encoding methods. 2019S

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



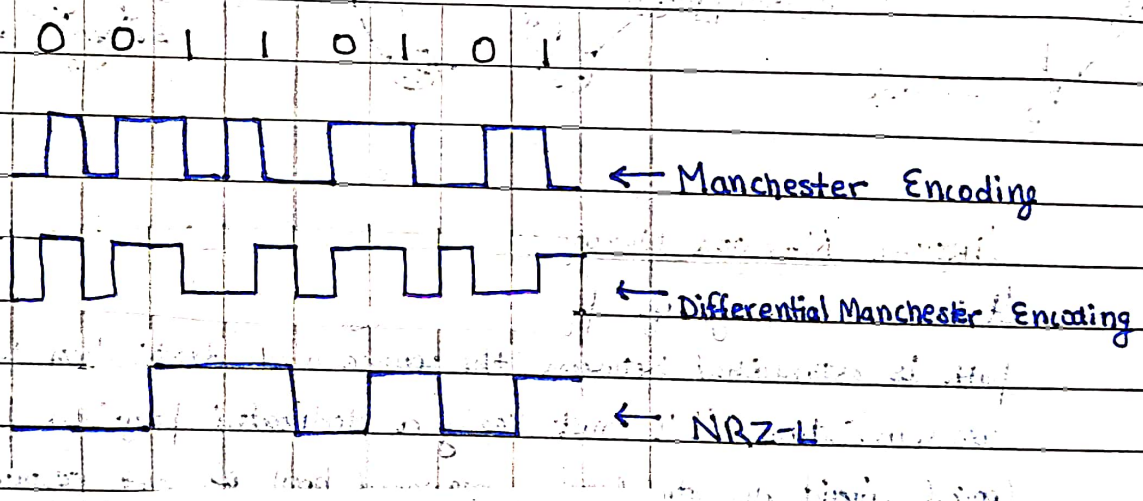
4[a] Draw the following encoding scheme for the bit stream: 0001110101
I. NRZ II. Manchester coding 2020M



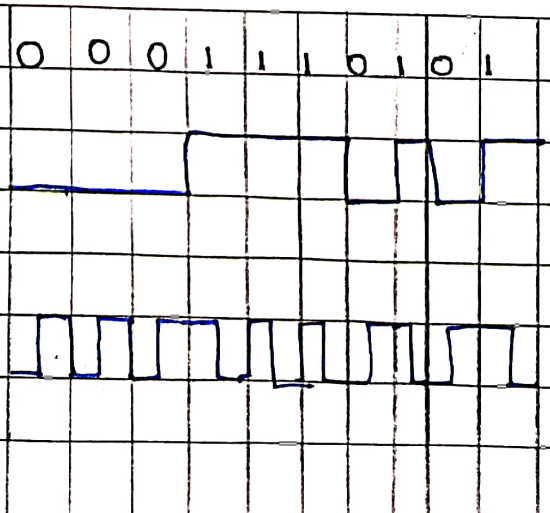
[b] What are different data encoding techniques? Explain and Encode data stream 00110101 by using Manchester, Differential Manchester and NRZ-L encoding methods. 2019S

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

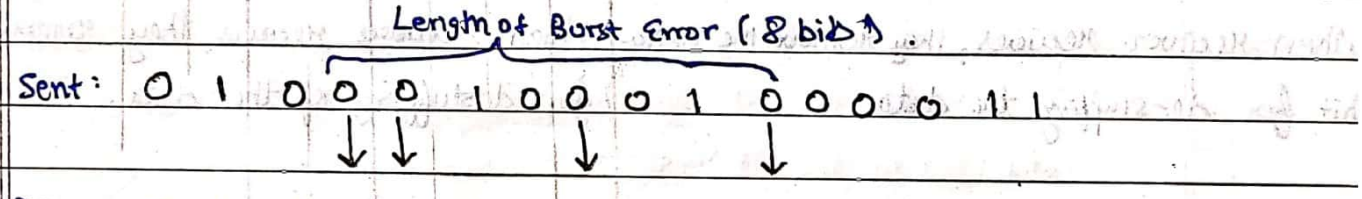
(b) Sketch the waveform for the bit steam 10110010 in differential Manchester encoding scheme. 2019M

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).



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

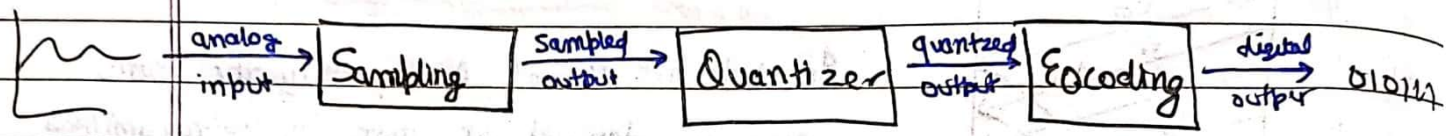
- 1 1 0 0 0 0 1 | 1

original data | parity bit (odd).

Page No.
Date

(c) PCM 2019M

Pulse Code Modulation is used to convert Analog Signal into Digital data.



- Sampling is done every T_s
  $\therefore f_s > 1/T_s$

  three sampling methods
  - Ideal : each instant impulse
  - Natural : pulse of short width with varying amplitude
  - Flat-top : ——————— fixed amplitude.

- Quantization is the process of measuring the numerical values of the samples and giving them a table value in a suitable scale
  It can be
  - Linear Modulation
  - Non Linear Modulation

It has European (30 channel) and American (24 channel) standards.

Page No.
Date

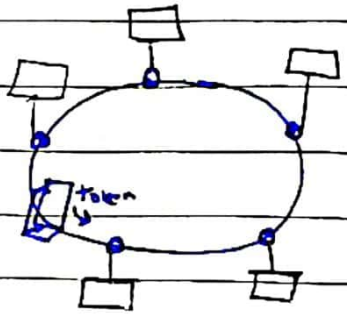
[b] If we want to detect two-bit errors, then what should be the minimum Hamming distance? 2020M

$t = 2$

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

(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)	EDA	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 architecture 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 ETHERNET (10 Base-T)	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.

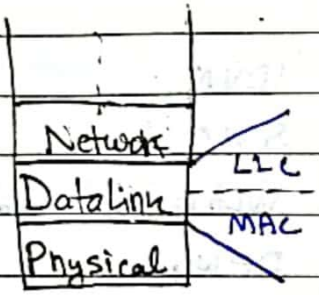
→ CRC : 4Byte CRC is used to detect errors in a given frame.

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 & it. 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 address) 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

When two or more users want to access a shared channel, a model is needed

→ Interface Adaptive Dynamic Channel Allocation (IA-DCA)

→ Location Adaptive Dynamic Channel Allocation (LA-DCA)

→ Traffic Adaptive Dynamic Channel Allocation (TA-DCA)

(b) HDLC 2019M

It is a bit oriented protocol, SDLC (synchronous DLC) developed by IBM later standardized by ISO as High-Level Data Link Control protocol

Beginning and Ending Seq: 01111110
This sequence is also transmitted during any times that the link is idle so that the sender and receiver can synchronize their clocks.

Header: Address and control Field

Body: Payload

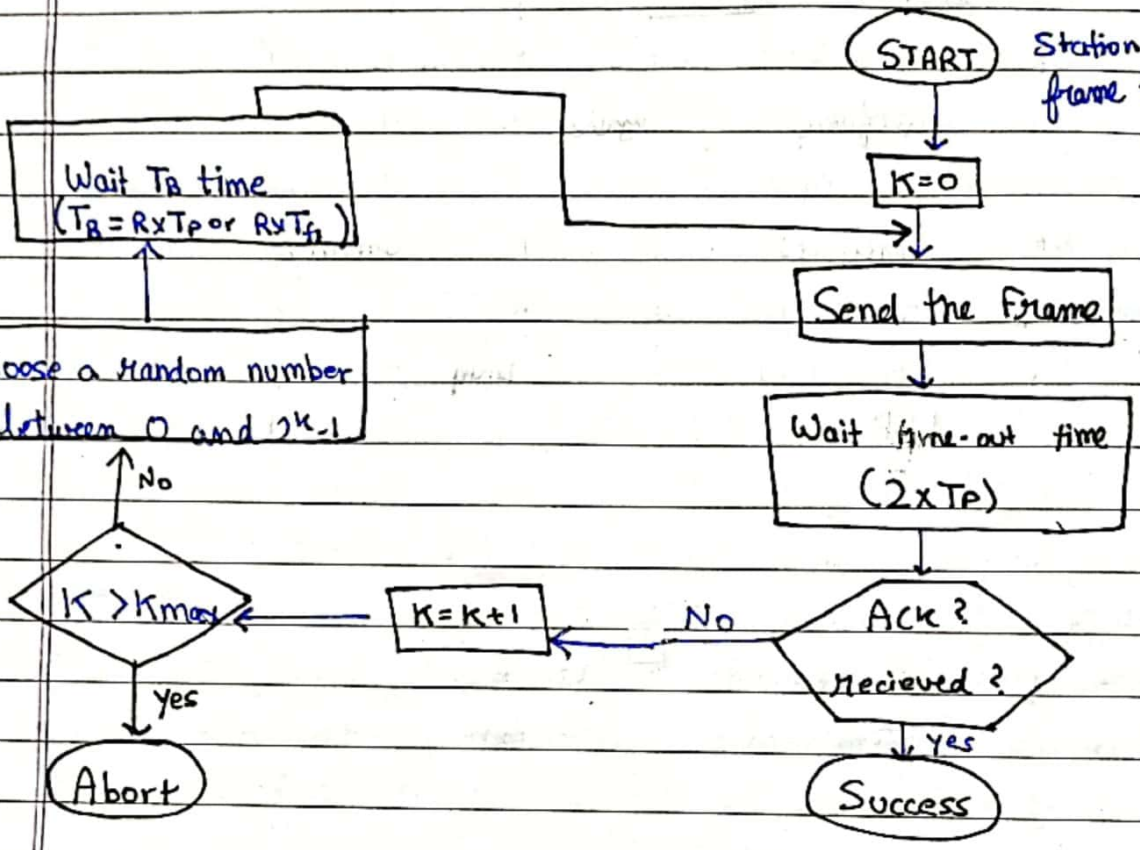
The type of frame is determined by control field
I-frame (information) : 1st bit is 0
S-frame (supervisory) : 1st 2 bits is 10
U-frame (unnumbered) : 1st 2 bits is 11

UNIT 2.1 : Medium Access Control Sublayer

Page No. | Date

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

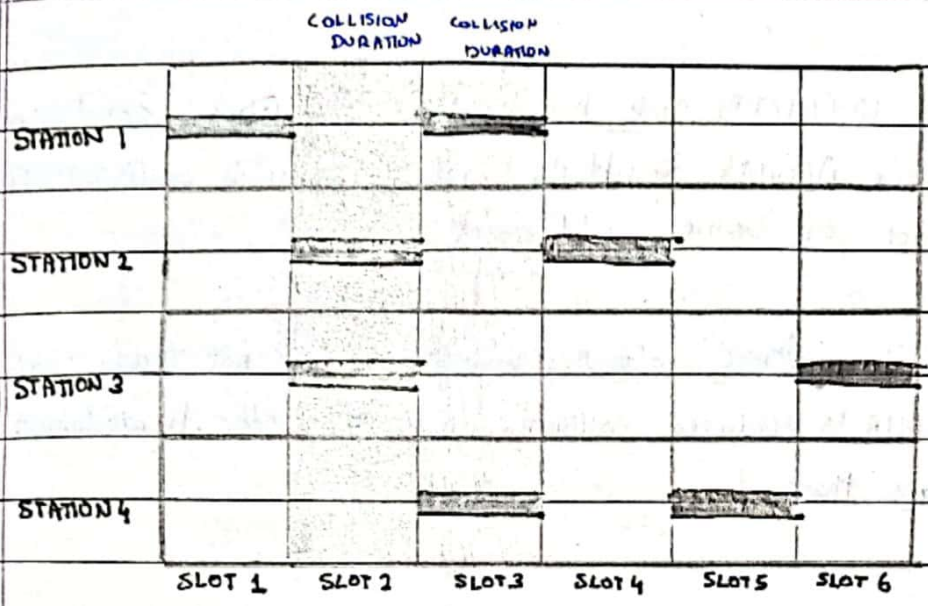
5. Write Short notes on any two: 3.5x 2 = 7 marks
a. Flow diagram of Pure Aloha 2018M



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 ALOHA, so in scenarios with more active devices

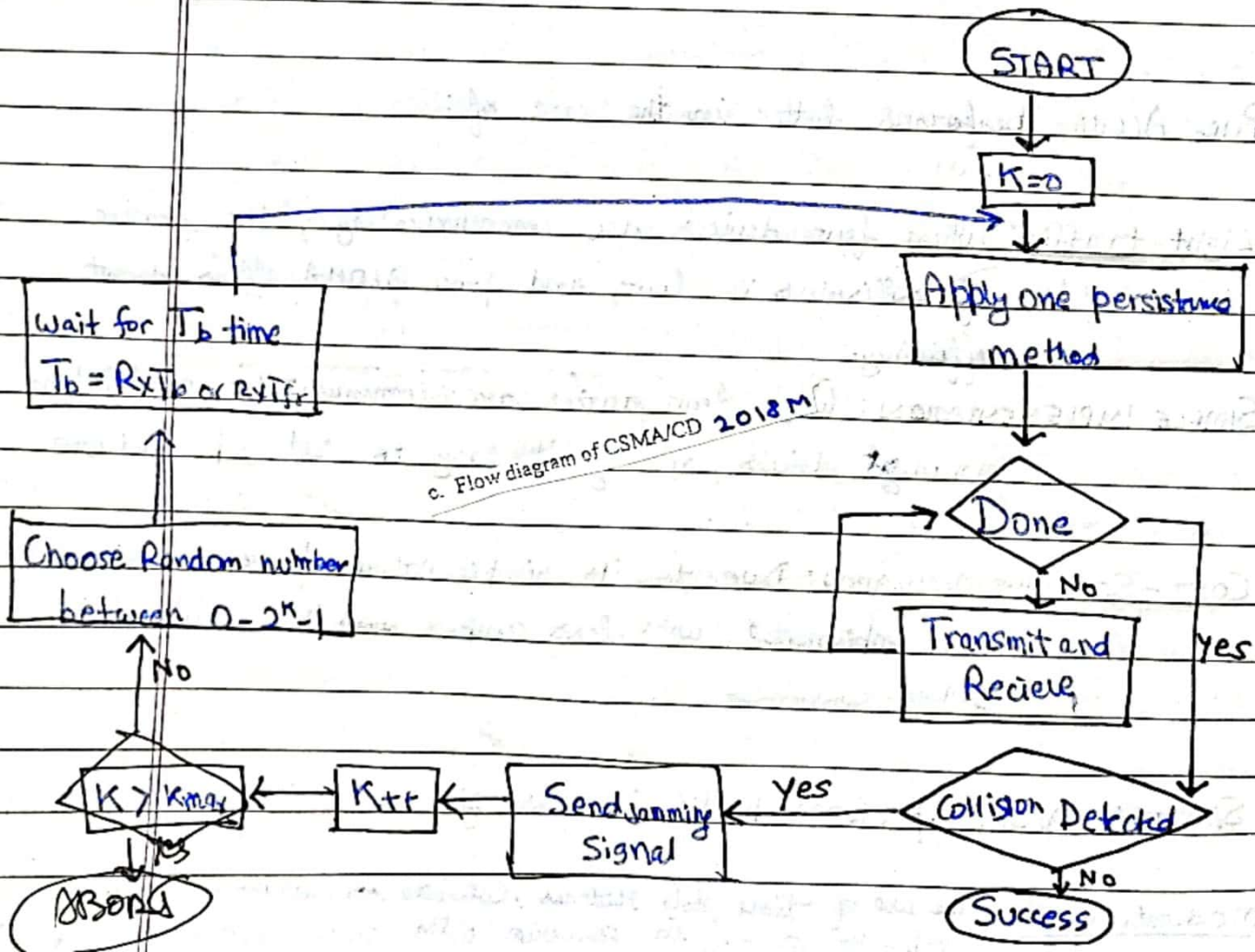
- **BALANCING SIMPLICITY AND performance:** Offers a good compromise between pure ALOHA's simplicity and CSMA's collision avoidance at the cost of some additional complexity.

- **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 $\geq 2 \times T_p$

$\Rightarrow T_t \geq 2 \times T_p$ —(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,

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

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

$L = 512 bytes$

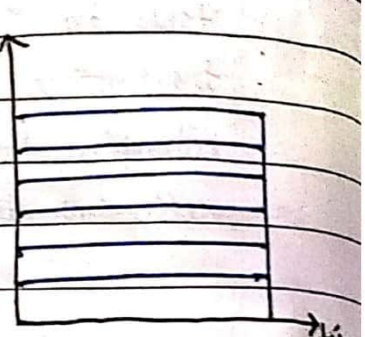
$\therefore T_t \geq 2 \times T_p \quad \therefore T_{tmin} = 2 \times T_p = \boxed{10^{-5} s}$?

Page No.
Date

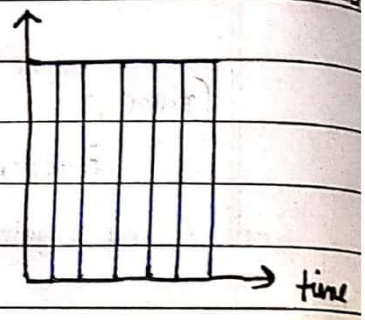
5. Write short note on (any two): (5x2 =10 marks)
a. Channel Access Methods 2018S

5. Write short note on (any two): (5x2 =10 marks)
a. Channel Access Methods 2018E

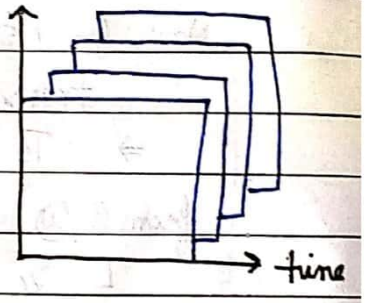
FDMA: Frequency division multiple access divides the spectrum of frequency into multiple channels, allowing users to communicate simultaneously without any interface.



TDMA: Time division multiple access divides the time domain into multiple slots, enabling users to share the same frequency by transmitting in turns.



CDMA: Code division multiple access assigns unique spreading codes to users, allowing them to transmit data simultaneously over the same frequency.



SDMA: Spacial division multiple access utilizes the spacial domain to create directional, non-overlapping communication channels, enabling multiple users to transmit data in the same frequency and time slots.

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

$T_p = 100ms$
$T_t = 10ms$

Analysis for 1 packet

T_t (packet) = 10mS

T_p (packet) = 100mS

T_p (ack) = 100 ms

∴ total time for one packet = $T_t(p) + T_p(packet) + T_p(ack)$ =

= (10 + 100 + 100) ms = 210ms

3. Similarly for all packets

packets = 10

total trips time = 210 ms / packet

∴ Total time = 10 × 210 ms

= 2100 milliseconds

= 2.1 seconds

[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 whom 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

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

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

Effiuency, $\eta = 0.5$

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

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

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

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? 2019S

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)

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

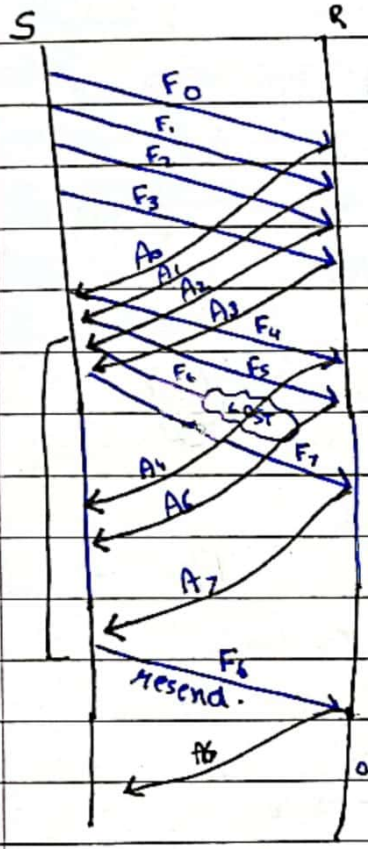
$= 0.2 * (1-0.5)^4$

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

ms is equal to $30 \times 10^{-3} \times 1 \times 10^{6} = 30{,}000$ bits. But in the stop-and-wait ARQ, only 800 bits can be transmitted in this time period. This inefficiency is due to the fact that in stop and wait ARQ, the transmitter waits, for an acknowledgment from the receiver before sending the next frame. The product of the bit rate and the delay that elapses before an action can take place is called the Delay-bandwidth product. The delay-bandwidth product helps in measuring the lost opportunity in terms of transmitted bits.

Important Point :

Stop and wait ARQ was used in IBM's Binary Synchronous Communications (Bisync) Protocol. It is also used in Xmodem, a popular file transfer protocol for modem.

9. Drawback of stop and wait protocol

Problem with stop and wait protocol is that it is very inefficient. At any one moment, only one frame is in transition. The sender will have to wait at least one round trip time before sending next. The waiting can be long for a slow network such as satellite link.

3.16.2. A Protocol Using Go Back n* *(Expected)*

1. Definition

In stop and wait protocol, it was assumed that the transmission time required for a frame to arrive at the receiver plus the transmission time for the acknowledgment to come back is negligible. But in some practical situations, this assumption is not correct. In the systems like satellite system, the round trip time can be as long as 500 ms (propagation delay). This protocol is also known as **Go-Back-n ARQ.** It is a method used to overcome the inefficiency of the stop and wait ARQ by allowing the transmitter to continue sending enough frames so that the channel is kept busy while the transmitter waits for acknowledgments. In this method, if one frame is damaged or lost, all frames are sent since the last frame acknowledged are retransmitted.

2. Principle of Go-Back-n ARQ

Let us consider figure 3.44 to understand the principle of GO-Back-n ARQ.

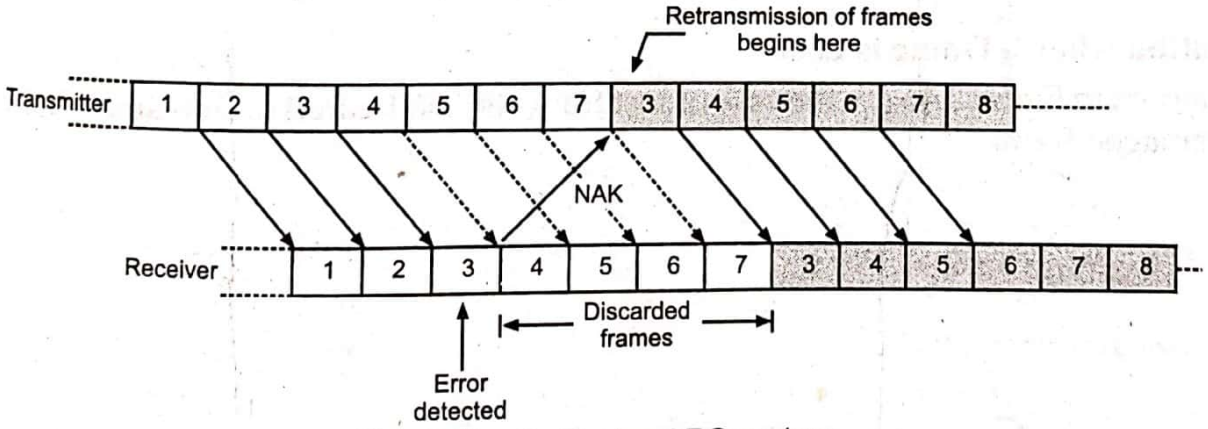


Fig. 3.44 Go Back n ARQ system

The major difference between this and the previous system is that the sender does not wait for ACK signal for the transmission of next frame. It transmits the frames continuously as long as it does not receive the *NAK* signal. NAK is the negative acknowledgment signal sent by the receiver to the transmitter. When the receiver detects an error in the third frame as shown in figure 3.44 the receiver sends a NAK signal back to sender. But this signal takers some time to reach the transmitter. By that time, the transmitter has transmitted frames upto frame 7. On the

* Describe with the help of suitable diagram the Go-back *n* ARQ error control scheme.
(U.P. Tech. Sem. Exam, 2006-07)(05 marks)

reception of the NAK signal, the transmitter will retransmit all the frames from 3 onwards. The receiver discard, all the frames it has received after 3 i.e. 3 to 7. It will then receive all the frames that are retransmitted by the transmitter.

3. Sources of error

The error can get introduced, if the transmitted frames are damaged or lost or if the acknowledgment is lost. Let us consider the operation of this protocol under these conditions.

4. Operation when the Frame is Lost

This condition is illustrated in figure 3.45. The second data frame is damaged, so the error is detected and receiver send NAK-2 signal back. On receiving this signal, the transmitter starts retransmission from frame 2. All the frames received after frame 2 are discarded by the receiver.

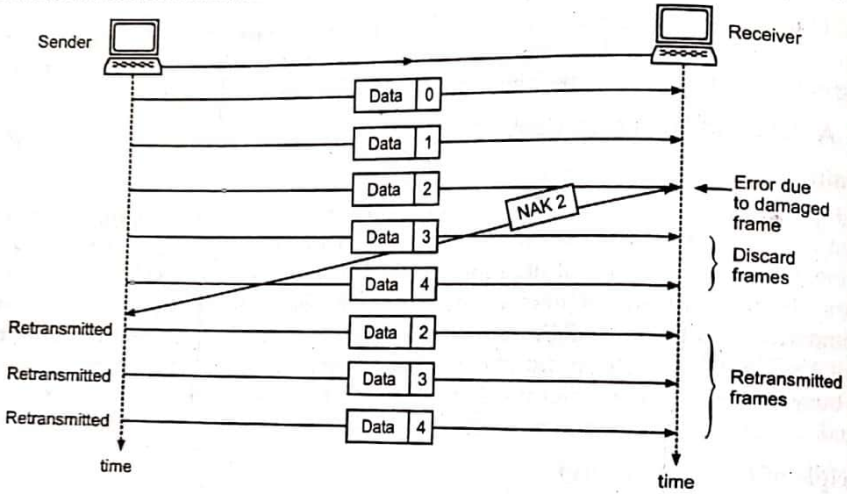


Fig. 3.45 Go-Back-n Damaged Data Frame

5. Operation when a Frame is Lost

As shown in figure 3.46 (*a*), the case of lost frame is also treated in the same manner as that of the damaged frame.

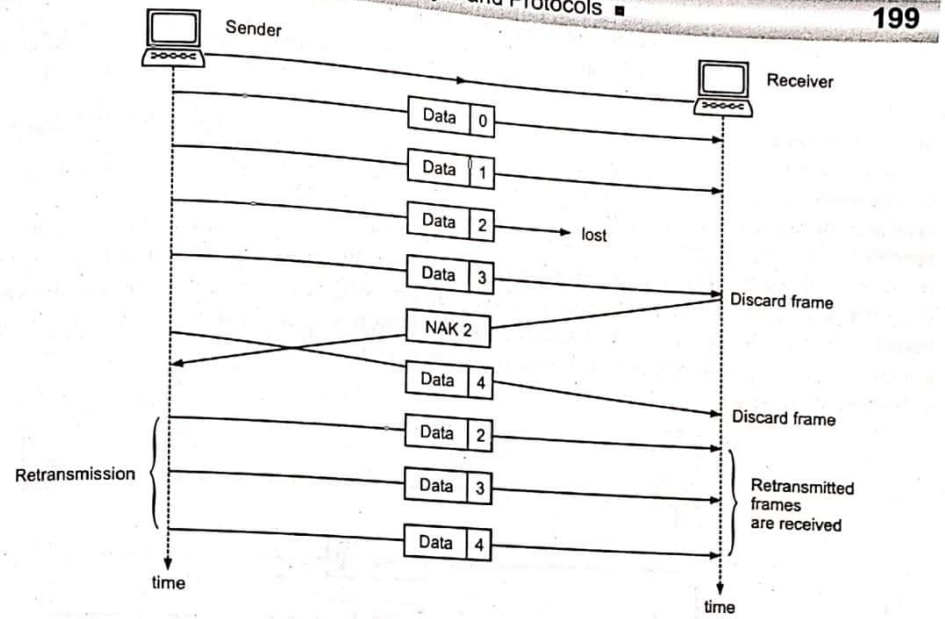


Fig. 3.46 (a) Go-Back-n, Lost Data Frame

The receiver, if it does not receive a particular data frame it sends a NAK to the transmitter and the transmitter retransmits all the frames sent since the last frame acknowledged.

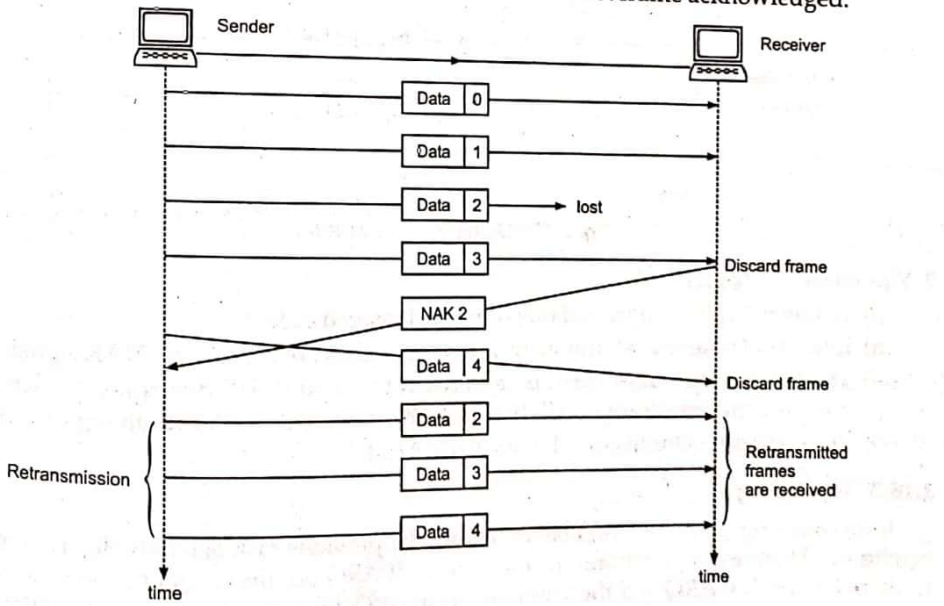


Fig. 3.46 (b) Go-Back-n, Lost Data Frame

6. Operation When the Acknowledgment is Lost

The figure 3.47 shows the condition for lost acknowledgment. In case of go-back-n method the transmitter does not expect an acknowledgment after every data frame. It cannot, use the absence of sequential ACK numbers to identify lost ACK or NAK frames, instead it uses a timer. The transmitter can send as many frames as the window allows before waiting for an acknowledgment. Once the limit has been reached or the transmitter has no more frames to transmit it must wait till the timer goes off and retransmit all the data frames again. The disadvantage of Go-back-n ARQ protocol is that in noisy channels, it has poor efficiency because of the need to retransmit the frame in error and all subsequent frames.

DO YOU KNOW?

In go-back-n ARQ, retransmission begins wtih the last unacknowledged frame even if subsequent frames have arrived corectly. Duplicate frames are discarded.

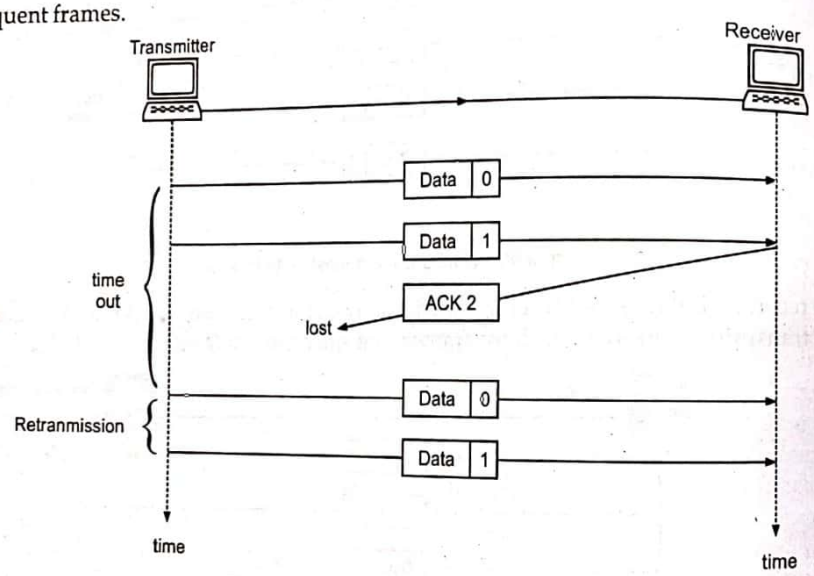


Fig. 3.47 Go-back-n, lost ACK frame

7. Drawbacks of Go back n

(*i*) It transmits all the frames if one frame is damaged or lost.
(*ii*) It transmits frames continuously as long as it does not receive the NAK signal.
(*iii*) The NAK signal takes some time to reach the sender. Till that time, the sender has already sent some frames. All those will be retransmitted after receiving the NAK.
(*iv*) The error can get introduced if the NAK is lost

3.16.3. Pipelining

In networking, a task is often begun before the previous task is complete. This is called pipelining. There is no pipelining in stop-and -wait ARQ but the concept of pipelining does apply to GO-Back-n ARQ and the selective repeat ARQ. Pipelining improves the efficiency of transmission.

3.16.4. Selective Repeat ARQ

(U.P. Tech, Sem. Exam; 2004-2005) (05 marks)

In this method, only the specified damaged or lost frame is retransmitted. A selective repeat system differs from the go-back-n method in the following ways :

(*i*) The receiver can do sorting of data frames and is also able to store frames received after a NAK has been sent until the damaged frame has been replaced.
(*ii*) The retransmitter must contain a searching mechanism that allows it to find and select only the requested frame for retransmission.
(*iii*) The window size in this method is less than or equal to $(n+1)/2$, whereas in case of go-back-n, it is n – 1.

The principle of operation of this protocol is illustrated in figure 3.48.

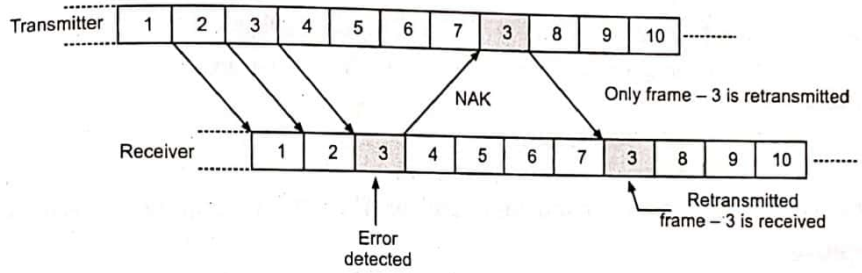


Fig. 3.48 Selective repeat ARQ system

In this system as well, the transmitter does not wait for the ACK signal for the transmission of the next code word. It transmits the code words continuously till it receives the *NAK* signal from the receiver. The receiver sends the *NAK* signal back to the transmitter as soon as it detects an error in the received frame. For example, the receiver detects an error in the third frame. By the time this *NAK* signal reaches the transmitter, it had transmitted the frame upto 7 as shown in figure 3.48. On reception of *NAK* signal, the transmitter will retransmit only the frame-3 and then continues with the sequence 8, 9... as shown in figure 3.48. The frames 4, 5, 6 and 7 received by the receiver are not discarded by the receiver. The receiver receives the retransmitted frames in between the regular frames. Therefore, the receiver will have to maintain the frames sequentially.

DO YOU KNOW?

In selective-repeat ARQ, only the unacknowledged frame is retransmitted.

Hence the selective repeat ARQ is the most efficient but the most complex protocol, of all the ARQ protocols.

Thus in selective repeat ARQ, only the frame which is damaged or lost is retransmitted by the transmitter. The lost ACK or NAK frames are treated in the same manner as the go-back-n method. When the transmitter reaches either the capacity of its window [(n + 1)/2] or the end of its transmission it sets a timer. If no acknowledgment arrives in the time allowed, all the frames that remain unacknowledged retransmitted. The disadvantage of this method is that because of the complexity of sorting and storage required by the receiver and the extra logic required by the transmitter to select frames for retransmission, the system becomes more expensive. The advantage of this system is that it gives the best throughput efficiency. This is due to the use of pipelining in selective repeat ARQ.

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

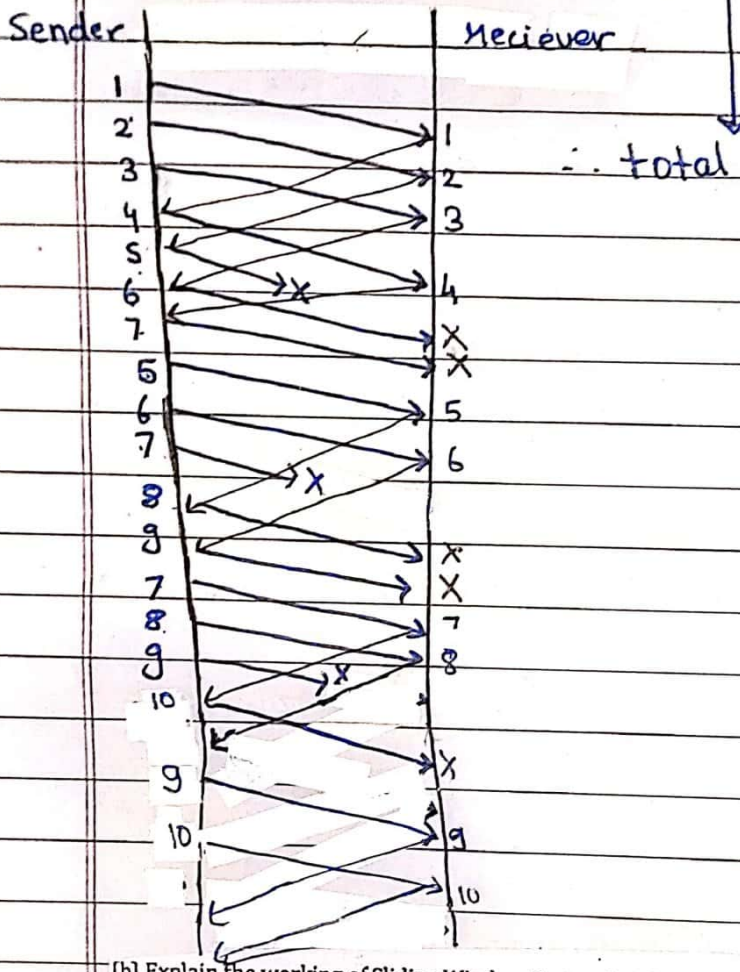
b. Let the system wants to send 10 packets using Go back N protocol with sliding window size (N) as 3. What are the total no of transmissions if every 5th packet is lost. 2018E (10 marks)

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 = 18

[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 $T_p = 2 \times 2 = 4$ 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 $\log_2(201) + 1 = 8$ bits.

Page No.
Date

Q.7 Write short notes on the following

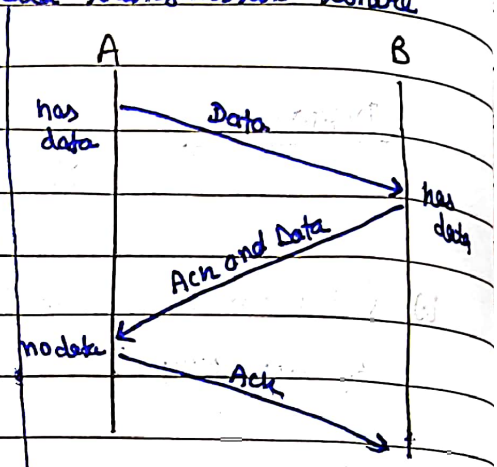
a) Piggy back and Sliding Window Syndrom. 2019S

PIGGY BACK

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

Piggybacking is a technique used in data transmission where acknowledgements are attached to outgoing data frames, optimizing Bandwidth by allowing bidirectional communication without wasting resource 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:

This problem degrades TCP performance when the sender transmit data in large blocks but an interactive application on the reciever side reads one byte at a time.

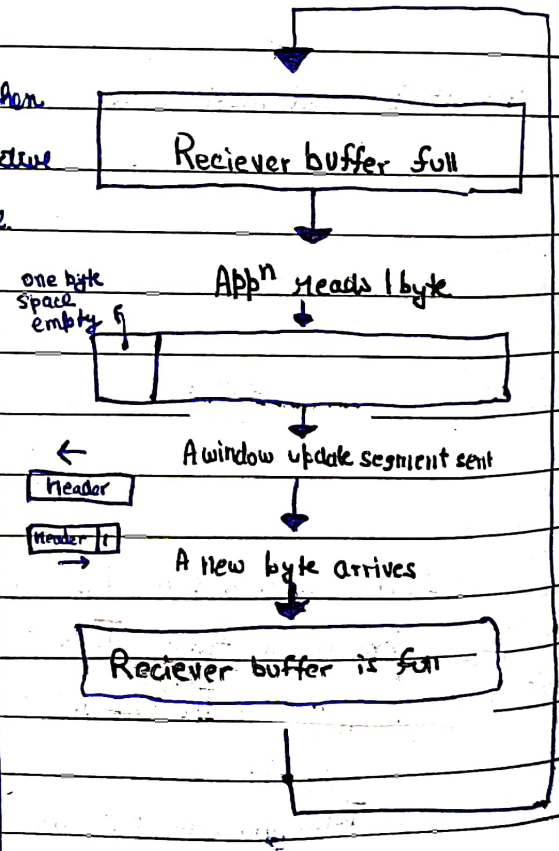
i.) Initially the reciever's buffer is full so it sends window size 0 to block the sender.

ii.) but the app reads one byte from the buffer. So, one byte space becomes empty.

iii.) The recieving TCP sends a window update to the sender informing that it can send 1 byte.

iv.) The sender send 1-new byte

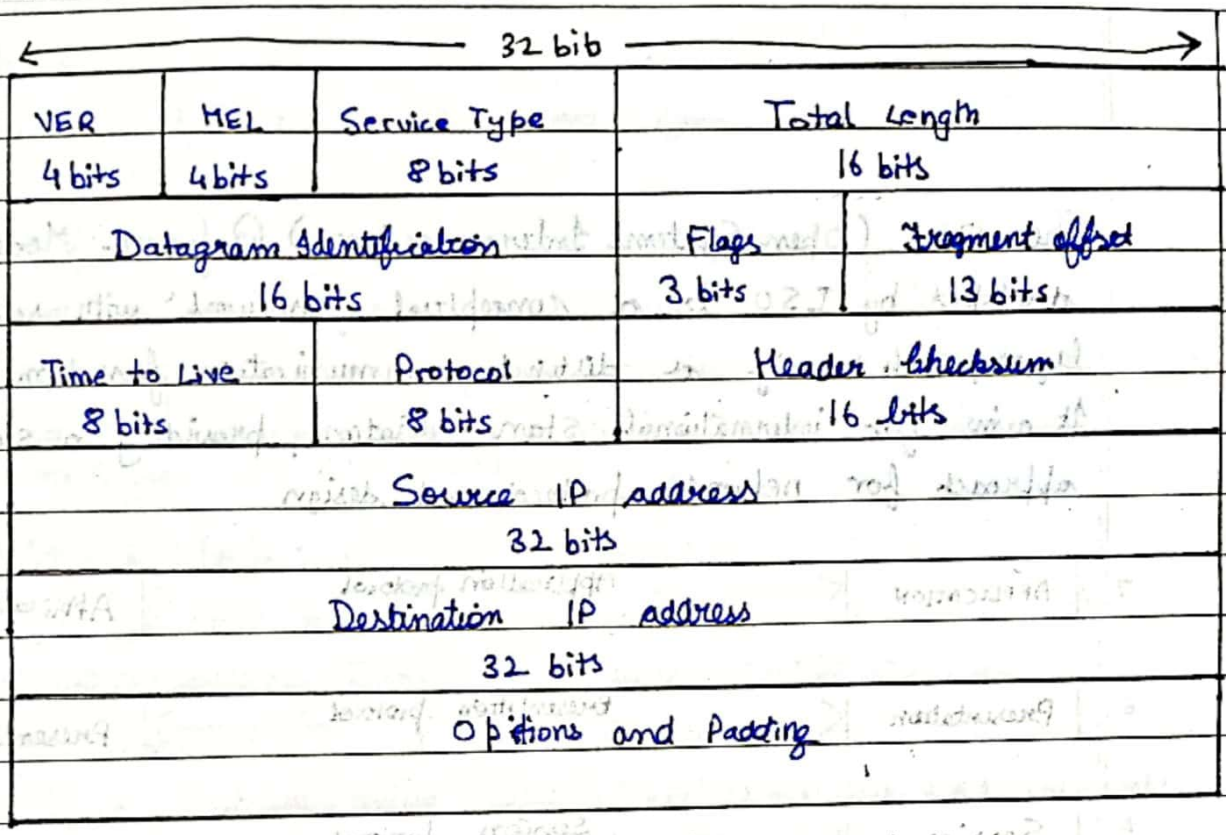
v) The buffer is full again and window size is 0.
This behaviour can continue forever.



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. Eg) 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. Eg) Timestamp, Record and record route.

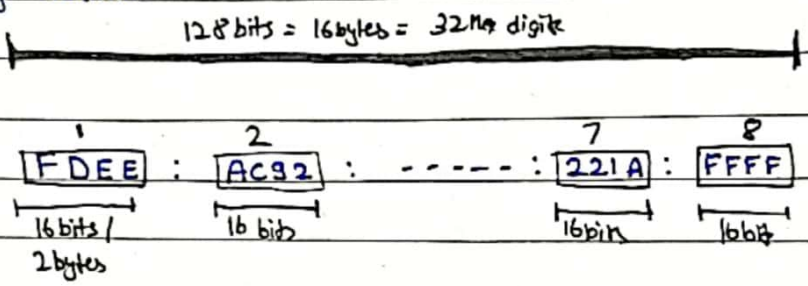
Q4(a) Answer IPv4 header questions 2023E [2][CO3]

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:

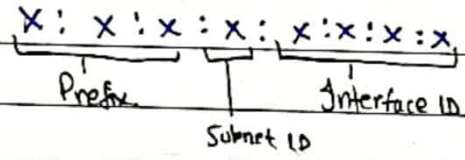


IP addresses can be shortened / abbreviated by omitting leading zeros within each group and collapsing consecutive group of zeros into double colon (::). (only once)

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 seperate from base header which are inserted when needed. Speeds up Routing.

Page No.
Date

→ 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 don't 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.

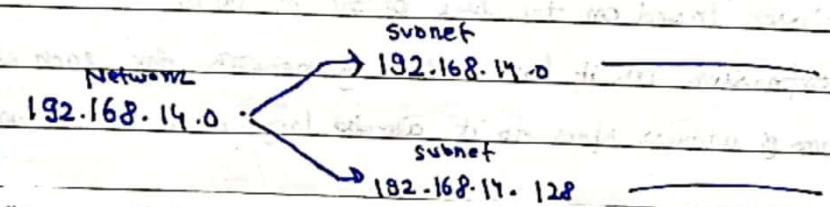
Page No. | Date

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? 2023E [2][CO3]

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

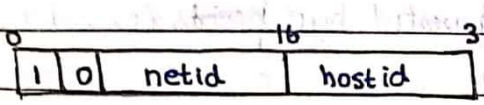
GATE 2015

	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 = $2^6 = 64$

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. 20185

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

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.

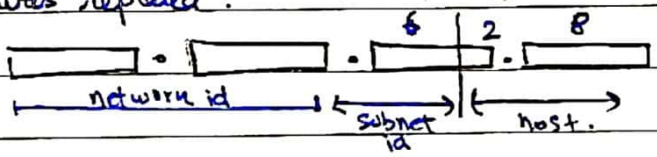
Page No.
Date

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]

Given IP address : 00001010.00010100.00011110.00101000
Subnet Mask : 11111111.11111111.11111111.11000000

∴ Net address = IP (AND) MASK = (10.20.30.0)

Broadcast address = 10.20.30.$(00111111)_{10}$ = (10.20.30.63)

= IP OR !(MASK)

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

BASE HEADER

VER	PRI	FLOW LABEL	
PAYLOAD LENGTH		NEXT HEADER	HOP LIMIT
SOURCE ADDRESS			
DESTINATION ADDRESS			
Payload Extension Header + Data Packet from the upper layer			

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.

(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.

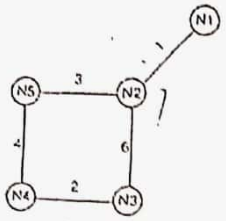
3.) Updating: When router receives a distance vector table from neighbour, it checks for
→ new destination and adds them in its table.
→ Shorter paths and updates their distance.

4.) This process continues till the network stabilizes.

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



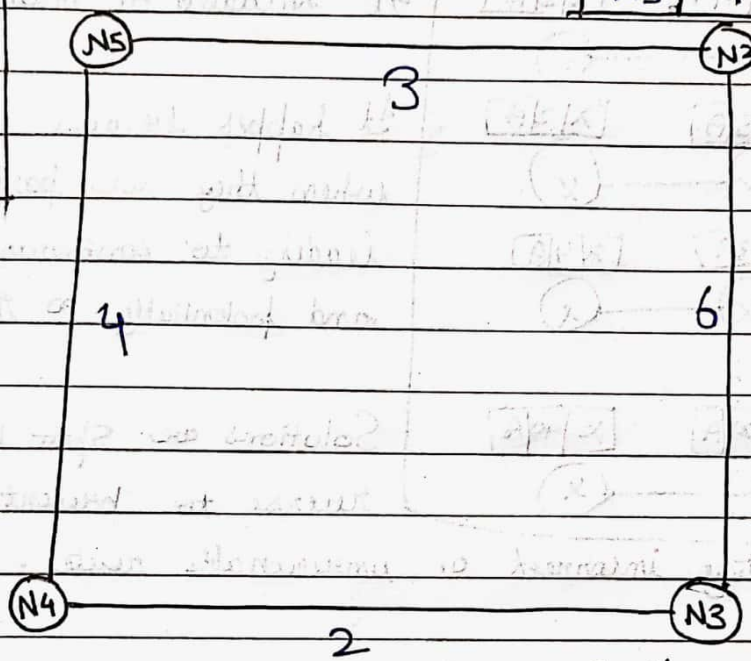
Page No.
Date

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_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	—



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_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_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

c) What is count to infinity in distance vector routing? How does split horizon prevents routing loops in distance vector routing, Explain. [4][CO3] 2023E

[b] What is count to infinity problem? How it can be solved? 2018S

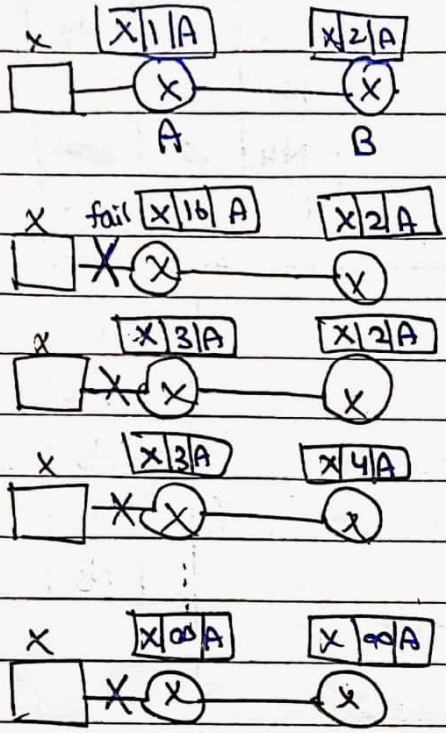
[b] What is count to infinity problem? How it can be solved. What are its limitations?
2019S

B) Explain distance vector algorithm with suitable example. 2019S

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.

Q.3

[a] Describe the link state routing algorithm with suitable example in detail. 2018S

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:)

Page No.
Date

Q.3

[a] Compare Link State and Distance vector routing algorithms and with the indicated link cost, use Dijkstra's shortest path algorithm to compare the shortest path from x to all nodes. 2019 S

Page No.
Date

Q.3 a) A packet has arrived in which the offset value is 100, the value of HLEN is 5, and the value of the total length field is 100. What are the numbers of the first byte and the last byte? 2023 M [6] [CO3]

First byte = offset × 8 = 800

Header Length = HLEN × 4 = 20 Bytes.

Total data byte = total length − header length = 100 − 20

= 80

∴ Last byte = 800 + 80 − 1 = 879

2. a. A user downloads the file of 4.5 MB from the website. The files routes through two routers R1 with maximum transmission unit (MTU) as 2.5 MB and router R2 with MTU as 1500 KB before finally reaching to the client. Show the fragmentation at each router and calculate the speed at which the file is downloaded by the client. Consider an instance of TCP's Additive Increase Multiplicative Decrease (AIMD) algorithm where the window size at the start of the slow start phase is 2 MSS and the threshold at the start of the first transmission is 8 MSS. Assume that a timeout occurs during the fifth transmission. Find the congestion window size at the end of the tenth transmission. (Assume 1 MB = 1000KB and IPv4 Header Length = 20KB). 2018 E

P.T.O.

Page No.
Date

b) If a datagram of size 5000 bytes is transmitted over a network with an MTU of 1200 bytes, and the header length is 20 Bytes. What is the offset of the first, second and third fragments? 2023E [3][CO4]

Datagram size = 5000 bytes
MTU = 1200 bytes
HLEN = 20 bytes

Offset = (Fragment No - 1) * (MTU - HLEN)

1. First segment,
   Offset 1 = (1-1) * (1200 - 20) = 0 bytes

2. Second segment,
   Offset 2 = (2-1) * (1200 - 20) = 1180 bytes

3. Third segment,
   Offset 3 = (3-1) * (1200 - 20) = 2360 bytes.

Page No.
Date

Page No.
Date

b) If a datagram of size 5000 bytes is transmitted over a network with an MTU of 1200 bytes, and the header length is 20 Bytes. What is the offset of the first, second and third fragments? 2023E [3][CO4]

Datagram size = 5000 bytes
MTU = 1200 bytes
HLEN = 20 bytes

Offset = (Fragment No - 1) * (MTU - HLEN)

1. First segment,
   Offset 1 = (1-1) * (1200 - 20) = 0 bytes

2. Second segment,
   Offset 2 = (2-1) * (1200 - 20) = 1180 bytes

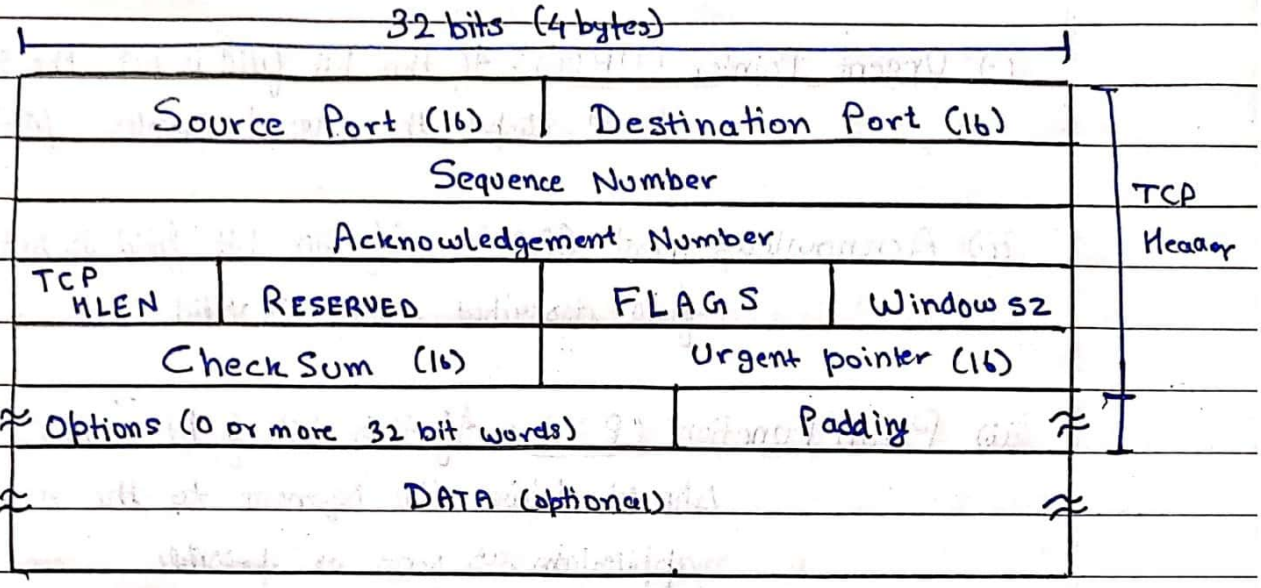
3. Third segment,
   Offset 3 = (3-1) * (1200 - 20) = 2360 bytes.

Q.2
[a] Explain in detail TCP header format. 2019S

[b] Explain TCP header format in detail. 2018S

Page No.
Date

Q.5 ·
A) Explain in detail TCP header format. 2019S



TCP Header Format.

Every segment begins with a 20 byte fixed format header.

1. Source Port (16 bits): Identifies the application the TCP segment originated from on the sending host.

2. Destination Port (16 bits): Identifies the destination application on the receiving host.

3. Sequence Number (32 bits): Identifies the position of the first data byte in the TCP connection's byte stream.

4. Acknowledgement Number (32 bits): Identifies the next data byte the sender expects from the receiver.

5. HLEN (4 bits): Specifies the total TCP header length in 32-bit words.

6. REserved (6 bits): Currently unused, reserved for future use.

7. Control bits / Flags (6 bits):

P.T.O.

Page No.
Date

i.) Urgent Pointer (URG): If this bit field is set, the receiving TCP should interpet the urgent pointer field.

ii.) Acknowledgement (ACK): If this bit field is set, the ack field described earlier is valid.

iii.) Push Function (PSH): If this bit field is set, the reciver should deliver this segment to the receiving application as soon as possible.

iv.) Reset the Connection (RST): If this bit is present, it signals the receiver that the sender is a right connection and all queued data and allocated buffers for the connection can be freely operated.

v.) Synthesis (SYN): When present, this bit field signifies that sender is attempting to achieve the sequence numbers.

vi.) No more Data from Sender (FIN): signifies end of stream for the current TCP connection.

8. WINDOW (16 bits): Specifies the amount of data the receiver is willing to accept.

9. Checksum (16 bits): Used to verify the integrity of the TCP header and data.

10. Urgent Pointer (16 bits): Indicates the last byte of urgent data in the segment.

12. Padding: Ensures the TCP header ends on a 32 bit boundary

11. Options (variable): Provide additional functionality like max segment size

Page No.
Date

(b) Why TCP is slower but more reliable than UDP Protocol in Transport Layer, Explain. 2023E [2][CO4]

TCP is Reliable as it establishes a connection between sender and recievers, like a handshake. It checks for errors and guarantees delivery by retransmitting lost packets. This back and forth adds some overhead slowing things down.

UDP is faster as it is connectionless. It just fires data packets off without any guarantees. This is quicker, but there is no check-up on delivery or errors.

Q5. a) In TCP, the initial RTT is 20 ms. The acknowledgements for the first four segments are received in time 25 ms, 18 ms, 23 ms, and 21 ms. Using the basic algorithm, find the timeout timer value for the first five segments. Use $\alpha = 0.5$. 2023E [3][CO6]

RTT → Round Trip Time.
D → deviation

$RRT = 20ms$
$I_D = 0$
$\alpha = 0.5$

Segment - 1

$T_o = 2 \times IRRT = 40ms$

Segment - 2

$T_o = 2 \times NRRT$
$= 2 \times (\alpha IRRT + (1-\alpha) ARRT_1)$
$= 2 \times \frac{1}{2} (20 + 25)$
$= 45ms$ (22.5)

Segment - 3

$T_o = 2 \times \frac{1}{2} (22.5 + 18)$
$= 40.5 ms$

segment 4

$T_o = 2 \times \frac{1}{2} (20.25 + 23) = 2 \times 21.625$

$T_o = 43.25ms$

Segment - 5

$T_o = 2 \times \frac{1}{2} (21.625 + 21)$

$= 42.625 ms$

Page No.
Date

User Datagram Protocol

a) Draw UDP header and explain each field. 2023E [2][CO2]

SOURCE ADDRESS		
DESTINATION ADDRESS		
Zero	Protocol	UDP length

UDP Pseudo Header

The purpose of using a pseudo-header is to verify that the UDP packet has reached its correct destination. Its fields include :-

1. Source Address : It contains the IP address of the sending machine. (32 bits)

2. Destination Address : It contains the IP address of the destination machine. (32 bits)

3. Zero : It is set to zero.

4. Protocol : This field specifies the protocol being used (UDP here)

5. UDP Length : Specifies length of UDP packet, including header and data.

b. Explain the block diagram of TCP. How is TCP different from UDP? (10 marks)
2018S

6.15.3. Performance Comparison of UDP and TCP

S.No.	Characteristic/ Description	UDP	TCP
1.	General Description	Simple, high-speed low-functionality *wrapper* that interfaces applications to the network layer and does little else.	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.
2.	Protocol Connection Setup	Connectionless data is sent without setup.	Connection-oriented; connection must be established prior to transmission.
3.	Data Interface to Application	Message-based data is sent in discrete packages by the application.	Stream-based data is sent by the application with no particular structure.
4.	Reliability and Acknowledgements	Unreliable, best-effort delivery without acknowledgements.	Reliable delivery of messages; all data is acknowledged.
5.	Retransmissions	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.
6.	Features Provided to Manage Flow of Data	None.	Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms.
7.	Overhead	Very low.	Low, but higher than UDP.
8.	Transmission Speed	Very high.	High, but not as high as UDP.
9.	Data Quantity Suitability	Small to moderate amounts of data (up to a few hundred bytes).	Small to very large amounts of data (up to gigabytes).
10.	Types of Applications that Use the Protocol	Applications where data delivery speed matters more than completeness, where small amounts of data are sent; or where multicast/broadcast are used.	Most protocols and applications sending data that must be received reliably, including must file and message transfer protocols.
11.	Well-known Applications and Protocols	Multimedia applications, DNS BOOTP, DHCP, TFTP, SNMP, RIP, NFS (early versions).	FTP, Telnet, SMTP, DNS, HTTP, POP, NNTP, IMAP, BGP, IRC, NFS (later versions).

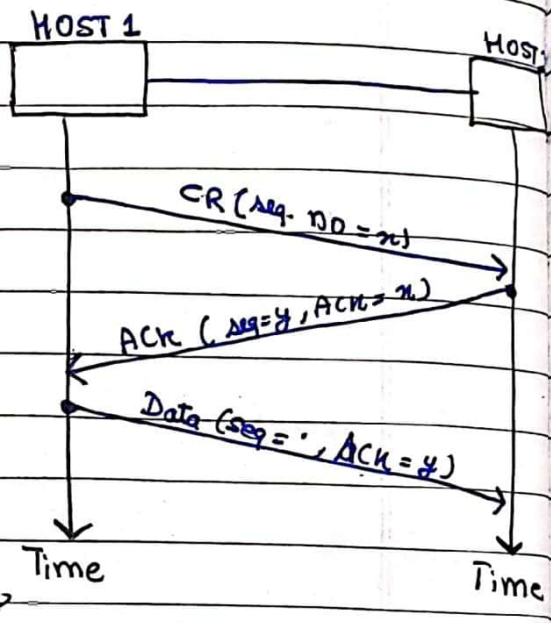
UNIT-4: Transport Layer

Page No.
Date

B) Explain connection establishment and release using 3-way handshaking in transport layer 2019 S

[d] Three way hand shaking of connection establishment. 2019 S

A three way handshake is a technique which solves delayed duplicate packet problem.



CONNECTION ESTABLISHMENT

1. Client sends SYN packet to server to initiate connection.
2. Server responds with SYN-ACK packet, acknowledging clients request.
3. Client sends ACK packet to confirms server's response and establish connection.

CONNECTION RELEASE

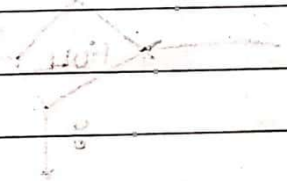
1. Each client or server sends FIN packet to initiate release
2. Recieving party acknowledges with ACK packet
3. Recieving party sends FIN packet back to agree on connection termination.

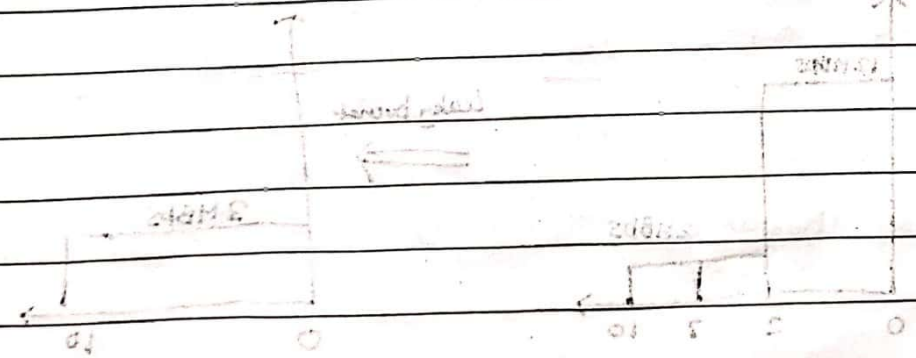
Page No.
Date

b) Write a short note (Any two) [4][CO5][CO6]

ii) Remote Procedure Call (RPC) 20236

Q5



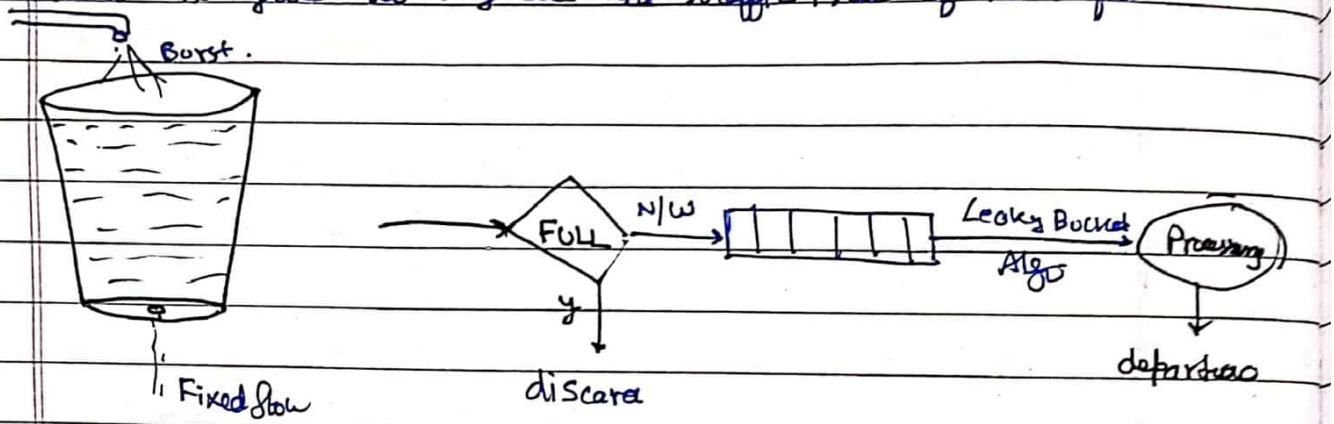


Page No.
Date

b) Explain congestion control algorithms with the help of a diagram. [3][CO3] 2023E

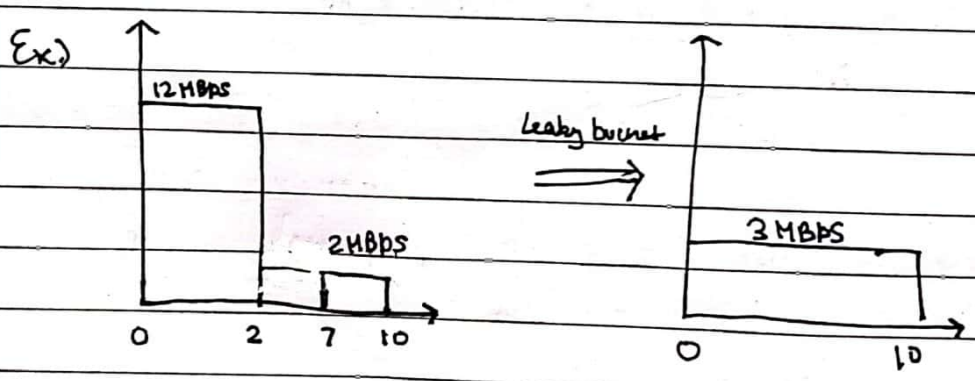
1. Leaky Bucket [c] Leaky Bucket Algorithm 2018S

In the leaky bucket algo, bursty flow of data is smooth out under fix flow to regulate the traffic / rate of data flow.



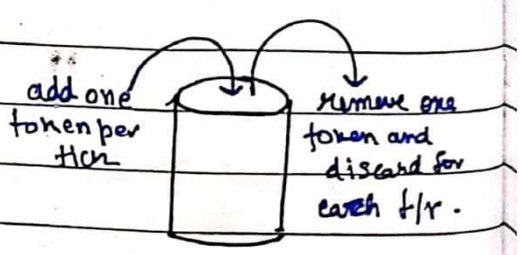
It operates by using a virtual bucket with a fixed capacity. Packets are added to the bucket as they arrive, and the bucket size leaks out the packets at a fixed rate. If the bucket becomes full and a new packet arrives, the new packet is either delayed or dropped, depending on the implementation.

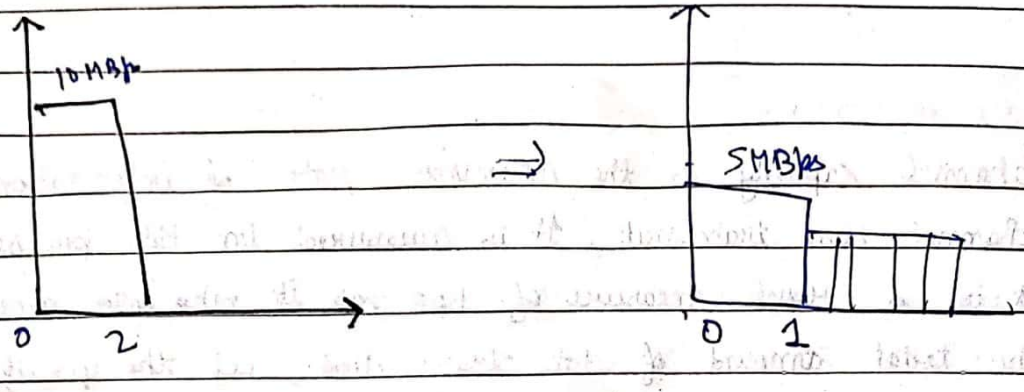
Ex)



2. Token Bucket

The token bucket is used to regulate the rate at which data is sent to a network





b. For a host machine that uses the token bucket algorithm for congestion control, the token bucket has a capacity of 1 megabyte and the maximum output rate is 20 megabytes per second. Tokens arrive at a rate to sustain output at a rate of 10 megabytes per second. The token bucket is currently full and the machine needs to send 12 megabytes of data. What is the minimum time required to transmit the data. **(10 marks)**

GATE 2016 2018 E

Rate at which it is emptying = (20 − 10) MBPS
= 10 MBPS

∴ Time taken to empty token bucket of 1MB = $\frac{1}{10}$ = 0.1 sec — (1)

Data sent in this time (0.1s) = 0.1 * 20 = 2 MB

∴ Data left to send = (12 − 2) MB = 10 MB

Time to send 10MB = $\frac{10}{10}$ = 1 sec — (2)

∴ Total time = 0.1 + 1 = **1.1 seconds**

Page No.
Date

Q.6.

[a] What is channel capacity? Find the Channel Capacity for a 3khz bandwidth and SNR of 3db. 2019S

Channel capacity is the maximum rate of information that a channel can transmit. It is measured in bits per second (bps). It is a rough measure of bps as it takes into account only the total amount of data transmitted, not the quality of the communication.

∴ Bandwidth of channel, B = 3000Hz
Signal to Noise Ratio, SNR_{db} = 3dB

∵ $SNR_{db} = 10 \log_{10}(SNR)$

⇒ $3 = 10 \log_{10}(SNR)$

⇒ $SNR = \log\left(\frac{3}{10}\right)$ ⇒ SNR = 1.995

∴ Channel Capacity, $\boxed{C = B \log_2(1 + SNR)}$

∴ $C = 3000 (\log_2(1 + 1.995))$

$= 3000 \log_2(2.995)$

$\boxed{C = 4752 \text{ bits/s}}$

[b] Firewall.. 2018S

Firewalls are an essential security mechanism used to protect computer networks from unauthorized access and malicious threats. A firewall acts as an electronic drawbridge, forcing all traffic to and from the corporate network to flow through it.

It consists of two key components:

Page No.
Date

1. Packet filtering routers: These routers inspect each incoming and outgoing packet and apply predefined rules to decide whether to allow or block the packet based on criteria like src / dest IP or port.

2. Application Gateway: This examines packets at the application layer looking at the parameters like size, message headers, content to determine if the traffic should be permitted or discarded. This provides a deeper level of security compared to just packet filtering.

These help protect against dangers like data leaks, virus/worms infections, and unauthorised access attempts.

d. DHCP vs BOOTP 2018

BOOTSTRAP PROTOCOL (BOOTP)	DYNAMIC HOST CONFIG PROTOCOL (DHCP)
It does not provide temp IP addressing	It provides temp IP addressing for a limited amount of time.
Does not support DHCP clients	Supports BOOTP clients.
Manual config. takes place	Auto-config takes place
Does not support mobile machines	Supports mobile machines.
It can have errors due to manual configuration.	Errors do not occur mostly due to auto configuration.

4. a. Explain DHCP protocol? What is the difference between multicast and broadcast? Suppose there are n stations in a slotted LAN. Each station attempts to transmit with a probability 'p' in each time slot. What is the probability that only one station transmits in a given slot. 2018E

Page No.
Date

Dynamic Host Configuration Protocol (DHCP) is a network protocol used to automatically / dynamically assign IP addresses and other network configuration parameters to devices connecting on a network. When a new device connects to a network, it can request an IP address and other settings from a DHCP server, rather than having to manually configure them.

The main steps in DHCP process are :-

1. Discovery : The client device broadcasts a DHCP discover message to find the available DHCP servers on the network.

2. Offer : One or more DHCP servers respond with a DHCP offer message, proposing an IP address and other config. params.

3. Request : The client device selects one of the offers and sends a DHCP request message to the corresponding DHCP server.

4. Acknowledgement : The DHCP server confirms the request and sends a DHCP ack. message back to the client, providing the allocated IP address and other n/w settings.

∴ It reduces IP conflicts and is widely used in home, office etc to provide "plug and play" network connectivity for devices.

P.T.O.

BROAD CAST	MULTICAST
The packet is transmitted to all the hosts connected to the network.	The packet is transmitted only to intended recipients of the network
transmission is one-to-all	transmission is one-to-many.
Broadcasting does not require any group management.	It requires grp mgmt. to define the group of hosts / stations which will receive packets.
Bandwidth is wasted	Bandwidth is utilized effectively.
Unnecessary huge amount of traffic	traffic is under control.

Let Stations be $S_1, S_2 \dots S_n$

∴ prob that only one station transmits =

S_1 transmits and no one +

S_2 transmits and no one +

⋮

S_n

$= p(1-p)^{n-1} + p(1-p)^{n-1} + p(1-p)^{n-1} + \dots$

$= \boxed{np(1-p)^{n-1}}$

P.T.O.

d. ICMP 2018 E

13.	ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional.	ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required.
14.	Header includes options.	All optional data is moved to IPv6 extension headers.

5.25 INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

The IP provides unreliable and connectionless datagram delivery. It was designed this way to make efficient use of network resources. IP is a best-effort delivery service that delivers a datagram from its original source to its final destination. However, it has two deficiencies : lack of error control and lack of assistance mechanisms.

The Internet Control Message Protocol (ICMP) reports errors and sends control messages on behalf of IP. ICMP does not attempt to make IP a reliable protocol. It simply attempts to report errors and provide feedback on specific conditions. ICMP messages are carried as IP packets and are therefore unreliable. IP also lacks a mechanism for host and management queries. A host sometimes needs to determine if a router host is alive. And sometimes a network manager needs information from another host or router. The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. It is a companion to the IP. ICMP itself is a network layer protocol. However, its messages are not passed directly to the data link layer as would be expected. Instead, the messages are first encapsulated inside IP datagrams before going to the lower layer. (The value of the protocol field in the IP datagram is 1 to indicate that the IP data are an ICMP message.) This has been shown in figure 5.63.

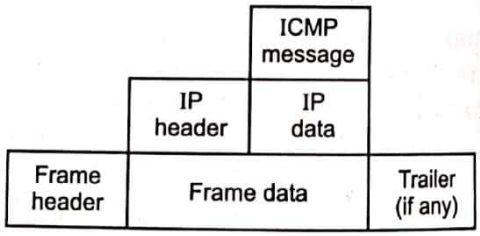


Fig. 5.63 ICMP encapsulation

The ping command uses ICMF as a probe to test whether a station is reachable. Ping packages an ICMP echo request message in a datagram and sends it to a selected destination. The user chooses the destination by specifying its IP address or name on the command line in a form such as :

ping 100.50.25.1

When the destination receives the echo request messages, it responds by sending an ICMP echo reply message. If a reply is not returned within a set time, ping resends the echo request several more times. If no reply arrives, ping indicates that the destination is unreachable. Another utility that uses ICMP is trace route, which provides a list of all the routers along the path to a specified destination.

5.25.1. Types of Messages

ICMP messages are broadly divided into following two categories as under:

(*i*) Error reporting messages

(*ii*) Query messages.

Error Reporting Messages

One of the important responsibilities of ICMP is error reporting. IP is an unreliable protocol.

So error checking and control are not concerns of IP. Hence, ICMP was designed. But ICMP does not correct the errors. It simply reports them and error correction is left to the higher level protocols. ICMP always sends the error reporting messages back to the original source. ICMP can handle five types of errors. Figure 5.64 shows different types of error reporting messages.

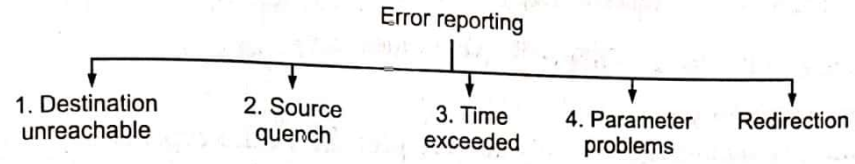


Fig. 5.64 Error reporting messages

1. Destination reachable

When a router cannot forward or deliver an IP packet, it sends a destination unreachable ICMP message back to the original source.

2. Source Quench Message

A host or router uses source quench messages to report congestion to the original source and to request it to reduce its current rate of packet transmission. There is no flow control or congestion control mechanism in IP. So, the source quench message is ICMP which is designed to add a kind of flow control and congestion control to IP.

This message serves following two purposes :

(*i*) It tells the source that the datagram has been discarded, and

(*ii*) It gives a warning to the source that the source should slow down (quench) because congestion has taken place somewhere.

3. Time Exceeded Message

This message is generated in two cases :

(*i*) If a router receives a datagram with a 0 in the TTL field then it discards that datagram and send a time exceeded message back to the original source.

(*ii*) If all the fragments which make up a message do not arrive at the destination host within a certain time limit then exceeded message is sent back.

4. Parameter Problem Message

There should not be any ambiguity in the header part of the datagram. If a router or destination host finds any such ambiguity or missing value in any field of the datagram then it discards that datagram and sends the parameter problem message back to the source.

5. Redirection Message

If a router or host wants to send a packet to another network then it should know the IP address of the next router. The routers and hosts must have a routing table to find the address of the next router and the routing table has to be updated constantly. For such an updating, the ICMP sends a redirection message back to its host.

5.25.2. Query

The ICMP can diagnose some of the network problems and such a diagnosis is accomplished through the query messages. The query messages is a group of four different pairs of messages as shown in figure 5.65.

UNIT-5 : Presentation Layer

Page No.
Date

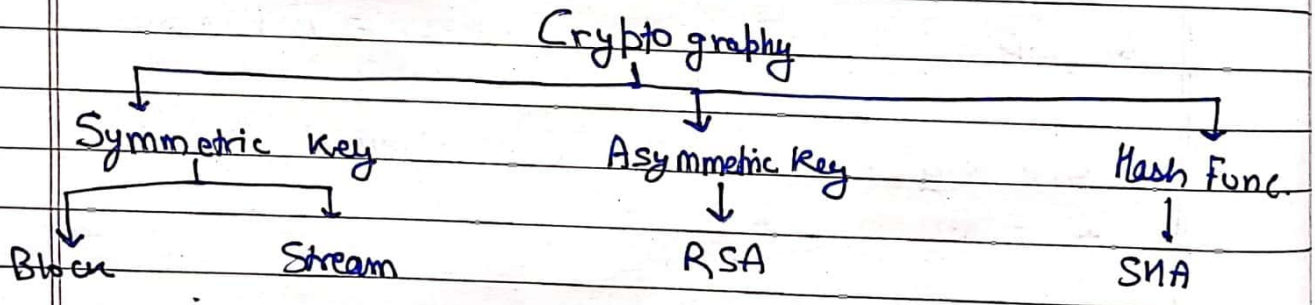
Q.4
[a] What is cryptography? Discuss various methods of cryptography with example and also explain the working of Data Encryption Standards (DES).

Q.4 20195 1
[a] What is cryptography? Discuss various methods of cryptography with example.
20185

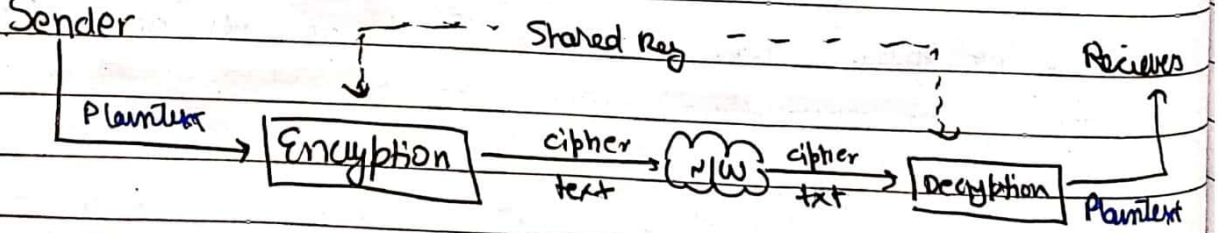
Cryptography is the study of various ways to disguise messages in order to avoid interception from an unauthorized interceptor.

The terms encipher and encrypt correspond to the message transformations performed at the transmitter in order to disguise the message. The terms decipher and decrypt correspond to the inverse t/r performed at the reciever to get recover the original message back.

Methods :

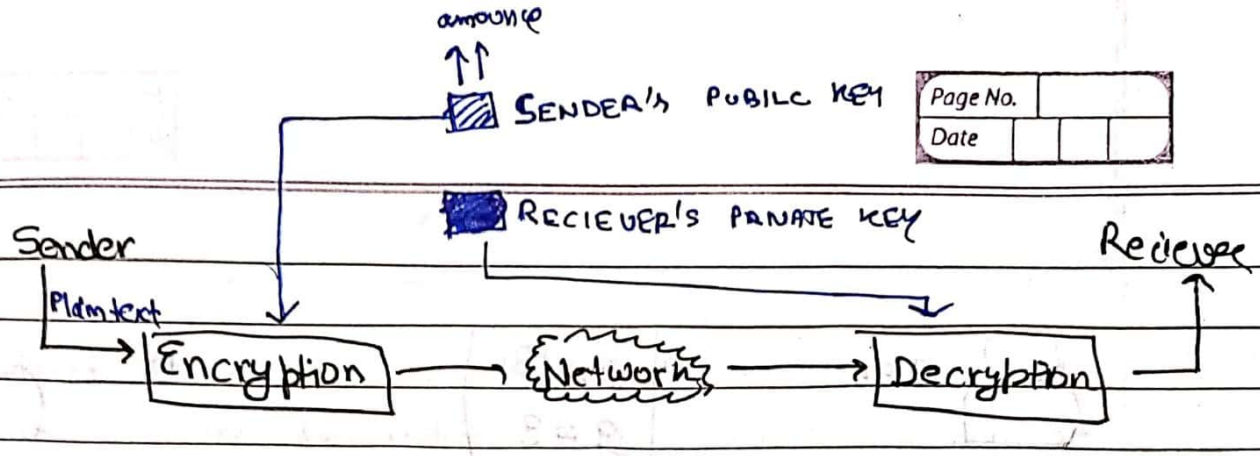


In Symmetric key, the same shared key is used by sender and reciever. The encryption algo uses a combination of addition and multiplication while the decryption algo uses division and subtraction.



In asymmetric key cryptography, there are two keys :
i) Public Key : announced to public
ii) Private Key : with reciever

Eg) RSA



b. The bank uses RSA algorithm at the presentation layer to encrypt the message M = 88 with its public key, e = 7. If the two prime no. used for encryption are p=17 and q=11, show the encrypted cipher and decrypted message at the receiver end. What is the remainder when $32^{32^{32}}$ is divided by 9? **(10 marks)**

Given, $p = 17$, $q = 11$ | $M = 88$, $e = 7$

$\therefore n = pq = 17 \times 11 = 187$

$\Rightarrow n = 187$

$\therefore$ Public Key : $\{e, n\} = \{7, 187\}$

Private Key : $\{d, n\} = \{23, 187\}$

to find d

$\phi(n) = (p-1)(q-1) = 10 \times 16$

$\Rightarrow \phi(n) = 160$

$\because d \cdot e = 1 \bmod (\phi(n))$

$7e = 1 \bmod 160$

$\Rightarrow d = 23$

Encryption (Using public key)

encrypted msg, $C = M^e \bmod (n)$

$\Rightarrow C = 88^7 \bmod 187$

$C = 11$

$\therefore$ encrypted cipher = 11

Decryption (using private key)

decrypted msg, $M = C^d \bmod (n)$

$\Rightarrow M = 11^{23} \bmod (187)$

$M = 88$

$\therefore$ decrypted cipher = 88

Now

$32^{32^{32}} \bmod 9 = (27+5)^{32^{32}} \bmod 9 = 5^{32^{32}} \bmod 9$

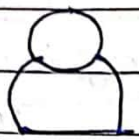
$\Rightarrow$

$\Rightarrow 32^{32} = 6n + x \Rightarrow 2^{160} = 6n + x \Rightarrow x = 4$

$\therefore 5^4 \bmod 9 = \boxed{4}$

Page No.
Date

A) Suppose Alice and Bob want to establish a shared secret key using Diffie-Hellman key exchange. They agree to use a prime modulus p = 13 and a base g = 3. Alice chooses a secret integer a = 4 and sends g^a mod p to Bob. Bob chooses a secret integer b = 3 and sends g^b mod p to Alice. What is the shared secret key that Alice and Bob can use to encrypt and decrypt their messages? 2023E [2][CO4]



a = 4

ALICE

b = 13
g = 3

h = 3

BOB

$A = g^a \bmod (p)$
$= 3^4 \,\%\, 13$
$\Rightarrow A = 3$

$B = g^b \bmod (p)$
$= 3^3 \,\%\, 13$
$\Rightarrow B = 1$

Send

Send

$B = 1$

$A = 3$

∴ Secret Key = k,
$k = B^a \bmod (p)$
$= 1^4 \,\%\, 13$
$k = 1$

∴ Secret key, k
$k = A^b \bmod (p)$
$= 3^3 \,\%\, 13$
$k = 1$

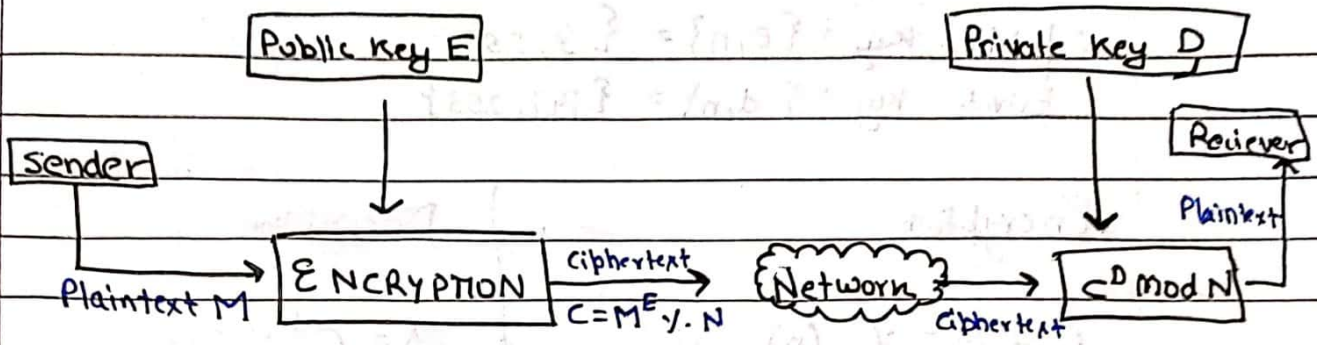
∴ Shared Secret Key is (1).

B) Explain working of RSA algorithm for encryption and decryption and also find cipher text corresponding to plain text M=9, also generate Public key and Secret key using RSA algorithm by taking two prime numbers p=11 and q=23. 2019 S

RSA is the most widely used public key algorithm named after its creators Rivest, Shamir and Aldeman. It is based upon the principle that it is easy to multiply two prime numbers but it is very difficult to factor their product and get them back.

The algorithm is as follows.

Page No.
Date



i.) Take two very large prime numbers A and B of equal lengths and obtain their product (N).

$\therefore N = A \times B$

ii.) Subtract 1 from A and B and take their product

$\therefore T = (A-1)(B-1)$

iii.) Choose a public key (E) which is randomly chosen such that it has no common factors with T.

iv.) Obtain the private key (D) as under:

$D = E^{-1} \bmod T$

v.) The rule for encryption of a block of plaintext M into ciphertext (C) is:

$C = M^E \bmod N$

vi) The received message C at the receiver is decrypted to obtain the plaintext back as

$M = C^D \bmod N$

Given,

$p = 11$

$q = 23$

$M = 9$

$e = 3$ (say)

$\therefore N = p * q = 253$

$\phi(N) = (p-1)(q-1) = 220$

$\therefore d = f^{-1} \bmod (\phi n)$

$\Rightarrow d = 147$

Page No.
Date

∴ public key : {e, n} = {3, 253}
private key : {d, n} = {147, 253}

Encryption	Decryption
$C = M^e \% (n)$	$M = C^d \% (n)$
$= 9^3 \% 253$	$= 223^{147} \% 253$
$= 223$	$= 9$

[b] What is the meaning of integrity and confidentially in network security? How you can use RSA algorithm to a accomplish them 2018S

INTEGRITY : It refers to the assurance that the data transmitted or stored has not been altered or tampered with in an unauthorized manner. It ensures that the data remains intact and accurate throughout its entire lifecycle.

CONFIDENTIALITY : It refers to ensurance that the data is accessible only to authorized individuals or entities. It prevents the unauthorized disclosure of sensitive information.

RSA can be used to accomblish both :-

→ For integrity, the sender uses their private key to sign the msg, and the receiver uses the sender's public key to verify the signature ensuring no tampering.

→ For confidentiality, the message is encrypted using the recipient's public key, ensuring only the recipient can decrypt the content

— 127 —

Page No.
Date

Q.6

A) What is cryptography? Discuss various methods of cryptography. Explain substitution &transposition encryption with suitable example and also discuss the working of Data Encryption Standards (DES).Explain distance vector algorithm with suitable example .

2019 S

Traditional Ciphers

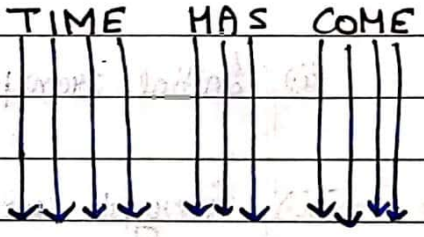
SUBSTITUTION ENCRYPTION

Substitution cipher refers to technique where cipher replaces characters in the plaintext with other characters or symbols to create cipher text:

i) Monoalphabetic Substitution

Each plaintext character is replaced by a fixed other character. The relationship b/w cipher and plaintext is one-to-one.

It is simple to implement but easy to break

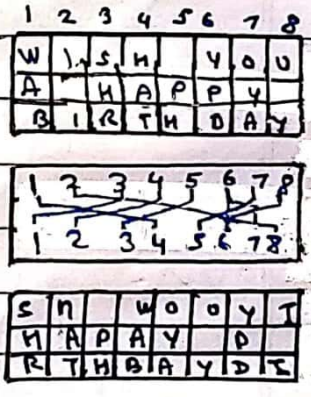


ii) Polyalphabetic Substitution

Each plaintext character is replaced by a group of other characters.
The relationship b/w plaintext and ciphertext is one to many.
The specific replacement is determined by a key.
It is more secure than mono — but is vulnerable to cryptoanalysis.

TRANSPOSITION ENCRYPTION

The transposition cipher rearranges plaintext characters based on key defined columns permutations.



While it's not highly secure, and susceptible to trial and error; it can enhance security when combined with other methods.

Page No.
Date

DATA ENCRYPTION STANDARDS (DES)

DES, developed in 1972 uses 56 bit key for encryption. Its steps for encryption are as follows and reverse steps are used for decryption:

i.) Divide the message into 64 bit blocks $M_1, M_2 \ldots M_n$

ii.) Initial transposition

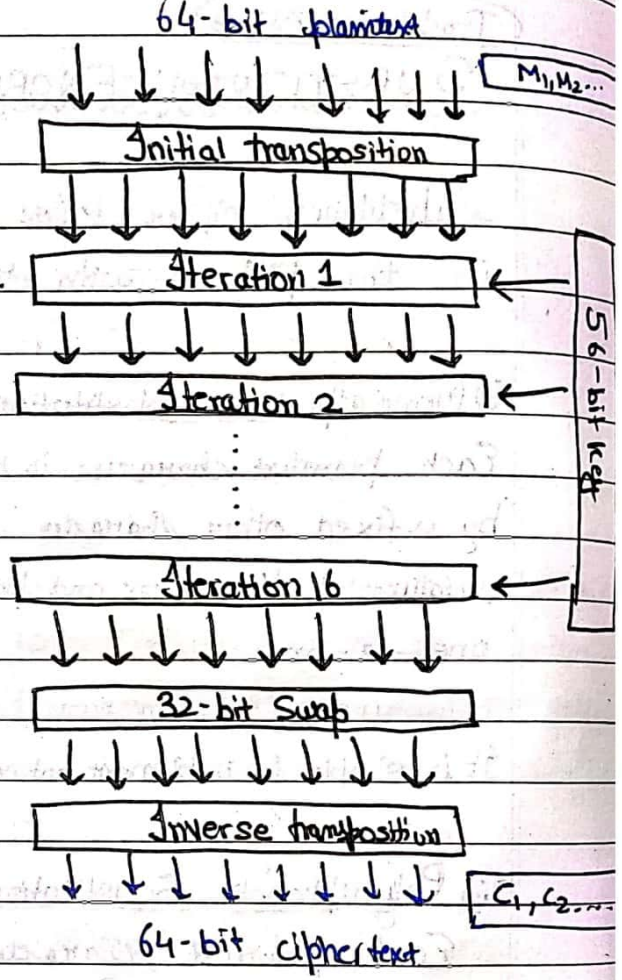
iii.) Encrypt rounds 1...16 with keys 1...16 (grinding XOR, shifting etc.)

iv.) 32 bit swap.

v.) Reverse the transposition

vi.) Now, you get cipher text $C_1, C_2 \ldots$

Send msg to receiver.



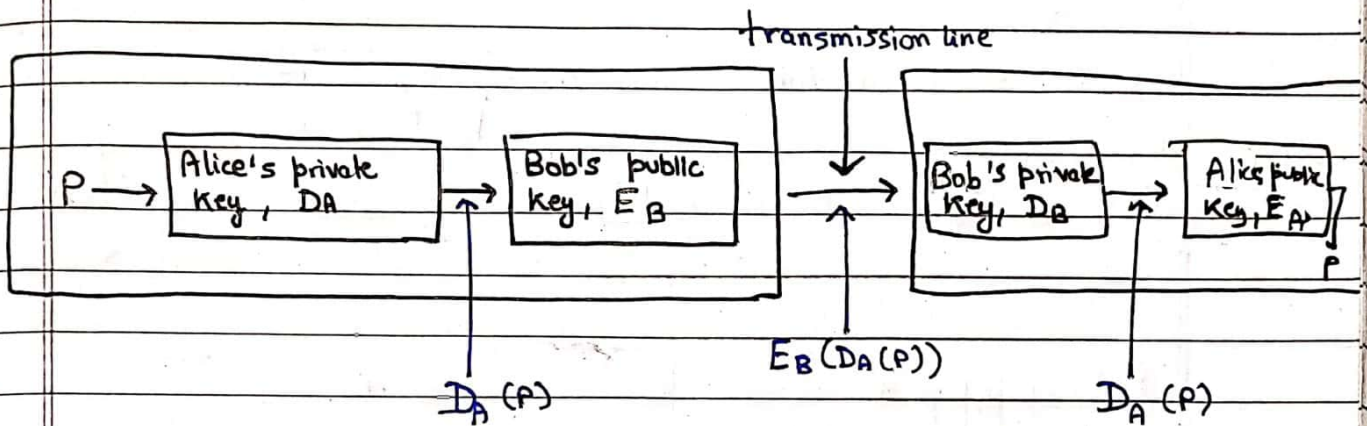
What is a digital signature, explain with the help of diagram and mention applications of digital signature. 2023E [2][CO6]

Q.7 Write short notes on the following:
[a] Digital Signature. 2019S

d) Digital signature using public-key cryptography 2019E

Q.7 Write short notes on the following:
[a] Digital Signature. 2018S

A digital signature is a data structure that provides proof of origin i.e, Authorization and integrity, and depending on how it is used, it can also provide non-repudiation.



Alice wants to send a msg to Bob w/o modification during t/r. To ensure this, Alice uses a hash digest of her msg and encrypts it using her private key. She then sends both the msg and encrypted digest, which serves as her digital signature.

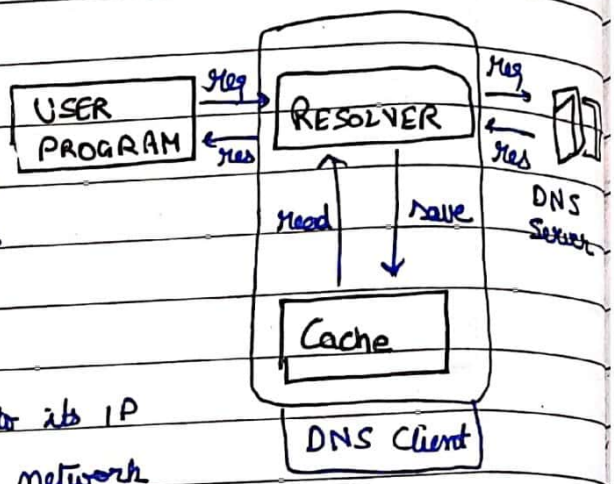
Bob can verify the signature by computing the hash digest of the received message and comparing it to the digest he obtains by decrypting the signature using Alice's public key. If the digest matches Bob knows the message came from Alice and has not been tampered.

Applications of Digital Signature:-
→ document signing
→ email security
→ Software distribution
→ financial transactions
→ goverment documents
→ legal proceedings
→ code signing

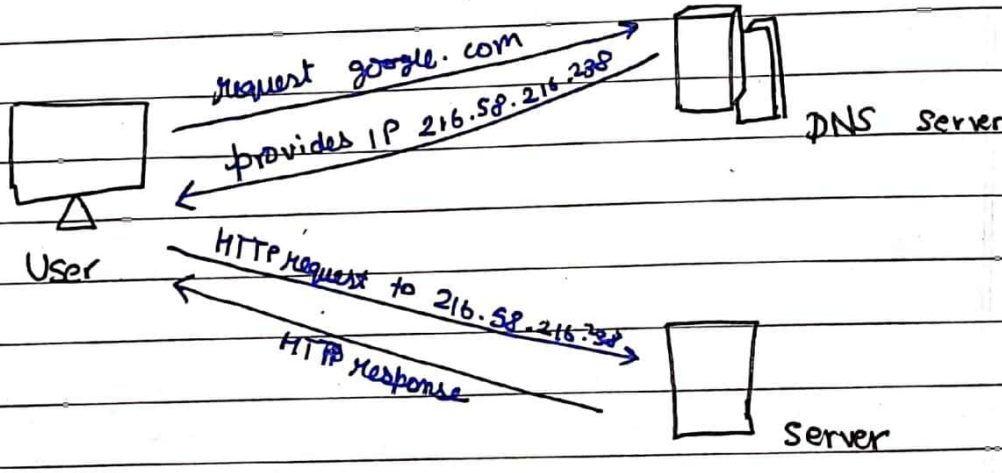
b. Domain Name System 2018S
c) DNS 2019S
iii) Domain Name System (DNS) 2023E
[c] DNS 2018S
[d] Domain Name System 2018S

DOMAIN NAME SYSTEM

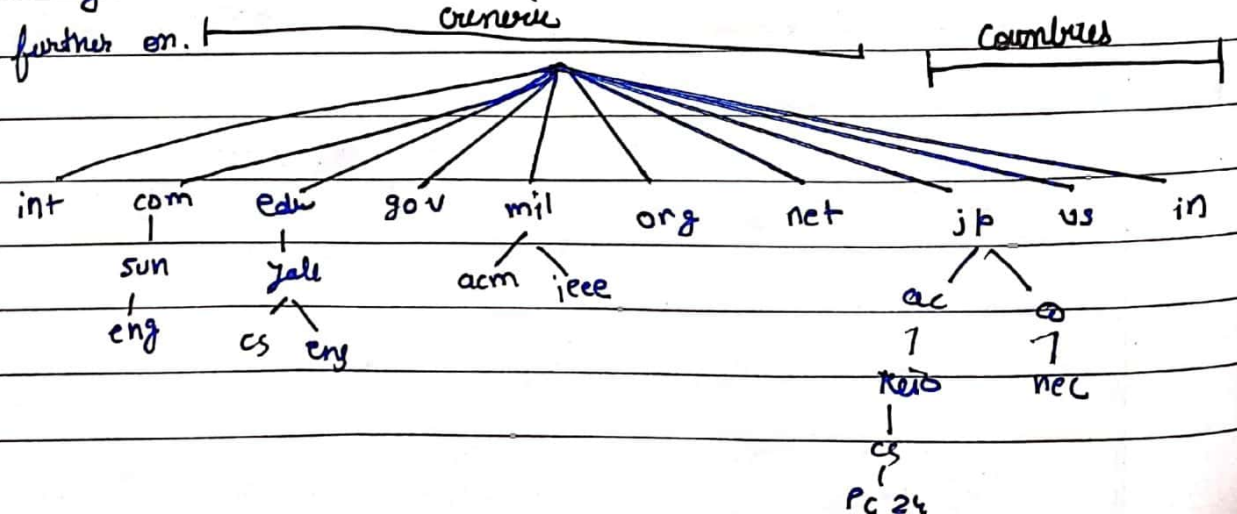
DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.



DNS translate the domain name into its IP address. This allows the users of network ease to look up names instead of remembering IP addresses.



Internet has been divided into hundreds of top level domains which cover many hosts. Each domain is divided into several subdomains and further on.



UNIT- 6: Application Layer

Page No.
Date

iv) Simple Mail Transfer Protocol (SMTP) 2023E
b. Mail Transfer Agent, SMTP, POP, IMAP 2018E

Mail Transfer Agent (MTA)

A mail transfer agent is a software application that is responsible for receiving, routing and delivering email messages. MTAs are the backbone of email communication, as they handle the entire process of transmitting messages from the sender to the recipient.

Ex.) Sendmail, Postfix, Microsoft Exchange Server.

Simple Mail Transfer Protocol (SMTP)

SMTP serves as the backbone of email transmission online. It meticulously dictates the structure, addressing and transmission of email messages between MTAs. Users initiate email transmission by connecting to the recipient's SMTP server, typically on port 25. Once connected, the SMTP server oversees the transfer ensuring the message is correctly formatted and directed to the recipients mailbox. Should any issues arise, the server promptly notifies the sender, maintaining integrity.

This ASCII based protocol relies on a series of commands and responses for effective communication. Upon connection, the server signals its readiness, prompting the client to identify sender and recipient details. Valid recipients trigger the server to instruct the client to relay the message, which it acts upon success. Despite its reliability, older SMTP versions may encounter challenges with large messages or abrupt connection terminations due to timeout discrepancies.

Page No.
Date

Post Office Protocol (POP)

POP is a protocol used by email clients (such as Gmail/Outlook) to download email messages from a remote mail server to a local device. When a user checks their email using a POP-based email client, the messages are typically downloaded to the local device and removed from server. It is an older protocol and has been largely superseded by IMAP.

Internet Message Access Protocol (IMAP)

IMAP is an alternative to POP for accessing email messages from a remote mail server. Unlike POP, IMAP allows users to access their email messages from multiple devices, as they messages are stored on the server. IMAP also provides more features such as ability to access and manage email folders, search messages, and synchronize email across multiple devices.

Total number of pages: 2 *Roll No.* _____

SIXTH SEMESTER **B.TECH**
MID SEMESTER EXAMINATION **MARCH 2024**

CO-306 COMPUTER NETWORKS

Time: 1:30 hr. ***Max. Marks: 20***

***NOTE**: Attempt all the questions unless a choice is specified.*
Assume suitable missing data, if any.

Q.1. i. What are the advantages and disadvantages of utilizing a hybrid topology comprising star, bus, and mesh components in terms of fault tolerance and network reliability? **[2]** [CO1]

ii. An IP datagram with a size of 4500 bytes, including a 20-byte header, arrives at a router. The MTU (Maximum Transmission Unit) of the router's outgoing link is 1400 bytes. Determine the values of length, fragment flag, and fragment offset for all fragments created by the router.
[3] [CO4]

Fragment 1:

Length: 1400 bytes (Maximum Transmission Unit)
Fragment Flag: 1 (Indicating more fragments to follow)
Fragment Offset: 0 (First fragment, offset in units of 8 bytes)

Fragment 2:

Length: 1400 bytes (Maximum Transmission Unit)
Fragment Flag: 1 (Indicating more fragments to follow)
Fragment Offset: 1400 bytes / 8 = 175 (Offset in units of 8 bytes)

Fragment 3:

Length: 1400 bytes (Maximum Transmission Unit)
Fragment Flag: 1 (Indicating more fragments to follow)
Fragment Offset: 2800 bytes / 8 = 350 (Offset in units of 8 bytes)
Fragment 4:

Length: 280 bytes (Remaining payload size)

Fragment Flag: 0 (Indicating this is the last fragment)
Fragment Offset: 4200 bytes / 8 = 525 (Offset in units of 8 bytes)
So, the values of length, fragment flag, and fragment offset for all fragments created by the router would be as follows:

Fragment 1: Length = 1400 bytes, Fragment Flag = 1, Fragment Offset = 0
Fragment 2: Length = 1400 bytes, Fragment Flag = 1, Fragment Offset = 175
Fragment 3: Length = 1400 bytes, Fragment Flag = 1, Fragment Offset = 350
Fragment 4: Length = 280 bytes, Fragment Flag = 0, Fragment Offset = 525

Q.2. i. Explain the concept of Cyclic Redundancy Check (CRC) and provide a detailed explanation of how CRC is generated at the sender side and calculated at the receiver end. Illustrate the process with the given dataword 1010011010 and divisor x^4+x^2+x+1 through binary division. **[3]** [CO2]

After performing XOR division properly, the remainder obtained is 0001

ii. What are the values of k and n in a Hamming code C(n, k) with a minimum Hamming distance $d_{min} = 3$, when a dataword of at least 16 bits is needed?**[2]** [CO2]

$$2^p \geq p + k + 1, k \text{ is number of datawords}$$
$$2^5 \geq 5 + 16 + 1$$

$$n \text{ is codeword},$$
$$n = p + k,$$
$$n = 21$$

Q.3. i. Explain the sliding windows protocol and compare window size, throughput, acknowledgement type, and other relevant details across different sliding window protocols. What is the maximum window size at the sender for each sliding window protocol when using 8 bits to represent the sequence numbers? **[3]** [CO3]

SWS in go back n 255 and Selective Repeat 128

ii. In a CSMA/CD network, if the signal propagation speed is 200,000 km/s and the round-trip time is 100 microseconds, calculate the maximum frame size (excluding preamble and SFD) to avoid late collisions.**[2]** [CO3]

In this ques need to assume the Ethernet transmission rate: 10 Mbps, as not mentioned so give marks to attempt the que.

Q.4. i. Consider the following subnet in fig 1. Distance vector routing is used, and the following vectors have just come into router C: from B: (5, 0, 8, 12, 6, 2); from D: (16, 12, 6, 0, 9, 10); and from E: (7, 6, 3, 9, 0, 4). The new measured delays to B, D, and E, are 6, 3, and 5, respectively. What is C's new routing table? Give both the outgoing line to use and the expected delay. **[3]** [CO4]

A	B	11
B	B	6
C	-	0
D	D	3
E	E	5
F	B	8

ii. Given the IP address 192.168.10.0/24, subnet it into four subnets, and provide the range of valid IP addresses for each subnet. **[2]** [CO4]

1. Original network: 192.168.10.0/24

- Network address: 192.168.10.0

- Subnet mask: 255.255.255.0

2. Borrow 2 bits for subnetting, resulting in a new subnet mask of /26 (24 + 2 = 26).

3. Determine the new subnet mask:

- 255.255.255.0 in binary is 11111111.11111111.11111111.00000000

- Borrowing 2 bits: 11111111.11111111.11111111.11000000

- Converted back to decimal: 255.255.255.192 (/26)

4. Calculate the number of hosts per subnet:

- With a /26 subnet mask, 2 bits are borrowed from the host portion, leaving 6 bits for hosts.

- 2^6 - 2 = 62 hosts per subnet (minus 2 for network address and broadcast address).

5. Determine the subnet ranges:

- Subnet 1:

- Network address: 192.168.10.0/26

- Range of valid IP addresses: 192.168.10.1 to 192.168.10.62

- Broadcast address: 192.168.10.63

- Subnet 2:

- Network address: 192.168.10.64/26

- Range of valid IP addresses: 192.168.10.65 to 192.168.10.126

- Broadcast address: 192.168.10.127

- Subnet 3:

- Network address: 192.168.10.128/26

- Range of valid IP addresses: 192.168.10.129 to 192.168.10.190

- Broadcast address: 192.168.10.191

- Subnet 4:

- Network address: 192.168.10.192/26

- Range of valid IP addresses: 192.168.10.193 to 192.168.10.254

- Broadcast address: 192.168.10.255

Total no. of Pages: 2

Roll no.....

SIXTH SEMESTER

B.Tech. CSE

ENDTERM EXAMINATION

May-2024

COURSE CODE CO306

COURSE TITLE COMPUTER NETWORKS

Time: 03:00Hours

Max.Marks:40

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

Q.1 (a). What is the function of transmission media? Differentiate between guided and unguided media, and explain the three principal classifications of guided media. **[4][CO 1]**

(b). Explain the concept of Framing in the data link layer. Write the difference between bit stuffing and character stuffing.If a bit string, 01111011111101111110, needs to be transmitted at the data link layer. What is the string transmitted after bit stuffing given flag as 01111110? **[4][CO2]**

Q.2 (a). Describe the role of TCP's additive increase and multiplicative decrease algorithm in congestion control. Considering an initial slow start phase followed by the congestion avoidance phase, how long does it take to reach the full transmission capacity on a network with a 10-millisecond RTT and no congestion, given a receiver window of 3200 KB and a maximum segment size of 200 KB? **[4][CO 4]**

(b). Explain the fundamental steps involved in performing a remote procedure call (RPC) and the respective roles of the client and server in this process. **[4][CO 4]**

Q.3 (a). Discuss the significance of firewalls in network security and the different types of firewalls employed to protect networks from unauthorised access and malicious activities. Describe the role of firewalls in filtering incoming and outgoing email traffic to prevent spam, malware, and other threats. **[4][CO 6]**

(b). Explain the three phases in TCP client-server communication. In TCP, the initial RTT is 20 ms. The ack for the first four segments are received in times 25 ms, 18 ms, 23 ms, and 21 ms. Using the basic algorithm, find the timeout timer value for the first five segments. Use $\alpha = 0.5$. **[4][CO 4]**

Q.4 (a). What role does cryptography play within the presentation layer? Describe the key selection algorithm in RSA and apply it to solve the following scenario: Given p = 13, q = 5, and e = 7 in the RSA algorithm, determine the value of d and the cipher value of '6' with the key (e, n). **[4][CO 5]**

(b). Give a diagram and explain the IPv4 header fields in detail. If a datagram of size 600 bytes is transmitted over a network with a Maximum Transmission Unit (MTU) of 200 bytes, and the header length is 20 bytes, what are the offsets of the first, second, and third fragments? **[4][CO 3]**

Q.5 (a). Describe IPV4 classful IP addressing. Discuss the limitations and the significance of subnetting. If a class B address is to be divided into subnets with a 6-bit subnet number, determine the maximum number of subnets and the maximum number of hosts in each subnet. **[4][CO 3]**

(b). Explain the difference between multicast and broadcast. Suppose there are n stations in a slotted LAN. Each station attempts to transmit with a probability 'p' in each time slot. What is the probability that only one station transmits in a given slot? **[4][CO 3]**

Q. 6 (a). Explain the concept of digital signatures in cryptography. What is the significance of digital signatures in ensuring data integrity, authenticity, and non-repudiation in electronic transactions? **[4][CO 5]**

(b). Discuss the flow control and error control collaboration in the Data Link Layer to ensure reliable data transmission. What is the minimum frame size needed to achieve a channel efficiency of at least 50% for a channel operating at 4 Kbps with a one-way propagation delay of 20 milliseconds, using the stop-and-wait protocol where the ack frame transmission time is negligible? **[4][CO 2]**