Q1. Mention the name of different framing techniques. Differentiate between bit stuffing and byte stuffing methods.

There are mainly three types of framing approaches:

- Byte-Oriented Framing
- Bit-Oriented Framing
- Flag Bytes-Oriented Framing

Bit stuffing and byte stuffing are two different methods used for data transparency in framing. The differences between bit stuffing and byte stuffing methods show in below:

Criteria	Bit Stuffing	Byte Stuffing
Purpose	To avoid the occurrence of a control character	To ensure special characters are not interpreted as data
Technique	An extra bit (0) is added after a certain pattern of bits	An escape character is added before a special byte
Implementation	Bit stuffing is done at the bit level	Byte stuffing is done at the byte level
Example	Adding an extra 0 after every 5 consecutive 1s in a data stream	Adding an escape character before an end-of-message byte to indicate that it is not a data byte
Advantages	Bit stuffing is efficient in terms of the amount of overhead it adds to the data stream	Byte stuffing is simple and easy to implement
Disadvantages	Bit stuffing may not be suitable for all data transmission scenarios	Byte stuffing may increase the length of the data stream and require additional processing by the receiver

So, the key difference between bit stuffing and byte stuffing is that bit stuffing adds extra bits to the data stream, while byte stuffing adds escape characters before special bytes.

Q2. Which type of error is present in data communication? How these errors can avoided?

There are different types of errors that can occur in data communication, including:

- **Transmission errors:** These errors occur due to noise or interference in the transmission medium, which can cause the transmitted signal to be corrupted or distorted.
- **Reception errors:** These errors occur when the receiver is unable to correctly interpret the transmitted signal, either due to noise or interference or due to incorrect decoding of the signal.
- **Timing errors:** These errors occur when the timing of the transmitted signal is not synchronized with the receiver's clock, which can cause the receiver to misinterpret the data.

- **Protocol errors:** These errors occur when there is a problem with the communication protocol, such as incorrect message format or sequencing.
- **Noise:** Noise is unwanted electrical or electromagnetic interference that can corrupt data signals. Noise can be caused by a variety of factors, such as lightning strikes, power lines, and other electrical equipment.

To avoid these errors, different error control techniques can be used, including:

- **Error detection:** This involves adding redundancy to the transmitted data so that errors can be detected at the receiver. Examples of error detection techniques include checksums, cyclic redundancy check (CRC), and parity checking.
- **Error correction:** This involves adding even more redundancy to the transmitted data so that errors can be corrected at the receiver. Examples of error correction techniques include forward error correction (FEC) and automatic repeat request (ARQ).
- **Synchronization:** This involves ensuring that the timing of the transmitted data is synchronized with the receiver's clock, so that the data can be correctly interpreted.
- **Checksums:** In this technique, a checksum value is calculated and sent along with the data. The receiver then recalculates the checksum value and compares it with the received value to detect errors.
- **Retransmission:** If an error is detected during transmission, the receiver can request that the sender retransmit the data packet.

Overall, a combination of these techniques can be used to ensure reliable and error-free data communication. The specific techniques used depend on the requirements of the system, the nature of the transmission medium, and the types of errors that are likely to occur.

Q3. What types of consequences are faced when the timer value of Stop-and-Wait protocol is set larger or smaller than the optimal value?

The simplest ARQ (**Automatic Repeat Request)** scheme is the stop-and-wait protocol algorithm. The idea of stop-and-wait is straight forward: After transmitting one frame, the sender waits for an acknowledgment (ACK) before transmitting the next frame. If the acknowledgment does not arrive after a certain period of time, the sender times out and retransmits the original frame. The time between sending a packet and receiving its ACK is controlled by a timer, which is set to a specific value.

If the timer value of the Stop-and-Wait protocol is set larger than the optimal value, it can lead to the following consequences:

- **Increased Latency:** Since the sender has to wait longer for the ACK, the overall latency of the transmission increases.
- **Reduced Throughput:** A larger timer value means that the sender can transmit fewer packets per unit time, leading to reduced throughput.

- **Network Congestion:** A larger timer value can lead to increased network congestion, as the sender is transmitting fewer packets, but still occupying network resources.

On the other hand, if the timer value of the Stop-and-Wait protocol is set smaller than the optimal value, it can lead to the following consequences:

- **Increased Error Rate:** A smaller timer value means that the sender is more likely to send packets before the receiver has a chance to process the previous packet, leading to increased errors.
- **Increased Overhead:** A smaller timer value means that the sender is sending more packets per unit time, leading to increased overhead due to additional headers and control information.
- **Network Congestion:** A smaller timer value can also lead to increased network congestion, as the sender is transmitting more packets per unit time, potentially causing network congestion.

Therefore, it is important to set the timer value of the Stop-and-Wait protocol to the optimal value to achieve the best possible performance and avoid these consequences. The optimal value can vary depending on factors such as network bandwidth, latency, and packet size.

Q4. Write down the working principle of Stop-and-Wait Protocol. Does there any inefficiency the Stop-and-Wait protocol suffer? If there is any, how it can be avoided?

The simplest ARQ (**Automatic Repeat Request)** scheme is the stop-and-wait protocol algorithm. The idea of stop-and-wait is straight forward: After transmitting one frame, the sender waits for an acknowledgment (ACK) before transmitting the next frame. If the acknowledgment does not arrive after a certain period of time, the sender times out and retransmits the original frame.

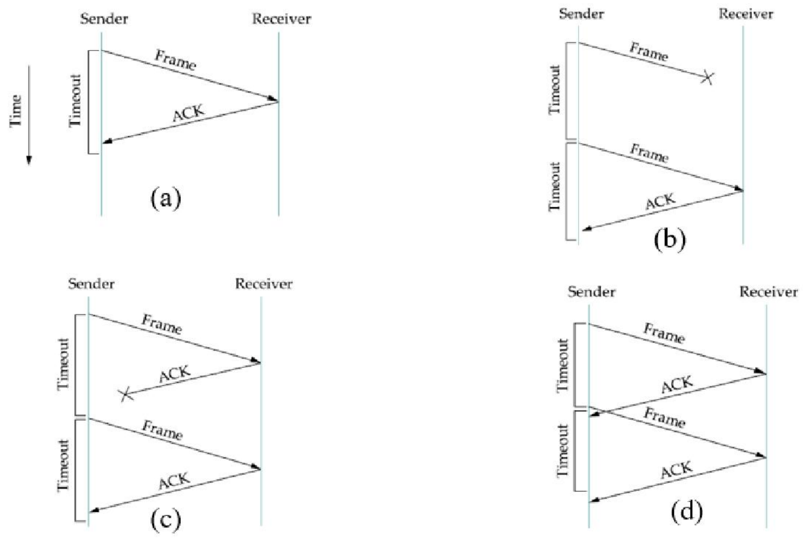


Figure below illustrates four different scenarios that result from this basic algorithm. Figure (a) shows the situation in which the ACK is received before the timer expires, (b) and (c) show the situation in which the original frame and the ACK, respectively, are lost, and (d) shows the situation in which the timeout fires too soon.

<u>Inefficiency</u> - The Stop-and-Wait protocol suffers from inefficiencies when used in high-speed networks or with large data packets. One of the main inefficiencies is that the sender can only transmit one packet at a time, and must wait for the acknowledgement (ACK) before transmitting the next packet. This results in low network utilization and reduced throughput.

Another inefficiency is that the sender must retransmit the entire packet if any error occurs during transmission, even if only a small part of the packet is corrupted. This can waste network bandwidth and increase the probability of collisions in the network.

<u>How it can be avoided</u> -To avoid these inefficiencies, various modifications to the Stop-and-Wait protocol have been proposed. The sliding window protocol allows the sender to send multiple frames before receiving ACKs for each frame. The receiver maintains a window of frames that it is expecting to receive, and sends an ACK for all frames that it receives within the window. The sender maintains a window of frames that it has sent but has not yet received ACKs for. As the sender receives ACKs for frames within the window, it slides the window forward and sends additional frames. This results in higher network throughput and efficiency.

Another modification is the Selective Repeat protocol, which allows the receiver to selectively retransmit only the packets that were not successfully received, instead of requesting the entire packet to be retransmitted. This reduces the amount of network bandwidth wasted on retransmissions and reduces the probability of collisions.

Other techniques such as pipelining, Go-Back-N, and buffering can also be used to improve the efficiency of data transmission and reduce the impact of transmission errors. These techniques allow for multiple packets to be transmitted and received simultaneously, and can recover from errors without requiring the entire packet to be retransmitted.

Q5. Differentiate between stochastic and deterministic medium access strategies. Which one is better for low traffic condition?

Stochastic and deterministic medium access strategies are two different ways of controlling access to a shared communication medium in a network. The main differences between them are as follows:

1. Deterministic medium access strategies allocate the communication medium to nodes in a predetermined order, while stochastic medium access strategies do not follow a fixed order and rely on random access.
2. Deterministic medium access strategies provide guaranteed access to the communication medium to all nodes in the network, while stochastic medium access strategies do not provide such guarantees and can result in collisions and contention.
3. Deterministic medium access strategies require more complex coordination and scheduling mechanisms, while stochastic medium access strategies are simpler and more flexible.

In low traffic conditions, stochastic medium access strategies are generally better as they provide more flexibility and simplicity, which can result in higher efficiency and lower overhead. For example, the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol is a stochastic medium access strategy commonly used in Ethernet networks. It relies on random access and collision detection to control access to the communication medium.

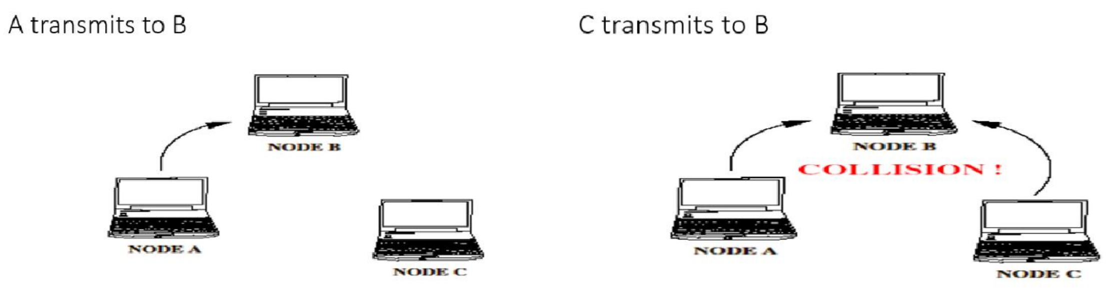
However, in high traffic conditions, deterministic medium access strategies may be more appropriate as they can provide better control and avoid collisions and contention. For example, the Time Division Multiple Access (TDMA) protocol is a deterministic medium access strategy commonly used in cellular networks. It allocates specific time slots to each node for transmitting and receiving data, ensuring that there are no collisions or contention for the communication medium.

Q6. Write down the characteristic of hidden terminal problem. How a hidden terminal problem can be avoided?

Hidden Terminal Problem - The hidden terminal problem is a phenomenon that occurs in wireless communication when two or more wireless nodes cannot hear each other but can hear a third node. This can result in collisions when the nodes transmit data simultaneously, leading to a decrease in network efficiency and an increase in packet loss.

- Appears when two nodes are unaware of each other’s attempt to send data to a third node
- “Unaware of each other” means “out of each other's signal range”
- The result is data collision at the receiving node
- The problem exists in contention-based protocols

For example, consider three wireless nodes A, B, and C. Node A is within range of nodes B and C, while nodes B and C are out of range of each other. If nodes B and C transmit data simultaneously to node A, node A will be unable to decode the data correctly, resulting in a packet loss. This is because node B and node C cannot detect each other's transmission due to being out of range, leading to interference at node A.



Solution- The RTS-CTS (Request-to-Send/Clear-to-Send) handshaking process is a technique used to address the hidden terminal problem in wireless LAN communication. This technique uses two frames, the RTS frame, and the CTS frame, to coordinate the transmission of data between wireless nodes.

- Using a handshake protocol would prevent collision
- The protocol is used to "reserve" the comm. channel
  - RTS = (R)eady (T)o (S)end
  - CTS = (C)lear (T)o (S)end
- RTS and CTS are broadcast-type messages
- Still not a bullet-proof solution!

The RTS-CTS handshaking process also helps to reduce the likelihood of collisions due to other factors, such as channel noise or interference from other sources, by reserving the channel for the duration of the data transmission. This technique ensures that the receiver is ready to receive data and that no other nodes are transmitting data simultaneously, leading to more efficient and reliable wireless LAN communication.

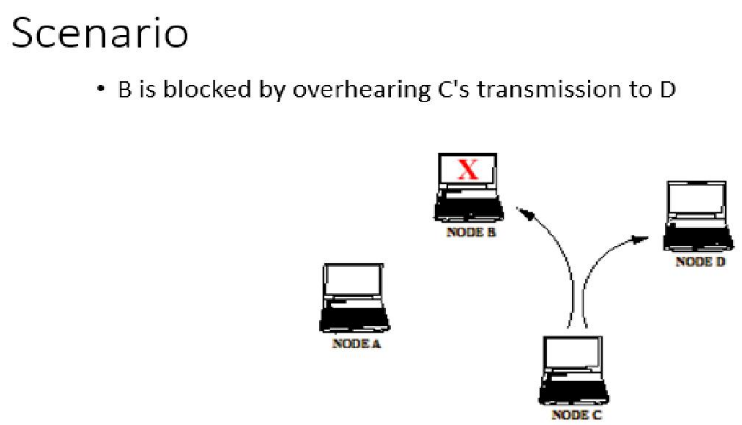
Q7. Show that exposed terminal problem is the result of using RTS-CTS handshaking (avoiding for hidden terminal problem) process.

The exposed terminal problem is another phenomenon that can occur in wireless networks, and it is the opposite of the hidden terminal problem. In this case, a wireless node is prevented from transmitting data even though there is no other transmission in progress, due to the transmission of another node within its range.

The exposed terminal problem can occur when using the Request-to-Send/Clear-to-Send (RTS/CTS) handshaking process to avoid the hidden terminal problem. This is because the RTS/CTS process allows a node to reserve the medium for a specified period of time, even if other nodes are out of range and not transmitting data.

Exposed Terminal Problem

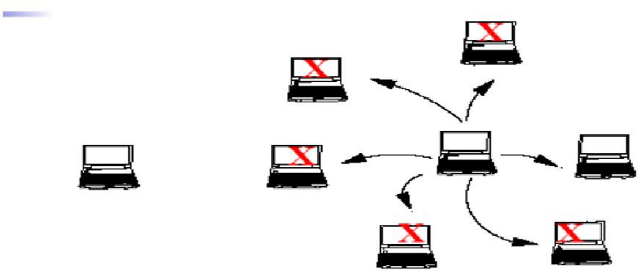
- Overhearing a data transmission from a neighboring node causes other neighboring nodes to stall their transmissions
- The exposed node is within the radio range of the transmitter
- but at the same time out of receiver's radio range



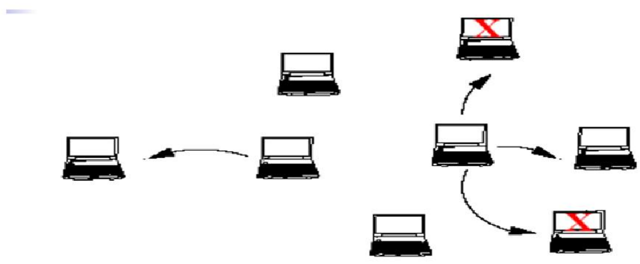
Solution: Directional Antennas

- Omni-directional antennas increase the probability of having "exposed" nodes
    - Consequence: lowers overall throughput and network availability
- Solution 1: Usage of directional antennas instead of omni-directional => Provide spatial isolation
- Solution 2: Separate data and control channels

Scenario: Omni-directional Antenna



Scenario: Directional Antenna



To avoid the exposed terminal problem, various techniques can be used, such as:

- **Virtual Carrier Sensing:** This technique involves using information from neighboring nodes to determine if the medium is in use, even if the node itself is out of range of the transmission. This allows nodes to avoid unnecessary backoffs and improve the efficiency of the network.
- **Frame Bursting:** This technique involves allowing nodes to transmit multiple frames back-to-back without the need for RTS/CTS handshaking, thus reducing the overhead and improving the efficiency of the network.
- **Dynamic Sensing Threshold:** This technique involves adjusting the sensing threshold of each node based on the signal strength of neighboring nodes, thus allowing nodes to detect transmissions from neighboring nodes more accurately and avoid unnecessary backoffs.

Q8. What is the function of backoff in CSMA based MAC protocol? Why the backoff is applied in different location in CSMA/CD and CSMA/CA protocol?

The backoff mechanism is used in Carrier Sense Multiple Access (CSMA) based Medium Access Control (MAC) protocols to avoid collisions and improve the efficiency of the network.

In CSMA/CD (Collision Detection) protocol, backoff is applied after a collision occurs, and before a retransmission attempt. When a collision is detected, the transmitting node stops sending and waits for a random amount of time before attempting to retransmit. The random wait time is determined by the backoff algorithm and helps to reduce the probability of another collision occurring.

In CSMA/CA (Collision Avoidance) protocol, backoff is applied before a transmission attempt. When a node wants to transmit data, it senses the medium to check if it is busy. If the medium is busy, the node waits for a random amount of time before attempting to transmit. The random wait time is determined by the backoff algorithm and helps to avoid collisions by allowing other nodes to finish their transmissions and reducing the probability of overlapping transmissions.

The backoff algorithm used in CSMA protocols typically increases the random wait time after each unsuccessful transmission attempt, to reduce the probability of repeated collisions. The backoff algorithm may also use a contention window, which is a range of possible wait times, to ensure that nodes do not all transmit simultaneously after waiting the same amount of time.

In summary, the backoff mechanism is an important component of CSMA-based MAC protocols that helps to avoid collisions and improve the efficiency of the network by introducing a random delay before transmission attempts. The specific location and timing of the backoff in CSMA/CD and CSMA/CA protocols depend on the protocol design and the requirements of the network.

Q9. Show the superiority of Asynchronous Transfer Mode (ATM) over Time Division Multiplexing (TDM) in delay time minimization.

- ATM and TDM are both digital multiplexing techniques used to transmit data over a shared medium. However, there are some key differences between the two technologies that make ATM superior in terms of delay time minimization.

- **Fixed-length cells:** ATM cells are fixed-length, 53-byte units. This means that the transmission time of each cell is always the same, regardless of the size of the data being transmitted. This is in contrast to TDM, where the transmission time of each frame varies depending on the size of the data being transmitted.
- **Virtual circuits:** ATM uses virtual circuits to establish connections between devices. This means that data is transmitted in a predictable manner, regardless of the traffic conditions on the network. This is in contrast to TDM, where data is transmitted in a contention-based manner, which can lead to variable delays.
- **Congestion control:** ATM has a built-in congestion control mechanism that helps to prevent data from being lost due to congestion. This mechanism is not present in TDM, which can lead to data loss if the network becomes congested.

As a result of these differences, ATM is able to minimize delay time more effectively than TDM. This makes ATM a better choice for applications that require low latency, such as voice and video.

Here is a table that summarizes the key differences between ATM and TDM:

Feature	ATM	TDM
Cell size	Fixed-length	Variable-length
Virtual circuits	Yes	No
Congestion control	Yes	No
Latency	Low	High

Overall, ATM is a superior technology to TDM in terms of delay time minimization. This makes ATM a better choice for applications that require low latency, such as voice and video.

Q10. For the variety of advantageous features, ATM uses fixed and small sized packet for data packet transmission. Discuss about those features.

Asynchronous Transfer Mode (ATM) is a packet-oriented (also connection oriented) transfer mode which allows multiple logical connections to be multiplexed over a single physical interface that uses fixed-length cells to transmit data over a high-speed network. ATM cells are 53 bytes long, and they are all the same size, regardless of the type of data being transmitted. This has a number of advantages, including:

Why fixed and small data packet?

- It is easy to build hardware routers to handle short, fixed-length cells. Variable length IP packets have to be routed by software, which is slower process.
- Hardware can copy one incoming cell to multiple output lines easily which is suitable for TV broadcasting.
- Small cell does not block a line for long which ensure QoS.
- ATM can provide a variety of security features, such as encryption and authentication.
- ATM has a built-in congestion control mechanism that helps to prevent data from being lost due to congestion.
- Fixed-length cells also improve the reliability of the network. This is because the cells are less likely to be corrupted in transit.

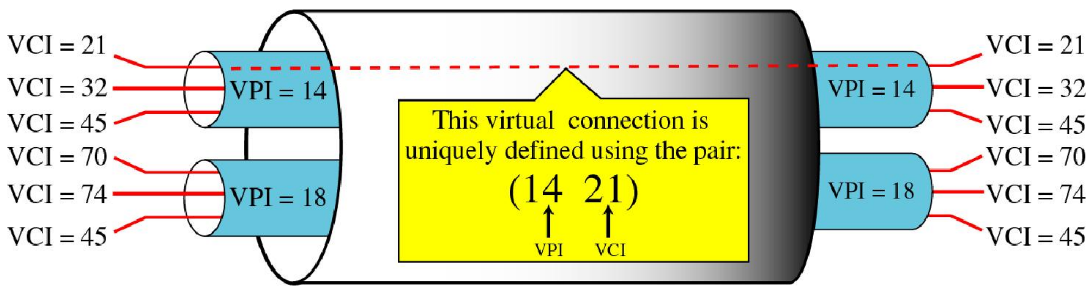
Overall, ATM is a versatile and reliable technology that is well-suited for high-speed networks. The use of fixed-length cells is one of the key factors that contributes to the performance and reliability of ATM networks.

Q11. With a clear figure, show the formation of an identifier from virtual path identifier and virtual circuit identifier.

In ATM, each connection is identified by a combination of VPI and VCI. VPI identifies the virtual path, which is a logical connection between two endpoints in the network, while VCI identifies the virtual circuit, which is a logical connection between two endpoints within the virtual path.

To form an identifier, VPI and VCI are concatenated together. The most significant bits of the identifier correspond to VPI, while the least significant bits correspond to VCI. The length of the identifier depends on the values of VPI and VCI, and can range from 16 to 32 bits.

Each connection is identified by a Virtual Path Identifier (VPI)/Virtual Circuit Identifier (VCI) combination, which can be found in the header of all ATM cells carrying information about that specific connection. A group of VC links, identified by a common value of VPI.



The VPI and VCI are an important part of the ATM protocol. They allow cells to be routed through the ATM network quickly and efficiently.

Q12. The Application Adaptation Layer (AAL) is able to support various types of services such as voice, video or data. With necessary figure, verify the above statement.

The use of ATM creates the need for an adaptation layer to support information transfer protocols not based on ATM. For example, PCM voice is an application that produces a stream of bits from a voice signal. To employ this application over ATM, it is necessary to assemble PCM bits into cells for transmission and to read them out on reception in such a way to produce a smooth, constant flow of bits to the receiver.

The AAL is divided into two sublayers: the Convergence Sublayer (CS) and the Segmentation and Reassembly (SAR) Sublayer. The CS sublayer is responsible for mapping the upper layer protocols to the AAL, while the SAR sublayer is responsible for breaking up large data units into smaller ATM cells for transmission, and then reassembling the cells at the receiving end.

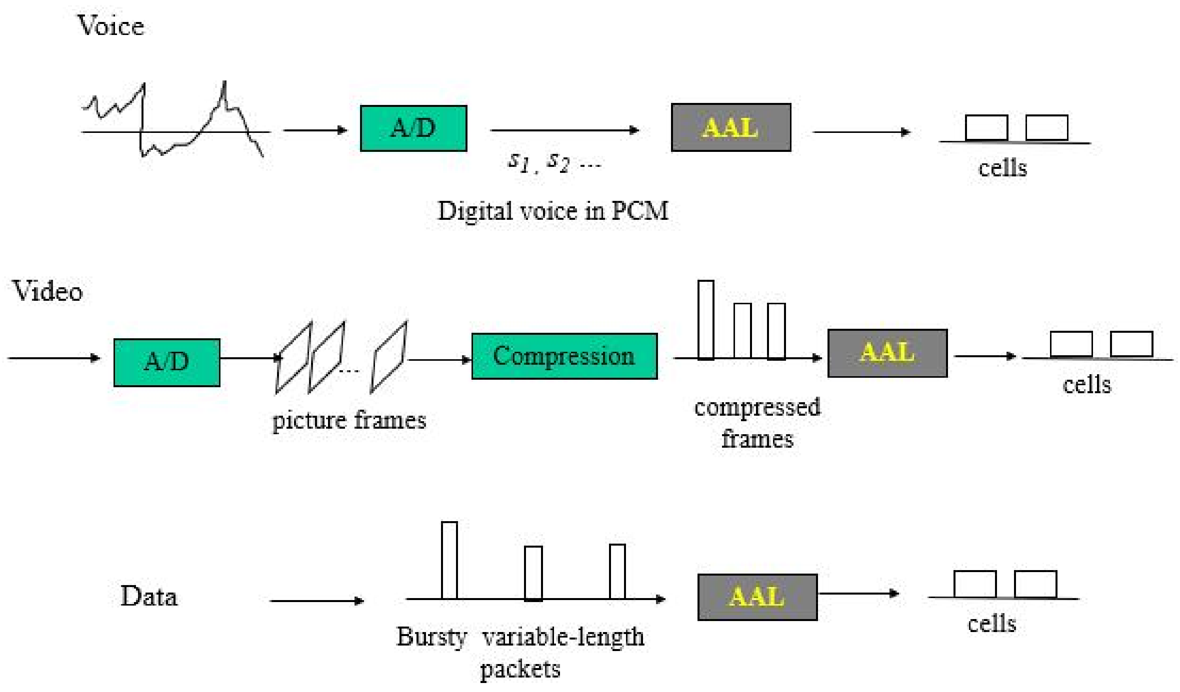


Fig: Application Adaption Layer is able to support various types of services such as voice, video or data.

- Supports variable bit rate (VBR) services such as compressed voice and video. AAL provides variable cell delay and higher cell loss tolerance.
- Supports real-time, constant bit rate (CBR) services such as voice and video. AAL provides fixed cell delay and low cell loss.
- Supports data services such as file transfer and email. AAL provides variable cell delay and moderate cell loss tolerance.

The AAL is a versatile layer that can support a variety of services. It is an important part of the ATM protocol stack and plays a key role in the delivery of data, voice, and video traffic.

Q13. Draw the Asynchronous Transfer Mode (ATM) data cell format; and therefore, give some idea about GFC, PT and C data field.

- **GFC (Generic Flow Control):** A 4-bit field used for flow control and congestion management in the ATM network. It is used to identify the source of the cell and to provide feedback on network congestion.
- **VPI (Virtual Path Identifier):** An 8-bit field used to identify the virtual path over which the cell is transmitted.
- **VCI (Virtual Circuit Identifier):** A 16-bit field used to identify the virtual circuit over which the cell is transmitted.
- **PT (Payload Type):** A 3-bit field used to indicate the type of information carried in the cell, such as user data, signaling, or management information.
- **CLP (Cell Loss Priority):** A 1-bit field used to indicate the priority of the cell. If the network becomes congested, cells with CLP=1 may be discarded first.
- **HEC (Header Error Control):** An 8-bit field used to detect errors in the cell header.

- **Payload Data:** A variable-length field containing the actual data being transmitted, up to a maximum of 48 bytes.

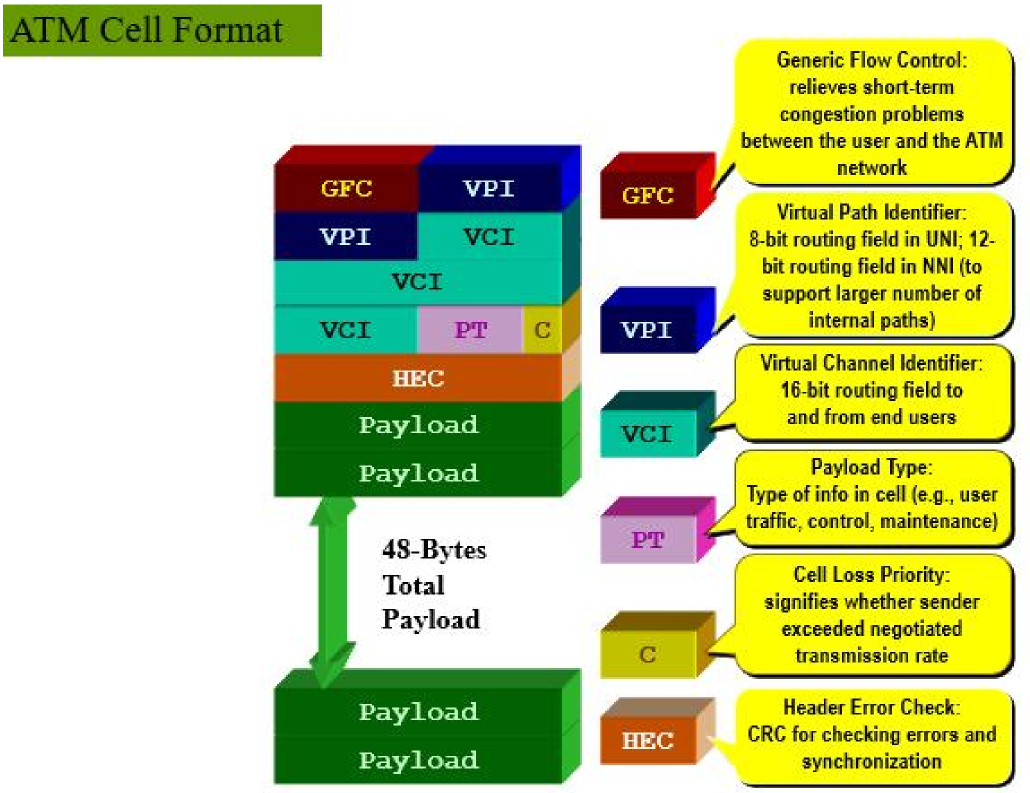


Fig: ATM Cell Format

The GFC, VPI, VCI, PT, and CLP fields are all fixed in length. The HEC field is variable in length, but it is always 16 bits long.

The ATM cell format is designed to be efficient and reliable. The fixed-length cells make it easy to switch data between different networks and devices. The HEC field helps to ensure that the cell header is not corrupted in transit. The GFC, VPI, VCI, and PT fields provide a variety of features that make ATM a versatile and reliable technology.

Q14. State the function of Packet Assembler/Dissembler (PAD) module in X.25 standard in delivering nonstandard data format.

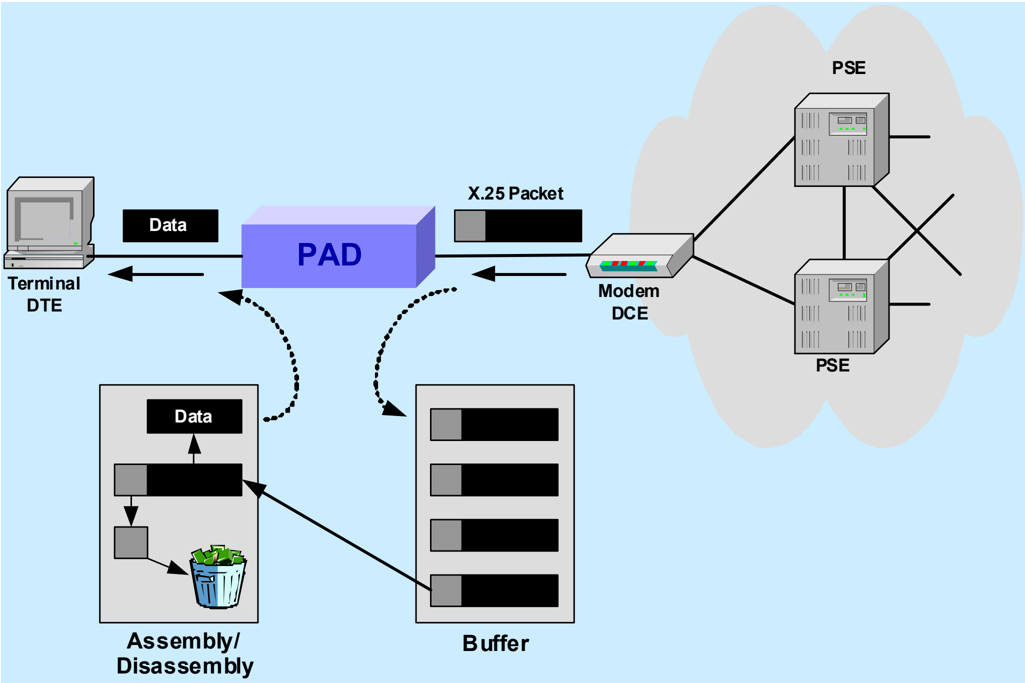
Packet Assembler / Disassembler (PAD) acts as intermediary device between DTE and DCE which performs three functions:

- Buffering to store data until a device is ready to process it
- Packet Assembly
- Packet Disassembly

The non X.25 network can be interfaced with X.25 network by Packet Assembler/Dissembler (PAD). The PAD protocol reads the non-standard data then translates them into X.25 packets, which then routed to their destinations on the X.25 network. The process is reversed when an X.25 station sends data to the nonstandard network.

Packet Assembling: The PAD assembles data packets from the incoming data stream. The data stream may consist of data in various formats, such as characters, blocks, or frames. The PAD converts these data formats into fixed-length packets that can be transmitted over the X.25 network.

Packet Disassembling: The PAD disassembles data packets from the incoming X.25 packets. The incoming packets may have fixed or variable length. The PAD converts these packets into the original data format before delivering it to the destination device.

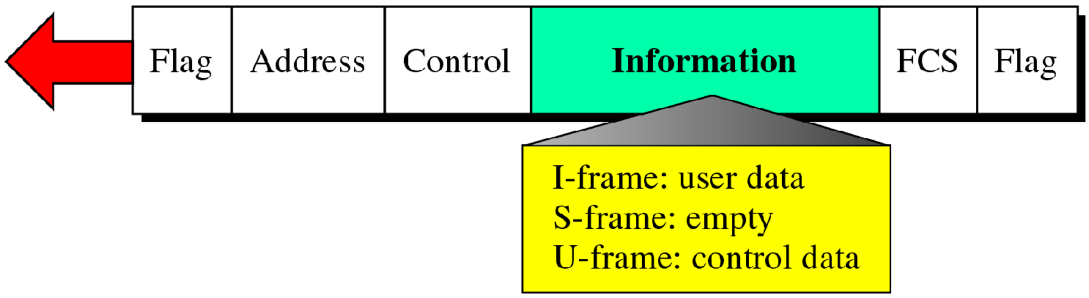


The PAD module is an important part of the X.25 standard. It allows users to transmit data in a nonstandard format over an X.25 network. The PAD module also provides a number of other features that improve the reliability and performance of X.25 networks.

Q15. In Link Access Procedure, Balanced (LAPB), how many types of data frames are conventionally used? Explain them clearly.

In Link Access Procedure, Balanced (LAPB), there are three types of data frames that are conventionally used:

- Three types of frames
  - **I-Frames (Information Frames):** used to send user data.
  - **S-Frames (Supervisory Frames):** Controls flow of data (using acknowledgement for received frames which includes the sequence number of the received frame)
  - **U-Frames (Unnumbered Frames):** The Unnumbered Frames are used by a terminal to report an error condition which is not recoverable by retransmitting the identical frame, then to initiate the link-resetting procedure.



Q16. Draw the Packet Layer Protocol (PLP) frame format. Explain the X.25 call setup procedure.

Packet Layer Protocol (PLP) is the X.25 network layer protocol like the third layer of OSI model. This layer specifies how packet are formed and exchanged using virtual circuits.

PLP Frame Format:

GFI	LCI	PTI	User Data

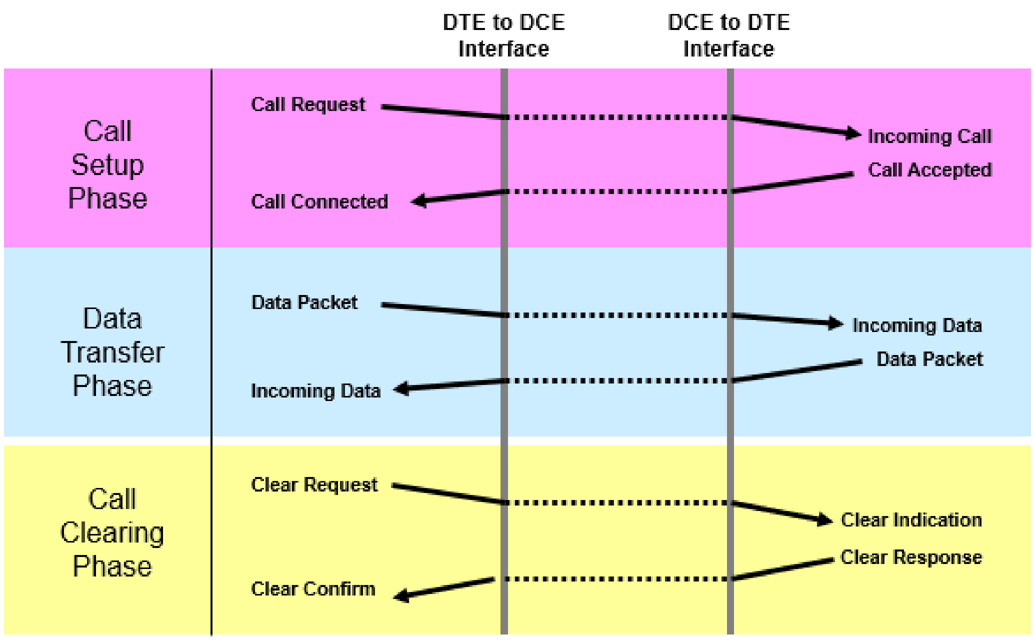
General Format Indicator: (4 bits) Identifies packet parameters, such as whether the packet carries user data or control information, what kind of windowing is being used, and whether delivery confirmation is required.

Logical Channel Identifier: (12 bits) Identifies the virtual circuit (1-4095) across the local DTE to DCE interface. This field consists of a 4-bit Logical Channel Group Number (LCGN) and an 8-bit Logical Channel Number (LCN)

Packet Type Identifier: (8 bits) It specifies the function of the packet (one of 17 different packet types)

User Data: varies is size but typically 128 octets.

X.25 Call Setup procedure:



Q17. Show the superiority of frame relay technology over other conventional MAC protocols. Discuss the various types of frame relay circuits.

Frame relay is a type of packet-switched data networking technology that uses a connection-oriented approach to transferring data between nodes. It is a popular choice for enterprise networks because it offers a number of advantages over other conventional MAC protocols, including:

- **High performance:** Frame relay is a very efficient way to transfer data. It uses a fixed-length frame format, which makes it easy to switch data between different networks and devices.
- **Reliable:** Frame relay is a very reliable technology. It uses a variety of error detection and correction mechanisms to ensure that data is not corrupted in transit.
- **Scalable:** Frame relay is a very scalable technology. It can be easily expanded to accommodate the growing needs of an enterprise network.
- **Cost-effective:** Frame relay is a very cost-effective technology. It is a good choice for enterprises that need to connect multiple sites or departments without breaking the bank.

There are two main types of frame relay circuits: permanent virtual circuits (PVCs) and switched virtual circuits (SVCs).

- **PVCs:** PVCs are dedicated connections between two points. They are always available and do not require any setup time.
- **SVCs:** SVCs are on-demand connections between two points. They are created when needed and torn down when they are no longer needed.

PVCs are a good choice for applications that require a high degree of reliability and predictability. SVCs are a good choice for applications that do not require a high degree of reliability or predictability.

Overall, frame relay is a versatile and reliable technology that is well-suited for a variety of enterprise networking needs. It offers a number of advantages over other conventional MAC protocols, including high performance, reliability, scalability, and cost-effectiveness.

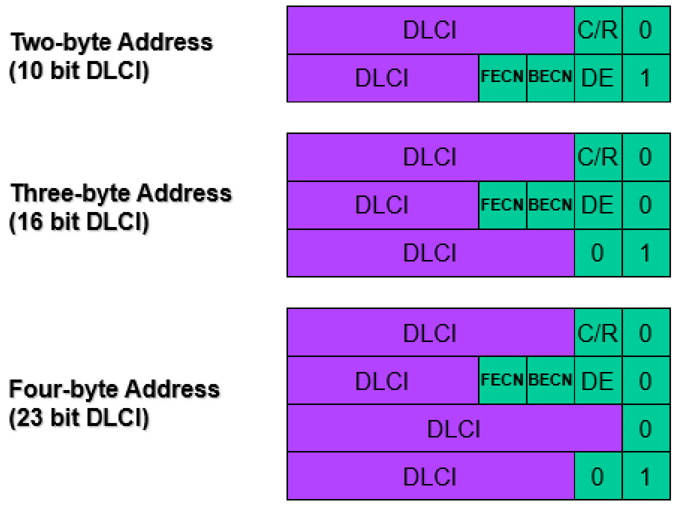
Q18. Using some necessary figures, show the usage of extended addressing process in frame relay technology.

Frame Relay uses Data Link Connection Identifiers (DLCIs) to identify connections between endpoints on the network. DLCIs are used to route data to the correct endpoint, similar to how IP addresses are used in the Internet.

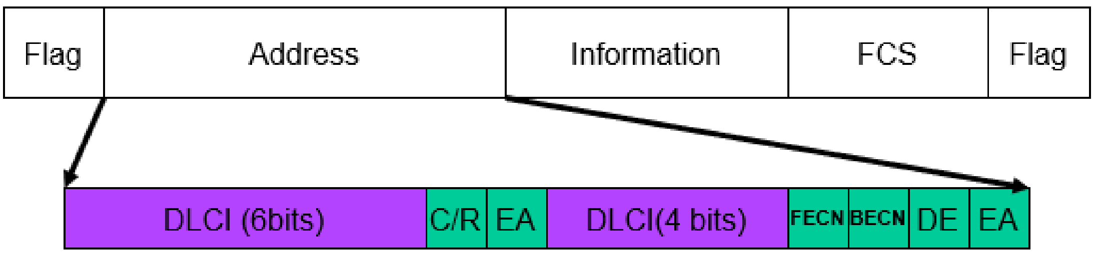
- To increase the number of virtual circuits the DLCI can be expanded from 10 bits to 16 bits and 23 bits

- The EA field is set to 0 to indicate that additional address bytes are present. The last address byte will have a 1 in the EA field.

Three Address Formats



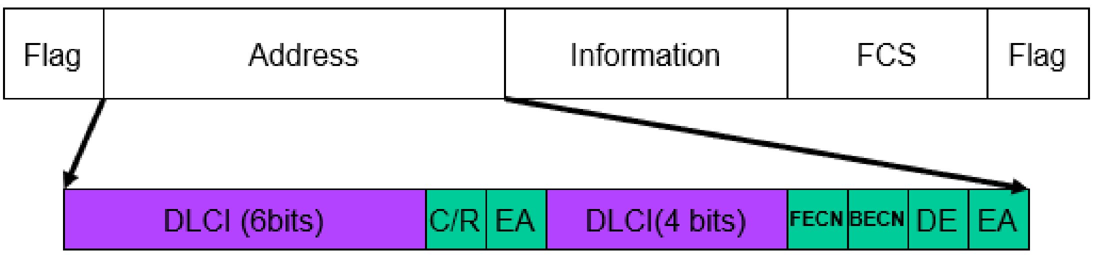
Flag Field. The flag is used to perform high-level data link synchronization which indicates the beginning and end of the frame with the unique pattern 01111110. To ensure that the 01111110 pattern does not appear somewhere inside the frame, bit stuffing and destuffing procedures are used.



<u>DLCI:</u> (10 bits) Data Link Connection Identifier is used to identify the Virtual Circuit number. In TCP/IP network each interface is given a DLCI number along with IP address.

<u>C/R:</u> (1 bit) Provided for up layers to determine commands and responses

<u>EA:</u> (1 bit) Extension Bit determines if this byte is last byte of address (0=more, 1=last). The last EA filed have reverse format like 1= more, 0 = last.



FECN: (1 bit) Forward Explicit Congestion Notification indicates congestion in the direction the frame is traveling. This is sensed by the receiver.

BECN: (1 bit) Backward Explicit Congestion Notification indicates congestion in the opposite direction the frame is traveling

DE: (1 bit) Discard Eligibility (priority of a frame) indicates that this frame should be discarded first in the event of congestion.

Q19. Make a clear comparison between frame relay and X.25 MAC technologies.

Comparison of X.25 and Frame Relay:

	X.25	**Frame Relay**
Layer 1 Specification	Yes	None
Layer 2 Protocol Family	HDLC	HDLC
Layer 3 Support	PLP	None
Error Correction	Node to Node	None
Propagation Delay	High	Low
Ease of Implementation	Difficult	Easy
Good for Interactive Applications	Too Slow	Yes
Good for Voice	No	Yes
Good for LAN File Transfer	Slow	Yes

The main differences between frame relay and X.25 packet switching are

1. There is no link-by-link flow control or error control. These are the responsibility of the user's terminals.
2. Switching of logical connections takes place at layer 2 instead of layer-3, thus eliminating one layer of processing.
3. Call-control signaling is carried out on a logical connection separate from the data. A a result, intermediate nodes do not need to process call-control message on basis of individual connections.

Q20. What do you understand by bandwidth of a signal? Show that Pulse Code Modulation (PCM) is able to reduce the asking bandwidth by sampling process.

Bandwidth is the difference between the highest and lowest frequencies in a signal. It is measured in hertz (Hz). The bandwidth of a signal determines the amount of data that can be transmitted in a given amount of time.

Pulse Code Modulation (PCM) is a digital modulation technique that samples an analog signal at regular intervals and converts the samples into a series of binary numbers. The binary numbers are then transmitted over a digital channel.
PCM is able to reduce the bandwidth of an analog signal by sampling it at a rate that is greater than twice the highest frequency in the signal. This is known as the Nyquist Sampling Theorem.

For example, if an analog signal has a bandwidth of 4 kHz, then it must be sampled at a rate of at least 8 kHz. This means that the PCM signal will have a bandwidth of 8 kHz, which is less than the bandwidth of the original analog signal.

PCM is a very efficient way to transmit analog signals over digital channels. It is used in a variety of applications, including telephony, audio and video recording, and data communications.
Here is an example of how PCM can reduce the bandwidth of an analog signal.

Let's say we have an analog signal with a bandwidth of 4 kHz. This means that the signal can contain frequencies up to 2 kHz. If we sample this signal at a rate of 8 kHz, then we will be able to capture all of the frequencies in the signal.

The PCM signal will have a bandwidth of 8 kHz, which is less than the bandwidth of the original analog signal. This is because the PCM signal only contains the samples of the analog signal, not the original analog signal itself.

The PCM signal can be transmitted over a digital channel, such as a telephone line or a fiber optic cable. The digital channel will have a bandwidth of at least 8 kHz, which is sufficient to transmit the PCM signal.

PCM is a very efficient way to transmit analog signals over digital channels. It is used in a variety of applications, including telephony, audio and video recording, and data communications.

Q21. What is Nyquist sampling rate? What will happen when the sampling rate is below or above the Nyquist sampling rate? Is there any necessity for using a guard band?

Nyquist sampling rate is the minimum sampling rate required to accurately represent a continuous-time signal in its discrete-time form without any aliasing. The Nyquist sampling rate can be determined by the formula: f_s > 2B

sampling rate formula: $f_c = G.B+2B$
where f_s is the sampling rate and B is the bandwidth of the signal.

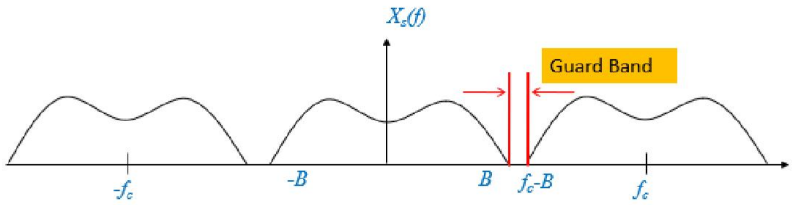


Fig. The condition $f_c \geq 2B$ is called Nyquist sampling rate.

If the sampling rate is below the Nyquist sampling rate, then aliasing occurs, which results in distortion of the original signal. If the sampling rate is above the Nyquist sampling rate, then the signal is oversampled, which means that unnecessary samples are taken, leading to waste of resources.

A guard band is a frequency range reserved for reducing the effects of interference between adjacent channels. It is usually added to the Nyquist rate to prevent aliasing and ensure proper signal reconstruction. The guard band helps to minimize the effects of inter symbol interference (ISI) and crosstalk. The use of a guard band is important for reducing the noise and distortion that can occur due to frequency interference.

Q22. What is signal-to-quantization ratio (SQR)? For the signal at transmitting end is quantized into total N discrete levels with maximum plus-minus signal excursion of P volts, maximum excursion in positive or negative direction is V and the range of quantized samples is A, show that $SQR = 4.8 + 20logN$.

Signal-to-quantization ratio (SQR) is a measure of the quality of the quantization, or digital conversion of an analog signal. It is defined as the ratio of the signal's dynamic range to the quantization noise.

The dynamic range of a signal is the difference between the maximum and minimum values that the signal can take. The quantization noise is the error introduced by the quantization process.

The SQR can be calculated as follows:
SQR = 20 log (dynamic range / quantization noise)

In the case of a signal that is quantized into N discrete levels, the dynamic range is equal to P, the maximum plus-minus signal excursion. The quantization noise is equal to A/2, where A is the range of quantized samples.

Therefore, the SQR can be calculated as follows:
SQR = 20 log(P / (A/2))

This can be simplified to:
SQR = 40 log(P) - 20 log(A)

Since P = V, and A = V/N, the SQR can be calculated as follows:
SQR = 40 log(V) - 20 log(V/N)

This can be simplified to:
SQR = 40 log(V) + 20 log(N)

Finally, since log(10) = 1, the SQR can be calculated as follows:
SQR = 4.8 + 20 log(N)

This equation shows that the SQR is directly proportional to the number of quantization levels. This means that the higher the number of quantization levels, the better the SQR will be.

Q23. A voice signal of highest frequency of 3.5 KHz sampled maintaining a guard band of 250 Hz. After sampling the signal is quantized into 256 levels. Determine sampling rate and bit rate of PCM.

Given:

- Highest frequency of voice signal = 3.5 KHz
- Guard band = 250 Hz
- Quantization levels = 256

To determine the sampling rate and bit rate of PCM, we can use the Nyquist sampling theorem which states that the sampling rate should be at least twice the highest frequency component of the signal.

Nyquist sampling rate = 2 × 3.5 KHz = 7 KHz

However, we need to add the guard band to this value to ensure that no important frequency component is lost due to under sampling.

Sampling rate = Nyquist sampling rate + guard band = 7 KHz + 250 Hz = 7.25 KHz

Now, the number of bits per sample can be calculated using the quantization levels:
Bits per sample = log2(256) = 8

Therefore, the bit rate of PCM can be calculated as:
Bit rate = Sampling rate × bits per sample = 7.25 KHz × 8 = 58 Kbps
Hence, the sampling rate of PCM is 7.25 KHz and the bit rate is 58 Kbps.

Q24. What is function of step size in Delta Modulation (DM)? Why the slop overload distortion is produced in DM? How the slop overload distortion can be avoided?

The step size in delta modulation is the size of the quantization step. It is the amount that the output signal can change in response to a change in the input signal. The step size is important because it determines the accuracy of the reproduction of the input signal. A larger step size will result in more quantization error, while a smaller step size will result in less quantization error.

Slope overload distortion occurs in delta modulation when the step size is too small to accurately represent a change in the input signal. When this happens, the output signal will not be able to keep up with the changes in the input signal, and the result will be a distorted signal.

Slope overload distortion can be avoided by increasing the step size. However, increasing the step size also increases the quantization error. Therefore, it is important to choose a step size that balances accuracy and efficiency.

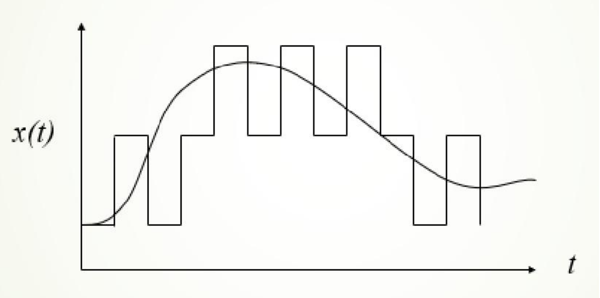


Fig. 21: Output of the demodulator for larger step size

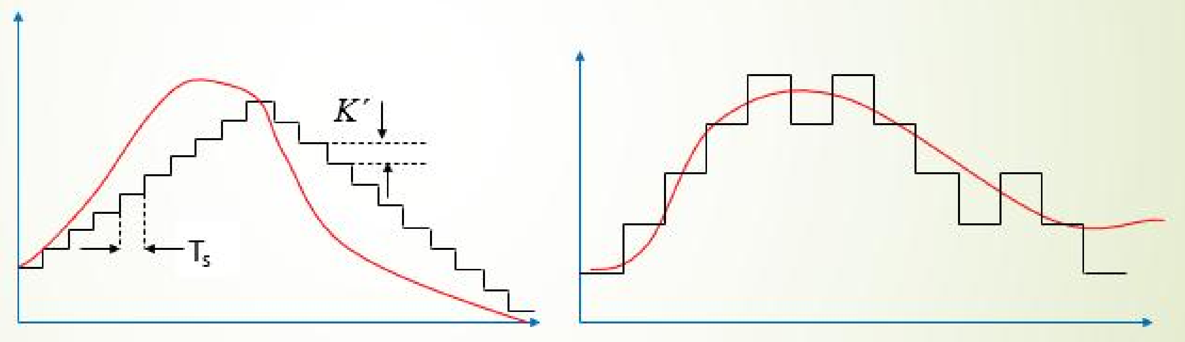


Fig. 22: Output of the demodulator for smaller step size

Fig. 23: Output of the demodulator for optimum step size

Here are some ways to avoid slope overload distortion in delta modulation:

- Use a larger step size.
- Use a higher sampling rate.
- Use adaptive delta modulation.

Adaptive delta modulation is a type of delta modulation that automatically adjusts the step size based on the characteristics of the input signal. This helps to reduce slope overload distortion without sacrificing accuracy.

Q25. Determine the optimum step size for the signal x(t)= 4.5sin(3π15t) considering sampling frequency of 8 KHz.

Answer: The slope of the signal *x(t)*, dx(t)/dt = 4.5 x 3π x 15 cos(3π15t)

The maximum slope is obtained taking cos(3π15t) = 1.

The maximum slope of the signal m_{max}= 4.5 x 3π x 15 = 202.5π. the maximum slope supported by it,

$\tan(\theta) = K/T_s = kf_s = k8000$

Therefore, k_{opt} = 202.5π/8000 = 0.0253 volt

Q26. Why line coding is used in data communication? Can you differentiate between digital data and digital signal?

Line coding is used in data communication to represent digital data as a physical signal that can be transmitted over a communication channel. This is necessary because digital data is represented as a series of binary digits (bits), which can be represented as two different voltage levels or two different states of a light wave. However, the communication channel may not be able to directly transmit these voltage levels or light wave states. For example, a copper wire may not be able to directly transmit a high voltage level, so a line code may be used to represent a high voltage level as a negative voltage level or a positive voltage level.

There are many different line coding schemes, each with its own advantages and disadvantages. Some of the most common line coding schemes include:

- Non-return to zero (NRZ)
- Return to zero (RZ)
- Manchester encoding
- Differential Manchester encoding

Digital data is data that is represented as a series of binary digits (bits). Each bit can be either a 0 or a 1. Digital data can be stored in memory, processed by computers, and transmitted over communication channels.

A digital signal is a physical signal that represents digital data. Digital signals can be electrical signals, optical signals, or acoustic signals. Digital signals are used to transmit digital data over communication channels.

The main difference between digital data and digital signal is that digital data is represented as a series of bits, while digital signal is a physical signal that represents digital data.

Q27. Why alternate mark inversion (AMI) seems to be superior to other line coding methods?

Bipolar Signalling is also called '**Alternate Mark Inversion**' (AMI) which uses three voltage levels (+*V*, 0, –*V*) to represent binary symbols.

There are a few reasons why alternate mark inversion (AMI) is superior to other line coding methods.

First, AMI is a DC-balanced line code, which means that the average DC level of the signal is zero. This is important because it helps to prevent accumulation of DC offset in the signal, which can lead to errors in the received signal.

Second, AMI is a self-clocking line code, which means that the receiver can recover the clock signal from the received signal. This is important because it does not require an external clock signal, which can be expensive and difficult to synchronize.

Third, AMI is a relatively simple line code to implement, which makes it cost-effective.

As a result of these advantages, AMI is a popular line coding method for many applications, including telecommunications and data communications.

Here are some of the advantages of AMI over other line coding methods:

- DC balance: AMI is a DC-balanced line code, which means that the average DC level of the signal is zero. This is important because it helps to prevent accumulation of DC offset in the signal, which can lead to errors in the received signal.
- Self-clocking: AMI is a self-clocking line code, which means that the receiver can recover the clock signal from the received signal. This is important because it does not require an external clock signal, which can be expensive and difficult to synchronize.
- Simplicity: AMI is a relatively simple line code to implement, which makes it cost-effective.

As a result of these advantages, AMI is a popular line coding method for many applications, including telecommunications and data communications.

Q28. How many types of scrambling techniques are used in data communication? For using scrambling technique, what three requirements are essential?

In data communication long sequence of 0 is replaced by combination of other levels to provide ***synchronization*** called **Scrambling Technique**.

There are many different types of scrambling techniques used in data communication. Some of the most common types include:

- **Bipolar with 8-zero substitution (B8ZS):** This technique replaces eight consecutive zeros with a special code to prevent long strings of zeros from occurring.
- **High-density bipolar-3 (HDB3):** This technique replaces four consecutive zeros with a special code to prevent long strings of zeros from occurring.

The three requirements essential for using scrambling techniques are:

- It must satisfy:
    - It should be recognized by receiver and replace with original
    - Same length as original
    - Error detection capability

Scrambling Technique Used for long distance transmission *e.g.,* WAN.

Q29. "The scrambling technique is highly necessary for Wide Area Network (WAN), not for Local Area Network (LAN)" – Justify the statement.

Scrambling is a technique used to randomize the data stream before transmission over a communication channel. The main purpose of scrambling is to provide synchronization and reduce the DC content of the transmitted signal.

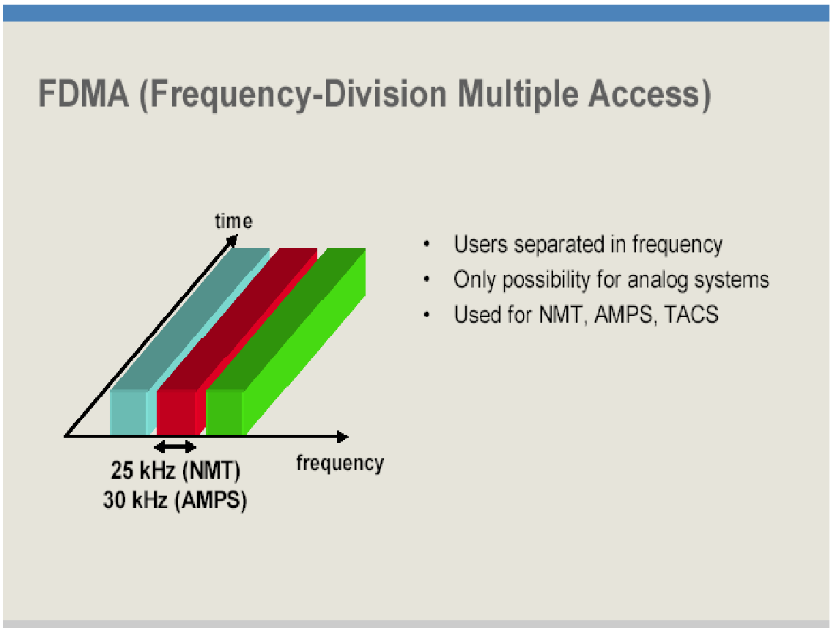
In LANs, the communication channels are typically short, and the probability of noise or interference on the channel is low. Therefore, the need for scrambling to reduce the DC content is minimal. Additionally, LAN protocols often use encoding schemes that already provide synchronization, such as Manchester encoding.

On the other hand, WANs typically use longer communication channels, which are more susceptible to noise and interference. Scrambling is therefore more critical in WANs to ensure that the data is transmitted reliably and without errors. In WANs, the use of scrambling ensures that the data is randomized before transmission, which makes it more resistant to noise and interference.

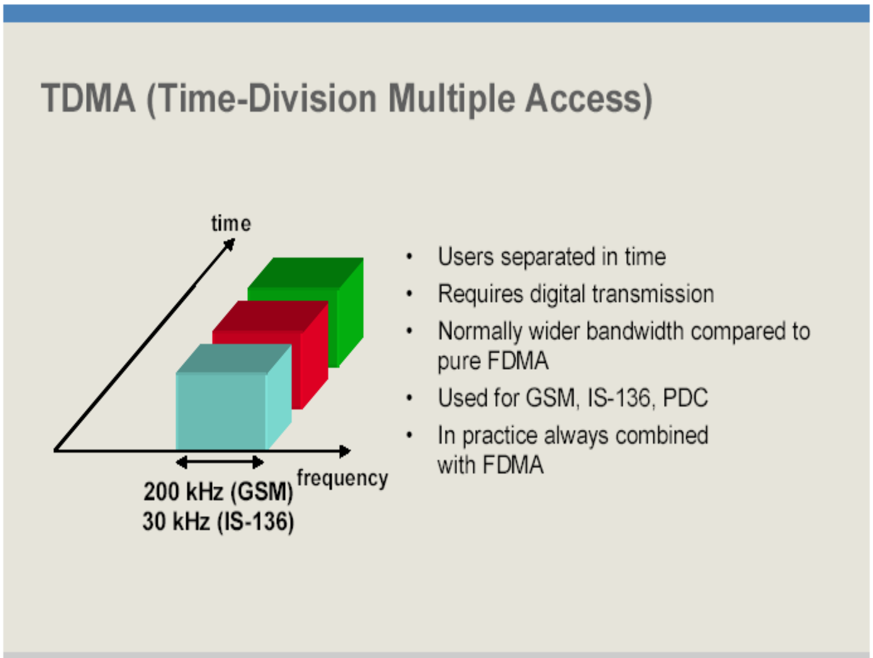
In summary, scrambling is more essential in WANs than in LANs because the former requires long-distance transmission of digital signals, which may be affected by various noise sources. However, LANs typically operate over short distances and are less prone to noise, and hence, the use of scrambling techniques is not as necessary as in WANs.

Q30. With necessary figures, name the three types of multiple accessing technique, and make a comparison table for three.

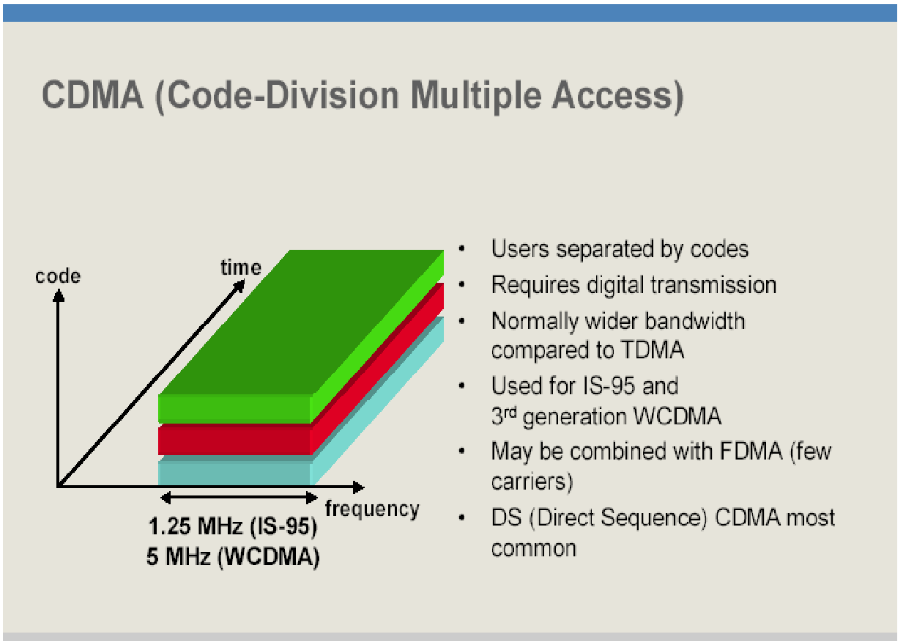
Frequency-division multiple access (FDMA): In FDMA, each user is assigned a unique frequency band. This ensures that no two users will interfere with each other. FDMA is a good choice for applications where there are a limited number of users and each user needs a large amount of bandwidth.



Time-division multiple access (TDMA): In TDMA, each user is assigned a unique time slot. This ensures that no two users will transmit at the same time. TDMA is a good choice for applications where there are a large number of users and each user only needs a small amount of bandwidth.



Code-division multiple access (CDMA): In CDMA, each user is assigned a unique code. This ensures that no two users will interfere with each other. CDMA is a good choice for applications where there are a large number of users and each user only needs a small amount of bandwidth.



Here is a comparison table for the three multiple access techniques:

Technique	FDMA	TDMA	CDMA
Acronym	Frequency Division Multiple Access	Time Division Multiple Access	Code Division Multiple Access
Principle	Multiple users share the frequency band	Multiple users share the time slots	Multiple users transmit data simultaneously, distinguished by unique codes
Bandwidth Allocation	Each user is allocated a dedicated frequency band	Each user is allocated a dedicated time slot	All users share the same frequency band, but each user uses a unique code
Interference	Interference is less likely as each user is allocated a dedicated frequency band	Interference may occur due to overlapping time slots	Interference is possible, but minimized due to unique codes
Capacity	Limited number of users can be accommodated due to limited frequency bands	More users can be accommodated by dividing time slots	Large number of users can be accommodated as all users can transmit simultaneously
Efficiency	Not very efficient as frequency bands may be underutilized	Efficient as users share time slots	Efficient as all users can transmit simultaneously
Security	Not very secure as eavesdropping is possible	More secure as users are allocated dedicated time slots	Very secure as other users cannot interpret the transmissions
Examples	Analog radio, TV broadcast	GSM, 3G cellular networks	CDMA2000, WCDMA, 4G LTE

Q31. Evan in multiplexing technique, show the importance of modulation technique for serving a large number of users.

Multiplexing techniques are used to combine multiple signals into a single transmission channel, thus increasing the channel utilization and serving a large number of users. Modulation techniques are used to modulate the signals onto a carrier signal, which is then multiplexed with other signals. The importance of modulation techniques in multiplexing can be understood as follows:

1. **Frequency Division Multiplexing (FDM):** In FDM, multiple signals are modulated onto different carrier frequencies and combined for transmission. The bandwidth of each modulated signal is equal to the bandwidth of the original signal. Modulation is essential in FDM as it allows multiple signals to be transmitted on different frequencies without interference.

2. **Time Division Multiplexing (TDM):** In TDM, multiple signals are time-multiplexed onto a single channel by assigning a time slot to each signal. The signals are modulated onto a carrier signal, which is then time-multiplexed. Modulation is necessary in TDM as it allows each signal to be transmitted during its assigned time slot without interfering with other signals.

3. **Code Division Multiplexing (CDM):** In CDM, multiple signals are modulated with different spreading codes and combined for transmission. Each signal is spread over a wide bandwidth using a unique code, and the modulated signals are combined. Modulation is essential in CDM as it allows each signal to be spread over a wide bandwidth using a unique code without interfering with other signals.

In all these multiplexing techniques, modulation is essential to ensure that the signals are combined and transmitted without interference. Modulation also allows multiple signals to share the same transmission channel without interfering with each other. Therefore, the use of modulation techniques in multiplexing is crucial for serving a large number of users over a single transmission channel.

Q32. In North American time division multiplexing (TDM) framing standard, show that the bit rate of T1 frame is 1.544 Mbps.

North American TDM frame contains 24 TS where each TS contains 8 bits of a user (equivalent of 8 PCM bits/sample) and the 0th TS contains a single bit for frame alignment called *T*1 frame like Fig. 4.

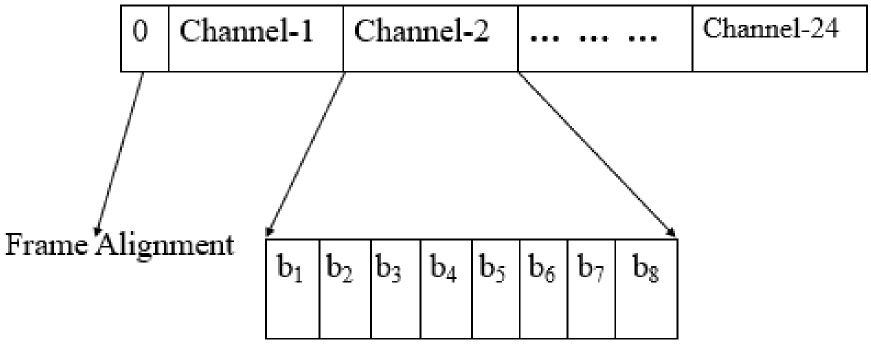


Fig.4: T1 frame of 30 Channels

The total number of bits/frames = 8×24+1 = ***193 bits***. The 8 PCM bits of each sample is placed in a TS, therefore the length of a frame, T_f = (1/8000) sec ***125 μs***. The bit rate of T1 frame = 193/125 =1.544 Mbps.

Q33. In European time division multiplexing (TDM) framing standard, show that the bit rate of E1 frame is 2.048 Mbps

Fig. below shows the frame of 30-channel system where out of 32 time slot (TS) the 0th TS is for frame alignment; 16th TS is for signaling and the rest 30 TS (1 to 15 and 17 to 31) for speech. Each TS contains 8 PCM bits, equivalent to each quantized pulse of ***256 level system***. Such frame is called **E1** frame followed by European.

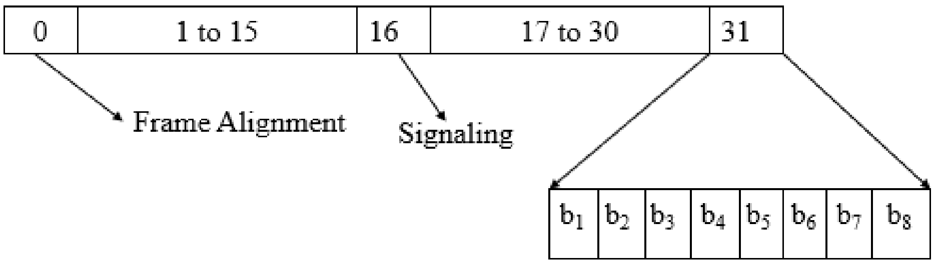


Fig. E1 frame of 30 Channels

The bit rate of the 30-channel PCM frame is, 8 kHz (sampling rate) × 8 (bits per sample or TS) × 32 (number of TS/frame) = 2.048 Mbps. The total number of bite/frame = 8×32 = 256bits. We know the sampling rate of voice signal is 8000 samples/sec, therefore sampling period, T_s = (1/8000) sec. The 8 PCM bits of each sample is placed in a TS, therefore the length of a frame, T_f = (1/8000) sec = 125 μs. The width of each bit, d = 125/256 = 0.488 μs.