University School of Information Communication and Technology
Guru Gobind Singh Indraprastha University, Delhi

IT-304 Computer Network

B-Tech IT IVth sem

NAME - HARSH BATRA Enroll No. - 02716401520

Assignment

Q1. Explain the telephone system (Structure, trunks, multiplexing and switching).

Ans The telephone is an important tool for sharing information for businesses. In a small company, the telephone system may be as simple as having one or two telephone lines for the company. In other companies the telephone system may include many lines and be integrated with a computer system.

Centralized Telephone systems

Centralized Telephone systems route calls coming into and going out of an organization. All calls in a centralized system are handled by a single computer or operator switchboard that routes calls to the requested location. older system required the assistance of a human switchboard operator to answer and transfer calls. Some systems that are handled by computer give callers the option of speaking to a human operator.

Many telephone system in business today are answered by an automated attendant. An automated attendant is a computerized system for handling telephone calls. When an incoming call is answered by an automated attendant, a recorded message is played. Messages vary depending on company needs. However the message usually instructs the caller to design/dial the extension number of person being sought. It may provide the caller with various

menu options. Callers make selection using the telephone number keypad. Some systems also allow users to select menu options by speaking a word or term into the receiver. A computer will identify the spoken command and perform the chosen action. This feature is called speech recognition. Additional message may then instruct and direct the Caller.

The option of speaking with a person is no longer always a choice for the Caller. However many companies continue to offer an option to speak with a person to provide better services for customers. Some Callers prefer to talk with a person rather than with a computer. Others Callers may not have a touch tone phone, which is usually required for the automated system.

1. Structure: The telephone system has a hierarchical structure that encompasses local, regional and long distance networks. At the local level there are telephone exchanges that serve a specific geographic area, typically covering a city or a neighbourhood. These exchanges are interconnected to form the regional network, which in turns connects to the long-distance network, allowing calls to made across different regions and countries.

2. Trunks: Trunks are the physical transmission lines that carry voice-signals between telephone exchanges. They can be copper wires, fire-optic cables or even satellite connections. Trunks can span long distance and have a higher capacity compared to regular telephone lines.

3. Multiplexing :- multiplexing is the process of combining multiple signals onto a single transmission medium. In the telephone system, multiplexing is used to maximize the utilization of trunks. Time-division multiplexing (TDM) is commonly employed, where each voice call is divided into small time-slots, and multiple calls are interleaved together for transmission.

4. Switching :- Switching is the mechanism that allows calls to be routed from one telephone line to another. There are several types of switching techniques used in the telephone system:

Q2 Explain transmission media and wireless transmission system. Mention the parameters for each.

Ans Transmission media refers to the physical pathways or channels used to transmit data or information from a source to a destination. It can be categorized into two main types. wired transmission media and wireless transmission media. let's explore each type along with their parameters.

1. **Wired Transmission media :-**

a) Twisted pair : consist of two insulated copper wires twisted together.
- Bandwidth : suitable for lower bandwidth applications.
- Distance : limited distance coverage, typically up to a few hundred met
- Interferences : susceptible to electromagnetic interference (EM and cross talk.

b) Coaxial Cable : Consist of a central conductor surrounded by an insulating layer, a metallic shield, and an outer insulating layer.

- Bandwidth : offers higher bandwidth compared to twisted pair.
- Distance : Can cover longer distances, typically up to a few Kilometers.
- Interference : Provides better resistance to EMI compared to twisted pair.

c) Fibre-optic Cable : Utilizes optical fibres to transmit data as pulses of light.
- Bandwidth : Provides high bandwidth capabilities.
- Distance : Can cover long distances, ranging from a few Kilometres to thousand of kilometres.
- Interference : Provides better resistance Immune to EMI, provides better security against eavesdropping.

2. Wireless Transmission Media :

a. Radio Waves : Utilizes radio frequencies to transmit data.
- Bandwidth : offers a range of bandwidth options, depending on the frequency and modulation technique used.
- Distance : Coverage can vary significantly from short to long-range transmission depending on the frequency and power.
- Interference : susceptible to interference from other wireless devices and environmental factors.

b. Microwaves : Utilizes higher frequency electromagnetic waves for transmission.
- Bandwidth : offers relatively high bandwidth capabilities.
- Distance : Typically used for medium to long-range communication, covering several kilometres to tens of kilometres.
- Interference : susceptible to atmospheric conditions and physical obstructions

:. Infrared : Utilizes infrared light for short range wireless communication

- Bandwidth : Suitable for lower to moderate bandwidth application
- Distance : Limited coverage, typically with a room or short distances.
- Interference : susceptible to physical obstacles and ambient light conditions.

1. Satellite : Utilizes communication satellites to transmit signals over long distances.

- Bandwidth : Can provide high bandwidth capabilities.
- Distance : Enables global coverage, connecting users across vast distances.
- Interference : susceptible to atmospheric conditions and signal degradation.

:. Explain LAN and WAN technologies and protocols.

LAN (Local Area Network) and WAN (wide Area Network) are two types of computer networks with distinct characteristics and technologies. Let's explore each one along with the protocols commonly associated with them:

- LAN (Local Area Network)
- Definition : A LAN is a network that covers a small geographical area, such as an office building, school, or home.
- Technologies : LAN's typically utilize wired technologies, such as Ethernet, to connect devices with the network. Wireless LANs (WLANs) can also be used, employing wi-fi standards.
- Protocols : The common protocols used in LANs include.
- Ethernet (IEEE 802.3) : A widely used protocol that defines the rules for data transmission over LANs. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD

for media access control.

- Wi-fi (IEEE 802.11): A set of wireless protocols that enable devices to connect and communicate wirelessly within a LA Wi-fi utilizes various standards, such as 802.11a, 802.11b 802.11g, 802.11n, 802.11ac and 802.11ax (Wi-Fi 6)

2. WAN (Wide Area Network):

- Definition: A WAN is a network that spans large geograph areas, connecting multiple LAN's or other networks acr different locations.
- Technologies: WANs typically rely on Telecommunications infrastructure, including leased lines, circuit switched networks, and packet switched networks, to transmit data over long distances.
- Protocols: The common protocols used in WANs include:
  - TCP/IP (Transmission Control Protocol/Internet Protocol): A suite of protocols that enables data transmission and netwo communication in WANs and the Internet. It incl protocols like IP (Internet protocol), ICMP (Internet Control message Protocol), TCP (Transmission Control Pro and UDP (User Datagram Protocol)
  - MPLS (multiprotocol label Switching): A protocol for rou and forwarding data packets in WANs. MPLS allows for efficient and reliable packet transmission by assigning la to packets and establishing predetermined paths through the network.

4. Explain sliding window protocols with an illustration for each.

Ans The sliding window is a technique for sending multiple frames at a times. It controls the data between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).

In this Technique, each frame has send from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Types of sliding Window Protocol

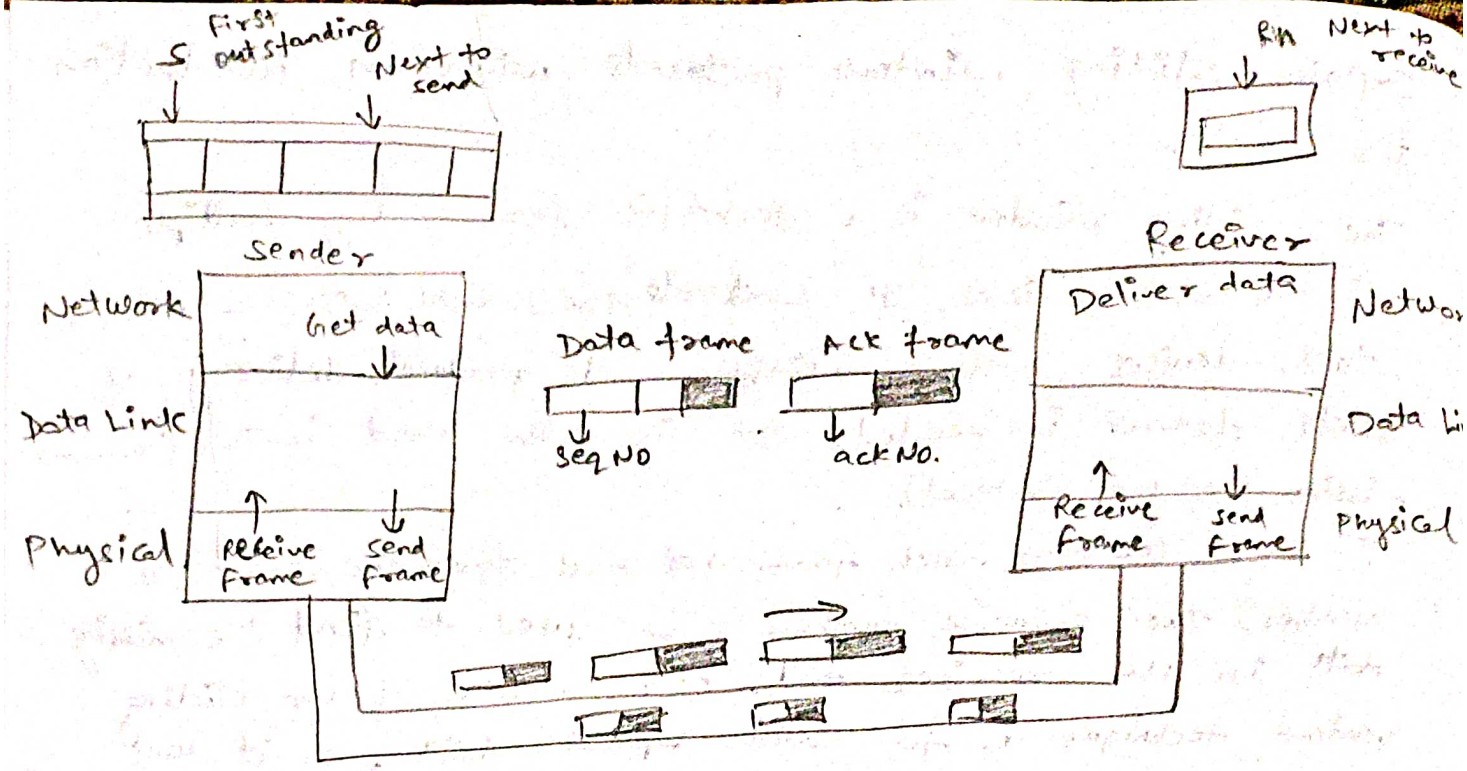
Sliding Window protocol has two types:

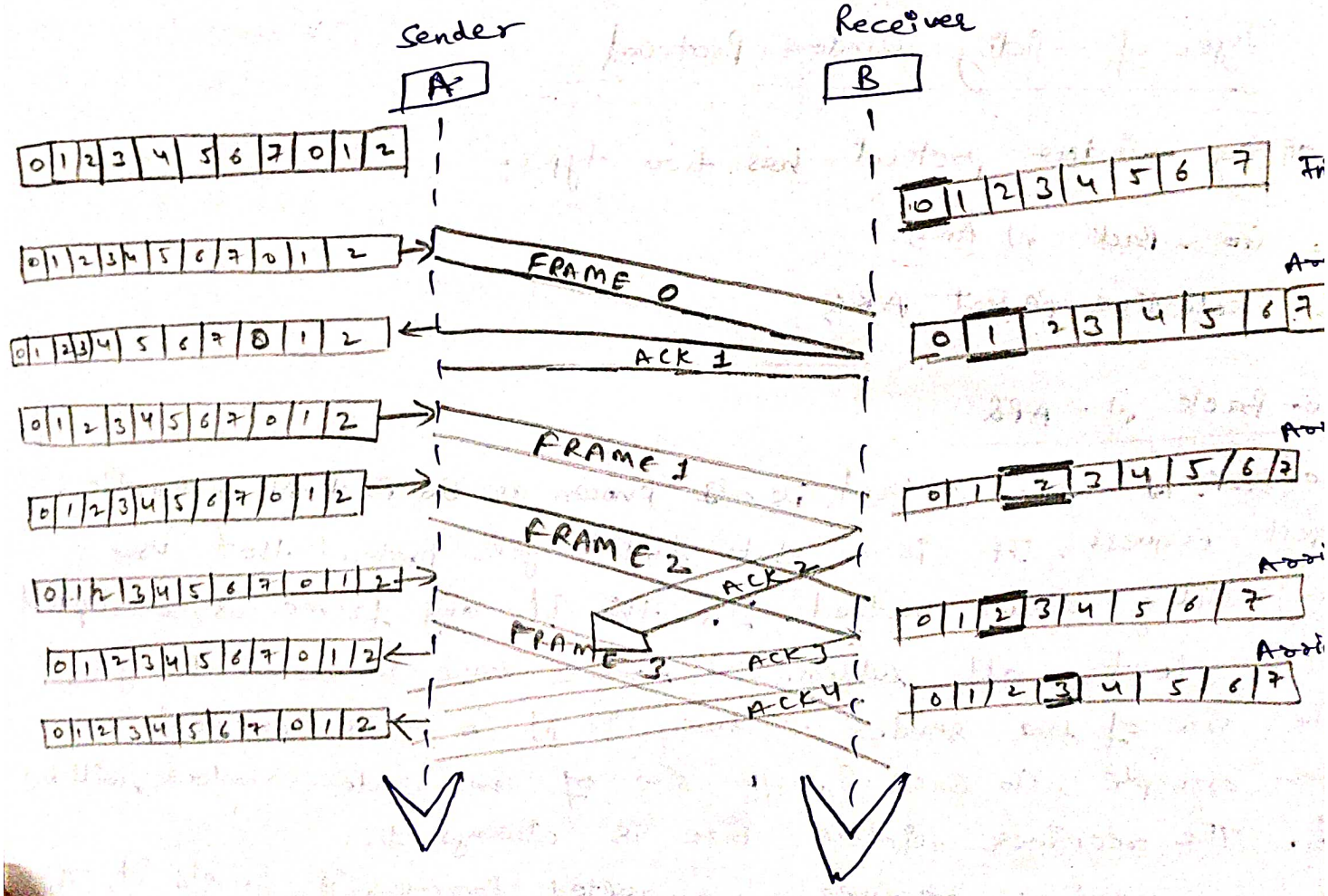
1. Go - Back N ARQ
2. selective Repeat ARQ

Go- Back N - ARQ

Go Back N ARQ protocol is also known as Go Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this if any frame is corrupted or lost, all subsequent frames have to be sent again. The size of the sender window is N in this protocol. for example, Go Back -8, the size of the sender window, will be 8. The receiver window size is always 1.

If the receiver receives a corrupted frame, it cancels it. The receiver does not accept a corrupted frame. when the timer expires, the sender sends the correct frame again. The design of the Go -Back-N-ARQ protocol is shown below.

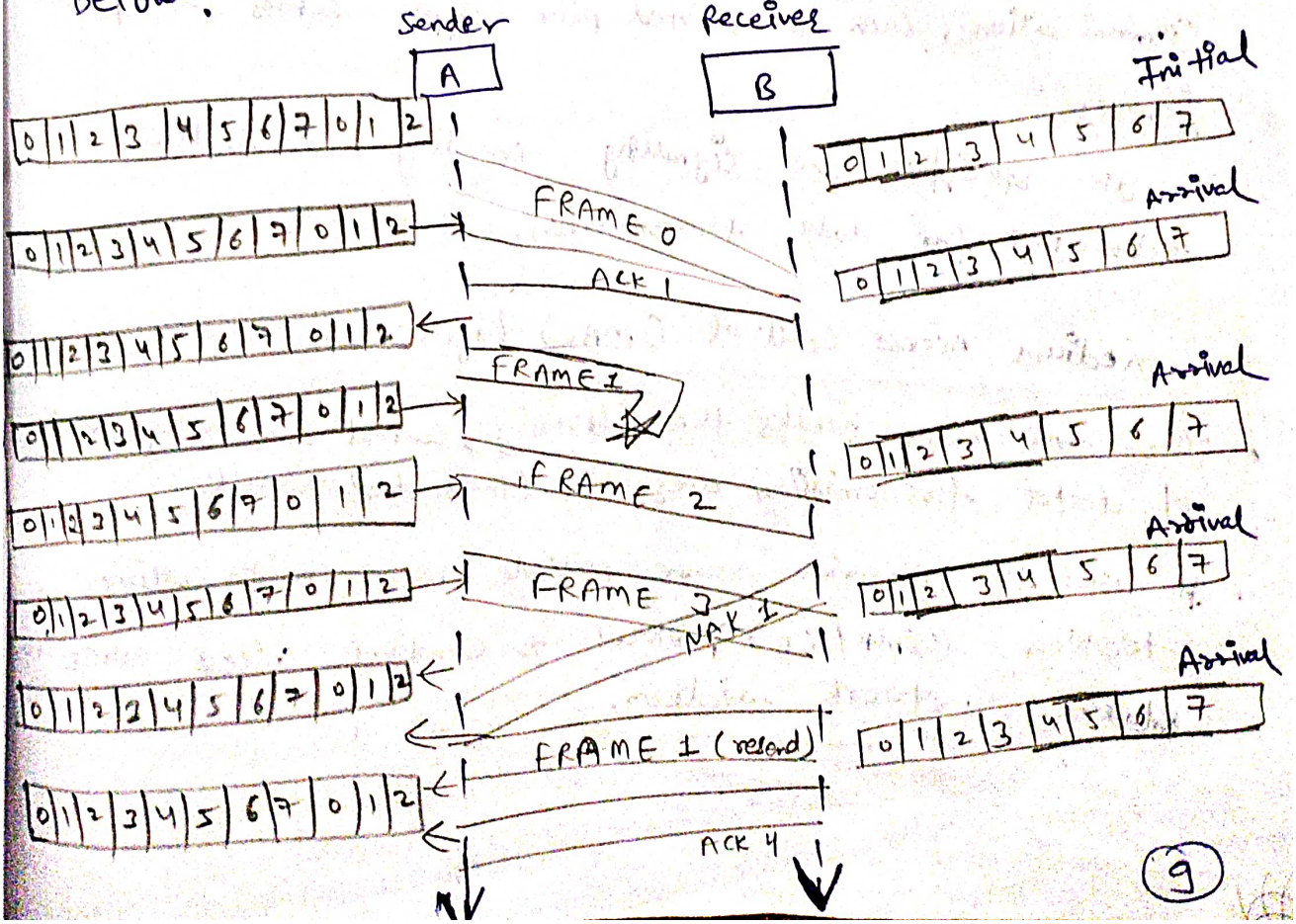

First outstanding
Next to send
Sender
Network
Get data
Data Link
Physical
Receive frame
Send frame
Data frame
Ack frame
SeqNO
ackNO.
Receiver
Deliver data
Receive frame
Send frame


Sender
A
Receiver
B
FRAME 0
ACK 1
FRAME 1
FRAME 2
ACK 2
FRAME 3
ACK 3
ACK 4

Selective Repeat ARQ

Selective Repeat ARQ is also known as the selective Repeat Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. The Go-back N- ARQ protocol works well if it has fewer errors. But if there is a lot of error in the frames, lots of bandwidth loss in sending the frames again. So, we use the selective Repeat ARQ protocol. In this protocol, the size of the sender window is always equal to the size of the receiver window. The size of the sliding window is always greater than 1.

If the receiver receives a corrupt frame, it does not directly discard it. It sends a negative acknowledgement to the sender. The sender sends that frame again as soon as on the receiving negative acknowledgement. There is no waiting for any time-out to send that frame. The design of the selective Repeat ARQ protocol is shown below.



Q5 Explain IEEE standard 802.3 and 802.11 and the protocol architecture for each.

Ans Here's an explanation of IEEE standard 802.3 and IEEE standard 802.11 along with the protocol architecture for each:

IEEE standard 802.3 (Ethernet)

IEEE standard 802.3 commonly known as ethernet, is a set of networking standards that governs wired LAN (Local Network) communication. It defines the physical and link layers of the Ethernet protocols. The protocol architecture for IEEE 802.3 includes the following components:

1. Physical layer (PHY):

- The physical layer defines the electrical & mechanical characteristics of the physical medium used for ethernet communication, such as twisted pair copper cables or optical fibres.
- It specifies the signaling encoding and modulation techniques for data transmission.

2. Medium Access Control (MAC) Layer

- The MAC layer handles the addressing, control and management of data transmission over the Ethernet network.
- It uses the Carrier sense multiple access with collision detection (CSMA/CD) protocol to control access over shared network medium.

Ethernet Frame format :

- The Ethernet frame format defines how data is structured and encapsulated for transmission over the network.
- It includes fields for source and destination MAC addresses, frame length, type / length, payload and error checking.
- The maximum frame size allowed in ethernet is 1518 bytes for standard Ethernet and 9000 bytes for jumbo frames.

IEEE standard 802.11 (Wi-Fi) :

IEEE standard 802.11 commonly known as Wi-fi is a set of wireless networking standards that govern wireless LAN (WLAN) communication. It specifies the protocols and mechanisms for wireless communication. The protocol architecture for IEEE 802.11 includes the following components :-

1. Physical Layer (PHY)

- The Physical Layer defines the radio frequency characteristics, modulation schemes, and channel access methods for wireless communication.
- It specifies different frequency bands, data rates and modulation techniques such as 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax (wifi 6)

2. Medium Access Control Layer (MAC) :-

- The MAC Layer manages the medium access control and provides data link layer service for wireless communication.

- It handles frame fragmentation, reassembly, acknowledg and error detection.
- The MAC layer uses various protocols for channel access, including the Distributed Coordination Funct

3. Security & Authentication:-

- The Wi-fi Alliance defines security protocols and mechanisms for wi-fi networks, including Wired Equi Privacy (WEP), wi-fi protected Access (WPA) and WPA 2 | WPA 3.
- These protocols ensure the confidentiality, Integrit and authentication of wireless data.

4. Wi - fi Direct and wi fi Multimedia (WMM):-

- wi-fi direct enables peer to peer communication b/ wi fi devices without the need for an access poi
- WMM (wi fi multimedia) provides QoS - (quality of service Support for wi-fi networks, allowing prioritization of different types of traffic, such as voice, video and data.

Q6 A bit stream 100 1110 1 is transmitted using the standard CRC method. The generator polynomial is x^3+1. Show the actual bit string transmitted. Suppose that the third bit from the left is inverted during transmission. Show that this error is detected at the receiver's end. Give an example of bit errors in the bit string transmitted that will not be detected by the receiver.

Ans

Our Generator $G(x) = x^3+1$ encoded as 1001. Because the generator polynomial is of the degree three we append three zeroes to the lower end of the frame to be transmitted. Hence after appending the 3 zeroes the bit stream is 100111010000. On dividing the message by generator after appending three zeroes to the frame we get a remainder of 100. We do modulo 2 subtraction thereafter of the remainder from the bit stream with the three zeroes appended. The actual frame transmitted is 100 111 011 00. See below.

```
          10001100
      ____________
1001 | 100111010000
       1001
       ----
        0011
        0000
        ----
         0110
         0000
         ----
          1101
          1001
          ----
           1000
           1001
           ----
            0010
            0000
            ----
             0100
             0000
             ----
              100   remainder
```

Actual frame transmitted : 1001110|000 - 100

= 1001110|100 (modulo 2 Subtraction)

Now suppose the third bit from the left is garbled and the frame is received as 1011110|100 Hence on dividing this by polynomial generator we get a remainder of 100 which shows that an error has occured. Had the received frame been error free we would have got a remainder of zero.

```
          1 0 1 0 1 0 0 0
        ---------------------
100   | 1 0 1 1 1 1 0 1 0 0 0
        1 0 0
        -------
          0 1 0
          0 0 0 0
          -------
            1 0 1 1
            1 0 0
            -------
              0 1 0 0
              0 0 0 0
              -------
                1 0 0 1
                1 0 0
                -------
                  0 0 0 1
                  0 0 0 0
                  -------
                    0 0 1 0
                    0 0 0 0
                    -------
                      0 1 0 0
                      0 0 0 0
                      -------
                        1 0 0
```

remainder indicating error

Explain Circuit Switching techniques and packet switching techniques. Explain the types of channel allocation.

Circuit Switching

Circuit switching is a communication method where a dedicated communication path, or circuit dedicated to the communication for the duration of the session, and no other devices can use it while the session is in progress. Circuit switching is commonly used in voice communication and some types of data communication.

Advantages

- Guaranteed bandwidth :- Circuit switching provides a dedicated path for communication, ensuring bandwidth is guaranteed for the duration of the call.
- Low latency :- Circuit switching provides low latency because the path is predetermined and there is no need to establish a connection for each packet.

Disadvantages

- Inefficient use of bandwidth :- Circuit switching is inefficient because the bandwidth is reserved for the entire duration of the call, even when no data is being transmitted.
- Limited scalability :- Circuit switching is limited in its scalability because the no. of circuits that can be established is finite, which can limit the number of simultaneous calls that can be made.

Packet Switching

Packet switching is a communication method where data is divided into smaller units called packets and transmitted

over the network. Each packets contains the ... addresses, as well as other information needed for routing. The packets may take different paths to reach their des and they may be transmitted out of order or delayed du network congestion.

Advantages

- Efficient use of bandwidth :- Packet switching is efficient bec bandwidth is shared among multiple users and resources ar allocated only when data needs to be transmitted.
- Flexible :- Packet switching is flexible and can handle a range of data rates and packet sizes.

Disadvantages

- Higher latency :- Packet switching has higher latency th circuit switching because packets must be routed through multiple nodes, which can cause delay.
- Limited Qos :- Packet switching provides limited Qos gu meaning that different types of traffic may be treated eq

Types of Channel Allocation Strategies

1. Fixed Channel Allocation (FCA) :-

Fixed Channel Allocation is a strategy in which fixed number channels or voice channels are allocated to the cells. Once th channels are allocated to the specific cells then they cannot Changed. In FCA channels are allocated in a manner that maximum frequency reuse.

2. Dynamic channel Allocation :-

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

Explain classful and classless addressing in IP addressing. Give an example for each.

Classful Addressing :-

In Classful addressing, IP addresses are divided into predifined classes (A, B, C, D and E) each with a fixed network and host portion length. Here is an example:

Class A addresses have an 8-bit network portion and a 24-bit host portion

Example : 10.0.0.1

Class B addresses have a 16 bit network portion and a 16-bit host portion

Example : 172.16.0.1

Class C addresses have a 24-bit network portion and a 8-bit host portion.

Example : 192.168.0.1

Class D addresses are used for multicasting purposes.

Example : 224.0.0.1

Class E addresses are reseaved for experimental purposes

Example : 240.0.0.1

Classful addressing the class of an IP address is determined by the range of the first octet. The network portion length is fixed based on the class, and the remaining bits represent the host portion.

Classless Addressing :-

Classless Addressing also known as Classless Inter-Domain Routing (CIDR) is a more flexible approach to IP addressing that allows for variable-length subnet masks.

Here is an example

IP addresses : 192.168.1.10

Subnet mask : 255.255.255.0

In classless addressing the subnet mask is represented in the form of a network prefix length. The network prefix is determined by the number of significant bits in the network position.

In this example the subnet mask 255.255.255.0 has 24 bits set to 1 (in binary) indicating that the first 24 bits represent the network portion, and the remaining 8 bits represent the host portion. Therefore, the IP address 192.168.1.10 with the subnet mask 255.255.255.0 can be represented as 192.168.1.10/24.

In classless addressing the network prefix length can be allowing for more efficient use of IP address and subnetting which enables the division of IP networks into smaller subnets.

Overall classfull addressing has fixed network and host portion length based on the class, while classless addressing allows for variable subnet mask providing more flexibility in address allocation and subnet

Q9 An organization is granted the block 130.56.0.0/16 The administrator wants to create 1024 subnets.

a) Find the number of addresses in each subnet.

b) Find the subnet prefix

c) Find the first and the last address in the first subn

d) Find the first and the last address with an example for each.

① $2^n = 1024$

Therefore $n = 10$

The address is here is a class B

So, the default mask is /16. 10 bits are necessary for subnets and hence the correct subnet is /(16+10) = /26.

In the format of dotted decimal format, it shall be 192 and therefore, the subnet mask will be 255.255.255.192.

) The rest of the bits must be used for the addressed i.e. there will be 32 - 26 = 6 bits available for the address component.

So, a total of $2^6 = 64$ bits shall be available. Also 2 bits per subnet cannot be allocated and subnet mask will be able to maintain 62 valid addresses.

First address in subnet 1 = 130.56.0.1

Last address is subnet 1 = 130.56.0.62

The first address can be estimated by Anding the addresses 130.56.0.0 with the subnet mask /26 like below:

10000010 00111000 00000000 00000000 (130.56.0.0

This address can not be allocated so we will consider the next address:

10000010 00111000 00000000 00000001 (130.56.0.1)

In similar manner the last address that can be allocated before the broadcast address will be 130.56.0.62

(4) First address in the 1024 subnet = 130.56.252.1

Last address in 1024 subnet = 130.56.255.254

Total number of addresses

Q/o Explain any three routing algorithms with an example for each.

Ans There are three commonly used routing algorithms with an example

1. Distance Vector Routing Algorithms :-

The distance vector routing algorithms is a distributed routing algorithms where routers exchanged information about their directly connected neighbours. Each router maintains a routing table with the distance (cost) to reach various network destinations. Examples of distance vector routing protocols :-

Eg Let's consider a network with three routers A, B and C

A ---2--- B ---3--- C

- Each router starts with an initial routing table where the cost to reach its directly connected neighbour is known.
- Router A updates its routing table with the cost to reach
- Router B receives the update from A and updates its routing ta
- Router B then updates its routing table with the cost to re

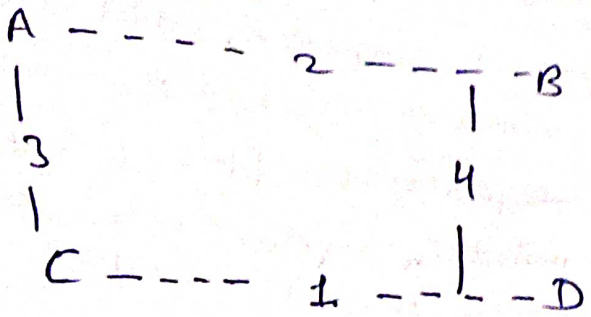
2. Link State Routing Algorithm :-

The link state Routing algorithm is a global routing algorithm where each router floods its link state information throughout the network. Each router constructs a complete map of the network and computes the shortest path to reach each destination

(Do)

algorithms like Dijkstra's algorithm.

Example:- Consider a network with four routers A, B, C, D



Each router collects information about its directly-connected links and their states.

Router A floods its link-state information throughout the network, indicating the cost of its links.

Routers B, C and D receive the link-state information and construction a complete network map.

Using Dijkstra's algorithm each router computes the shortest path to reach each destination.

Border Gateway Protocol :-

Border Gateway Protocol (BGP) is an exterior Gateway Protocol used for routing b/w autonomous system (AS) on the internet. BGP focuses on path attribute and policies to determine the best path for routing traffic b/w autonomous systems. BGP allows routers in different autonomous systems to exchange routing information and make routing decisions based on policies defined by network administrators.

→ Let's Consider two autonomous systems AS1 and AS2 connect through Router R_1 & R_2

AS1 ---- R_1 ---- R_2 ---- AS2

Routers R_1 & R_2 exchange routing information using BGP. R_1 advertise its routes and associated path attributes to R_2. R_2 receives the route updates from R_1 and applies policies to determine the best path to reach destinations in AS1.

Q11 Explain Congestion Control algorithms and give an example for each.

Ans Congestion Control algorithms are employed in computer networks to manage and prevent congestion, which occurs when the demand for network resources exceeds the available capacity. These algorithms aim to regulate the flow of data to prevent network congestion and maintain optimal network performance. Here are three well-known congestion control algorithms, along with an example for each:

1. TCP Congestion Control :-

TCP (Transmission Control Protocol) is a widely used transport layer protocol that implements congestion control to ensure liable and efficient data transmission. TCP Congestion Control algorithms adjust the transmission rate based on network conditions, aiming to avoid congestion and maintain network stability. One popular TCP congestion control algorithm is :

- TCP Reno :- TCP Reno utilizes a combination of slow start, congestion avoidance and fast retransmit/recovery mechanisms. It begins by slowly increasing the transmission rate until congestion is detected (e.g. through packet loss). Upon congestion detection, it reduces the transmission rate and dynamically adjusts its congestion window size to alleviate congestion. TCP Reno is implemented TCP/IP stacks and is commonly used in the Internet.

2. Random Early Detection (RED) :-

RED is an active queue management (AQM) algorithm used in the routers to manage congestion in packet-switched networks.

Instead of allowing the network buffer reaches its maximum capacity, the delay in signaling congestion to the sender. RED uses configurable parameters, such as minimum and maximum thresholds, to control the probability of packet discards. This mechanism helps prevent network congestion and avoids global synchronization of TCP flows.

Explicit Congestion Notification (ECN):

ECN is a congestion control mechanism that operates at the network layer. It provides early notification of network congestion to both endpoints of a communication session. ECN-enabled routers mark packets with an ECN bit in the IP header when congestion is detected. The endpoints can respond by reducing their transmission rate to alleviate congestion. ECN allows for a more proactive and responsive congestion control mechanism compared to relying solely on packet drops. It is used in conjunction with TCP and can be deployed in combination with other congestion control algorithms.

These are just a few examples of congestion control algorithms used in computer networks. Each algorithm employs different techniques to regulate network traffic and prevent congestion. The selection of the appropriate algorithm depends on factors such as network infrastructure, traffic characteristics, and specific requirements of the application or network environment.