Q. Why framing is used in data communication? Write down the purposes of using byte stuffing and bit stuffing. ***q 1st

Framing is used in data communication to break up a stream of data into discrete units, or frames, to enable reliable transmission and reception of the data. Frames provide a structure for transmitting data, including start and end markers, addressing information, and error detection codes. This helps ensure that the receiver can correctly interpret and process the data, even in the presence of noise or other errors that can occur during transmission.

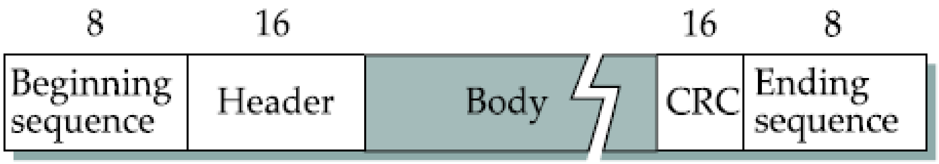
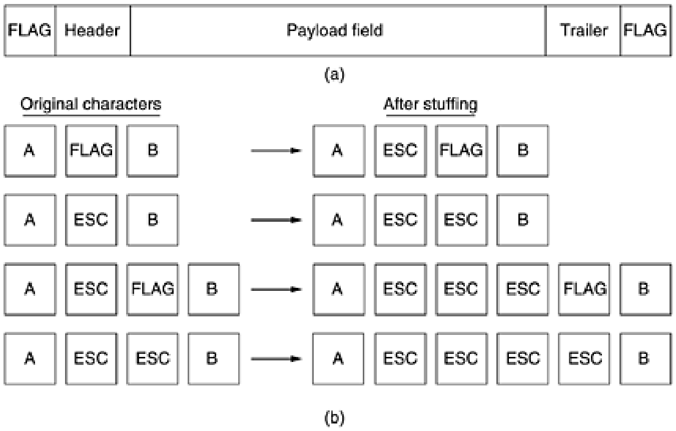


Fig.1 Frame format

Byte stuffing and bit stuffing are techniques used in framing to ensure that the data being transmitted conforms to certain protocols or standards.

Byte stuffing is used when a sequence of data needs to be transmitted that includes a byte pattern that could be mistaken for a control character. In this case, the data is "stuffed" with an extra byte so that the control character is not misinterpreted by the receiver. Byte stuffing is commonly used in protocols such as HDLC (High-Level Data Link Control) and PPP (Point-to-Point Protocol).



Bit stuffing, on the other hand, is used to ensure that there are no long runs of consecutive 1s or 0s in the transmitted data that could be mistaken for control characters or other patterns. In bit stuffing, a "stuffing bit" is inserted into the data stream after a certain number of consecutive bits of the same value. This helps ensure that the receiver can correctly identify the start and end of each frame, even in the presence of noise or other errors. Bit stuffing is commonly used in protocols such as Ethernet and HDLC.

When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically dyestuffs (*i.e.*, deletes) the 0 bit. If the user data contain the flag pattern 01111110, this flag is transmitted as 011111010 but stored in the receiver's memory as 01111110. Fig. below gives an example of bit stuffing.

0 1 1 1 1 1 1 0 0 1 1 1 1 1 0 1 0 1 0 1 1 1 1 1 1 0

Q. 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? ***q 1st CT

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.

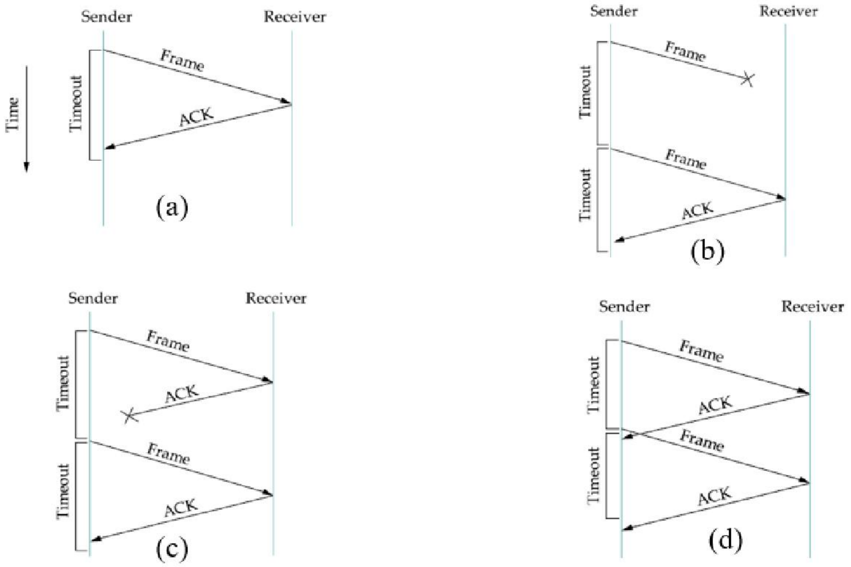


Figure below illustrates four different scenarios that result from this basic algorithm. Figure (a) shows the situation in which the ACK is received before the timer expires, (b) and (c) show the situation in which the original frame and the ACK, respectively, are lost, and (d) shows the situation in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

Q. What is the problem that we face in Stop-and-Wait link layer protocol? How Does the sliding window protocol resolve the problem? ***q 1st

The Stop-and-Wait protocol is a simple protocol used in the data link layer for reliable transmission of data over a communication channel. In this protocol, the sender sends a single frame of data to the receiver and waits for an acknowledgment (ACK) from the receiver before sending the next frame. If the sender does not receive an ACK within a certain time period, it assumes that the frame was lost and resends it.

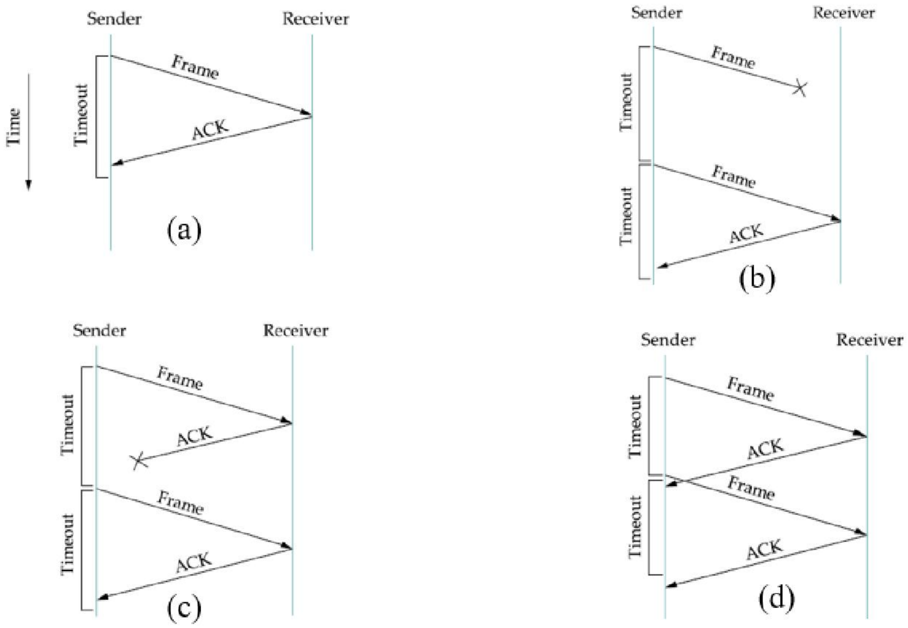
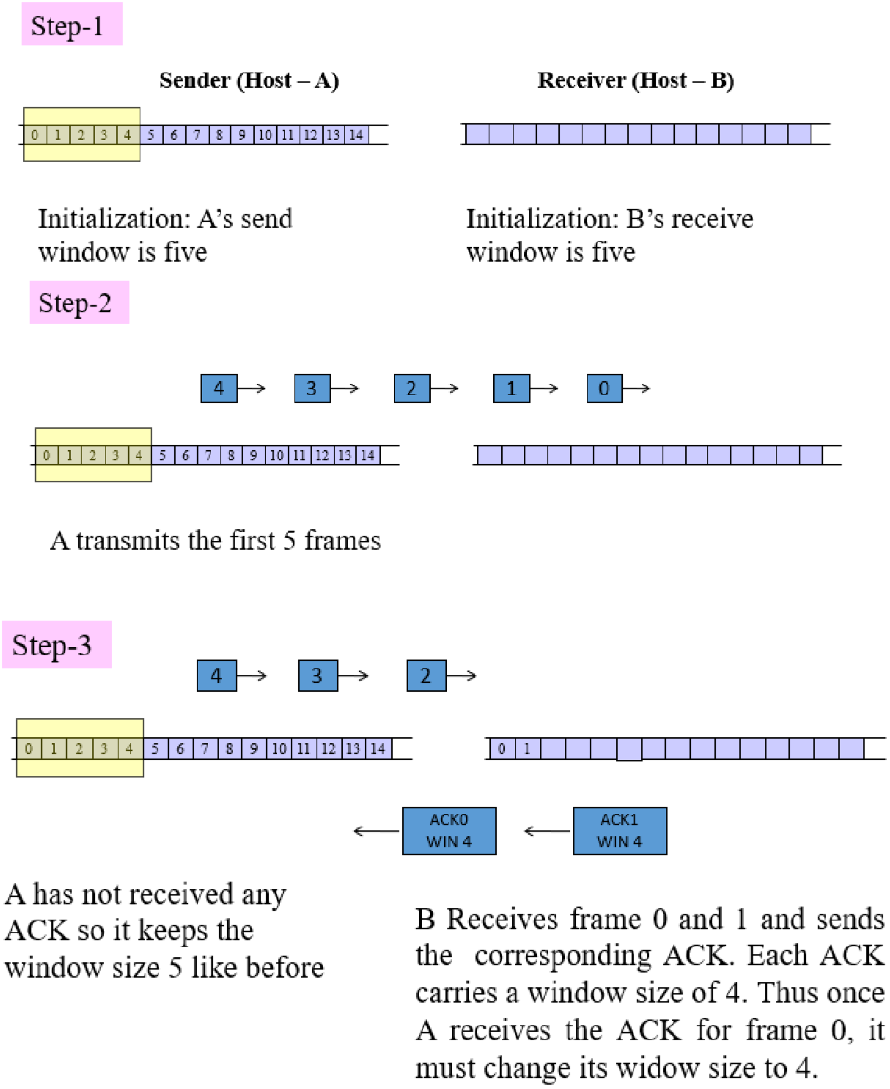


Figure below illustrates four different scenarios that result from this basic algorithm. Figure (a) shows the situation in which the ACK is received before the timer expires, (b) and (c) show the situation in which the original frame and the ACK, respectively, are lost, and (d) shows the situation in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

The main problem with the Stop-and-Wait protocol is that it has low efficiency, especially in high-speed networks, as it requires the sender to wait for the ACK for each frame before it can send the next frame. This can lead to significant delays in data transmission and can result in low network throughput.

The sliding window protocol is a solution to this problem that allows for more efficient use of the communication channel. In the sliding window protocol, the sender can 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.



Initialization: A's send window is five

Initialization: B's receive window is five

A transmits the first 5 frames

A has not received any ACK so it keeps the window size 5 like before

B Receives frame 0 and 1 and sends the corresponding ACK. Each ACK carries a window size of 4. Thus once A receives the ACK for frame 0, it must change its widow size to 4.

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. If a frame is lost or corrupted, the sender resends only that frame without waiting for ACKs for the other frames in the window.

By allowing the sender to send multiple frames without waiting for ACKs for each frame, the sliding window protocol can achieve higher network throughput and efficiency than the Stop-and-Wait protocol. It is widely used in many communication protocols, including TCP (Transmission Control Protocol), for reliable transmission of data over the Internet.

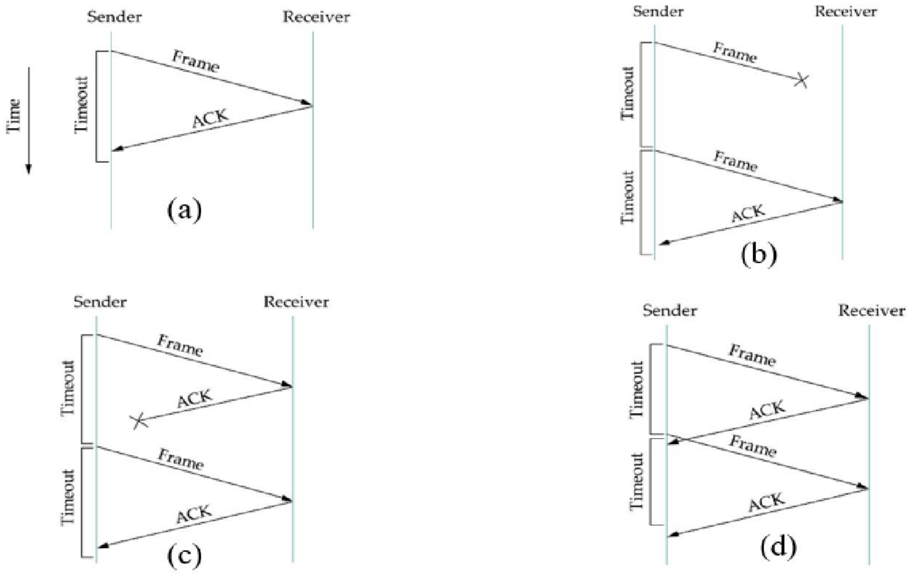
Q. Why flow control is necessary in LLC? Mention the problem that arises when the timer value is set small in stop-and-wait protocol. ***q 1st

Flow control is necessary in the Logical Link Control (LLC) layer to prevent a sender from overwhelming a receiver with data. The main purpose of flow control is to ensure that the receiver can process the data at a rate that is consistent with its capacity to handle the data, and to prevent the sender from overloading the receiver with data that it cannot handle.

The various stations in a network may operate at different speeds. **One of the tasks of the data link layer is to ensure that slow devices are not swamped with data from fast devices**. Flow control refers to the regulating of the rate of data flow from one device to another so that the receiver has enough time to consume the data in its receive buffer, before it overflows.

In stop-and-wait protocol, if the timer value is set too small, it can cause a problem known as "premature timeout". This occurs when the timer expires before the receiver has had sufficient time to process the data and send an acknowledgement (ACK) back to the sender.

When a premature timeout occurs, the sender retransmits the data unnecessarily, which can result in increased network traffic and decreased network efficiency. This problem can be particularly acute in high-speed networks, where the data transmission rate is much faster than the processing rate of the receiver.



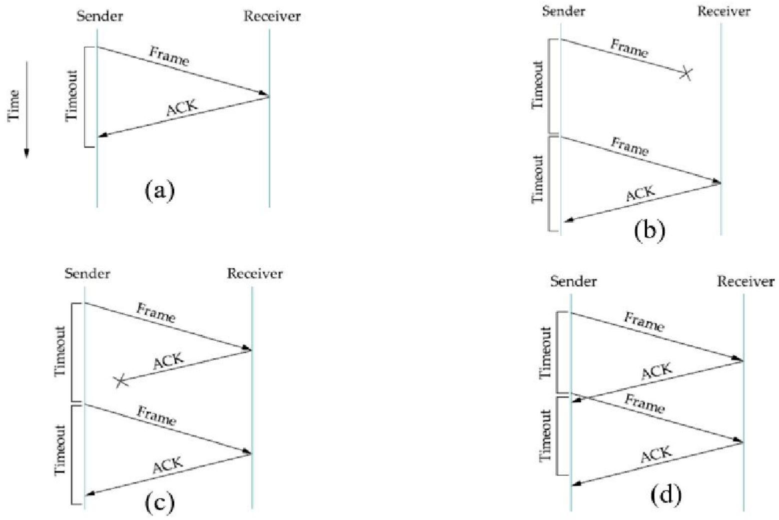
To prevent this problem, the timer value in stop-and-wait protocol should be set to a value that is long enough to allow the receiver to process the data and send an ACK back to the sender before the timer expires. The value of the timer should be carefully chosen to balance the need for timely transmission of data with the need to avoid unnecessary retransmissions due to premature timeouts.

In addition to the timer value, other flow control mechanisms such as window-based flow control and congestion control can also be used to ensure that data is transmitted at a rate that is consistent with the capacity of the receiver and the overall state of the network.

Q. With appropriate figures show, the sliding window protocol removes the data transmission inefficiency of stop-and-wait protocol. ***q 1st

- Certainly! Here's an illustration of how the sliding window protocol removes the data transmission inefficiency of the stop-and-wait protocol.

In the stop-and-wait protocol, the sender sends a single frame of data and then waits for an acknowledgement (ACK) from the receiver before sending the next frame. This results in low efficiency, especially in high-speed networks, as shown in the following diagram:

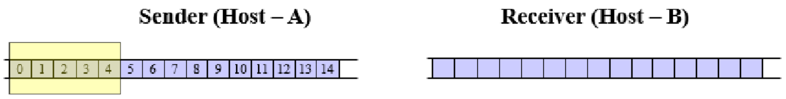


As you can see, the sender must wait for an ACK before sending each subsequent frame, resulting in a delay before the next frame can be transmitted.

In contrast, 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, as shown in the following diagram:

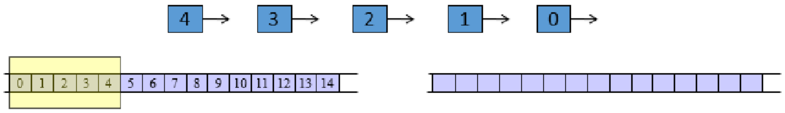
Step-1



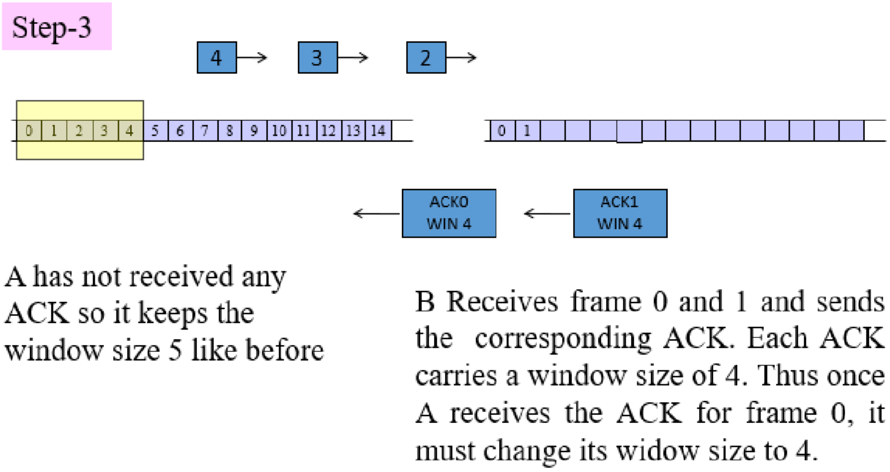
Initialization: A's send window is five

Initialization: B's receive window is five

Step-2

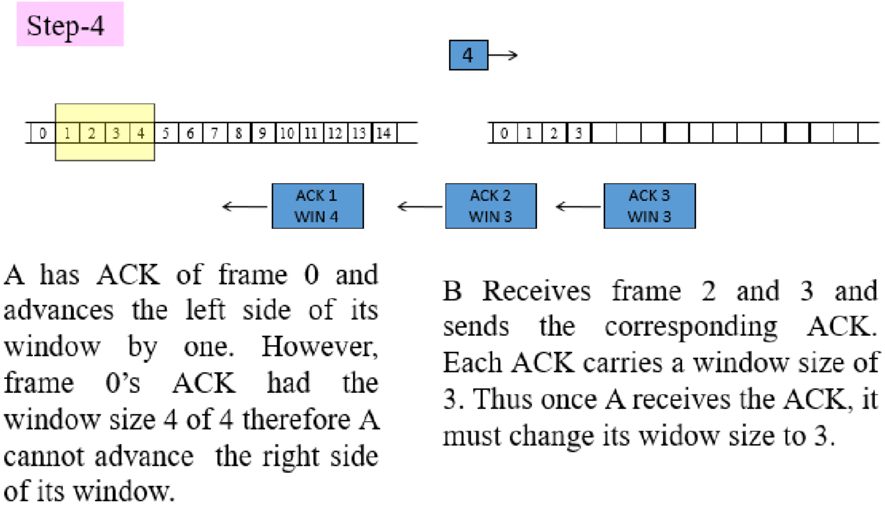


A transmits the first 5 frames



A has not received any ACK so it keeps the window size 5 like before

B Receives frame 0 and 1 and sends the corresponding ACK. Each ACK carries a window size of 4. Thus once A receives the ACK for frame 0, it must change its widow size to 4.



A has ACK of frame 0 and advances the left side of its window by one. However, frame 0's ACK had the window size 4 of 4 therefore A cannot advance the right side of its window.

B Receives frame 2 and 3 and sends the corresponding ACK. Each ACK carries a window size of 3. Thus once A receives the ACK, it must change its widow size to 3.

As you can see, the sender can send multiple frames before receiving ACKs for each frame, resulting in a much higher rate of data transmission and higher network efficiency. This is achieved through the use of a sliding window, which allows the sender to send multiple frames before receiving ACKs for each frame.

Q. What are the function of Logical Link Control (LLC) Layer? How is transmission synchronization archived in LLC layer? ***q 1st

- The Logical Link Control (LLC) layer is responsible for providing reliable data transfer between two devices on the same network. Its functions include:

1. Framing: The LLC layer receives data from the Network layer and encapsulates it into frames for transmission over the network.
2. Error control: The LLC layer performs error checking and correction, ensuring that the data received at the receiving end is error-free.

3. Flow control: The LLC layer ensures that the data transmission rate is consistent with the receiver's capacity to handle the data, preventing the sender from overwhelming the receiver with data that it cannot handle.
4. Access control: The LLC layer manages access to the shared network medium, ensuring that multiple devices can communicate over the network without interfering with each other.

In the LLC layer, transmission synchronization is achieved through the use of synchronization bits, which are added to the beginning of each frame. These bits are used to signal the start of a new frame and allow the receiver to synchronize its clock with the sender's clock.

The synchronization bits are followed by a frame delimiter, which is used to indicate the end of the synchronization bits and the beginning of the actual data in the frame. The frame delimiter allows the receiver to identify the boundaries of the frame and extract the data from the frame.

Once the synchronization bits and frame delimiter have been received, the receiver can then decode the rest of the frame and process the data contained within it. The use of synchronization bits and frame delimiters ensures that data transmission is synchronized between the sender and receiver, enabling reliable and efficient data transfer over the network.

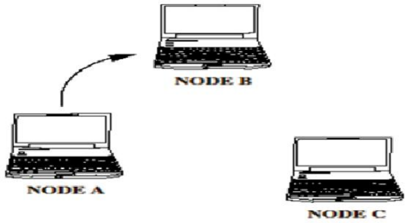
Q. Define hidden terminal problem. Can RTS-CTS handshaking avoid the hidden terminal problem completely? Is there any side effect of this avoiding process? ***q 2nd

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.

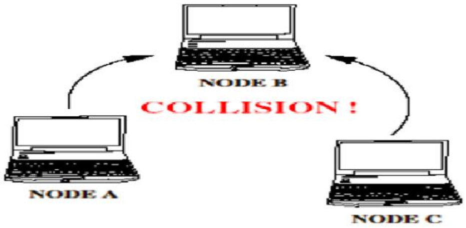
- Appears when two nodes are unaware of each other’s attempt to send data to a third node
- “Unaware of each other” means “out of each other's signal range”
- The result is data collision at the receiving node
- The problem exists in contention-based protocols

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.

A transmits to B



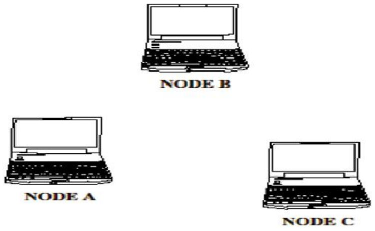
C transmits to B



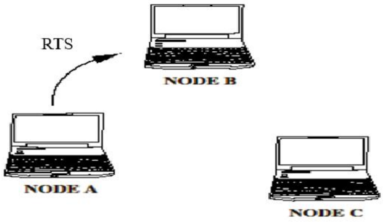
Solution- The RTS-CTS (Request-to-Send/Clear-to-Send) handshaking process is a technique used to address the hidden terminal problem in wireless LAN communication. This technique uses two frames, the RTS frame, and the CTS frame, to coordinate the transmission of data between wireless nodes.

- 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!

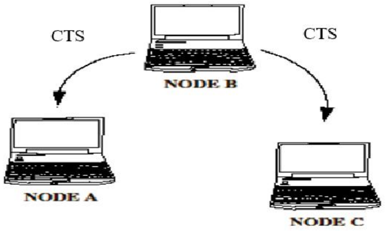
RTS-CTS Handshake



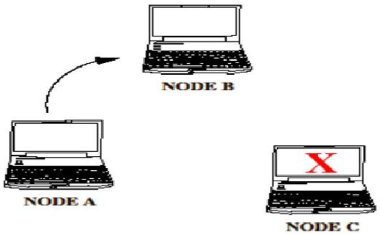
A sends RTS to B



B broadcasts CTS



A sends DATA to B



However, while RTS-CTS handshaking can reduce the likelihood of collisions due to hidden terminals, it does not completely eliminate the hidden terminal problem. It introduces additional overhead in the form of control frames (RTS and CTS), which consume some of the available bandwidth. This overhead can reduce the overall network throughput. Additionally, if the network is heavily congested or experiences high levels of interference, the RTS-CTS mechanism may add further delays and inefficiencies to the communication process.

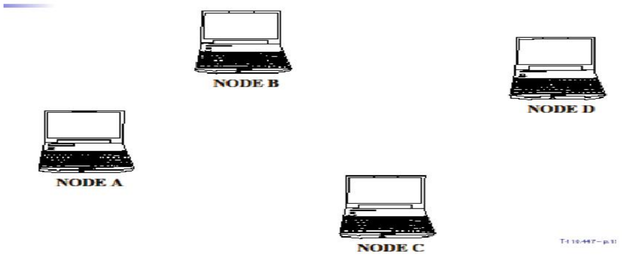
Therefore, while RTS-CTS handshaking is a useful mechanism to mitigate the hidden terminal problem, it is not a foolproof solution and has its own side effects in terms of increased overhead and potential performance impact. Network designers must carefully consider the trade-offs and adjust the usage of RTS-CTS based on the specific requirements and characteristics of the wireless network.

Q. Sketch different scenarios where the handshaking process cannot resolve the Hidden terminal problem. ***q 2nd

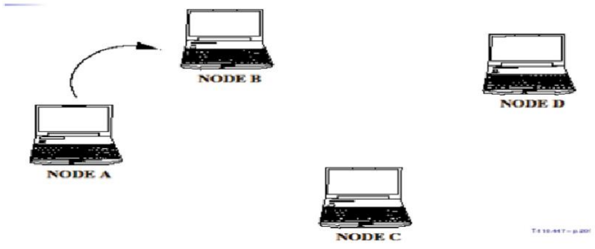
- While the RTS-CTS handshaking process can effectively resolve the hidden terminal problem in many scenarios, there are some situations where it may not be effective. Here are some scenarios where the handshaking process may not resolve the hidden terminal problem:

1. Multiple hidden terminals: If there are multiple hidden terminals that cannot hear each other but can hear the same sender, then the RTS-CTS handshaking process may not be effective. In such a scenario, the sender may receive a CTS frame from one of the receivers and transmit data, leading to collisions with the other hidden terminals that are transmitting data simultaneously.
2. Network congestion: If the network is congested, and there are many nodes trying to transmit data simultaneously, then the RTS-CTS handshaking process may not be effective. In such a scenario, the overhead of the handshaking process may lead to increased delays and reduced network throughput, making it difficult to resolve the hidden terminal problem.
3. Channel fading: If the wireless channel experiences fading, where the signal strength fluctuates due to interference or obstacles, then the RTS-CTS handshaking process may not be effective. In such a scenario, the CTS frame may not reach the sender, leading to collisions with other hidden terminals that are transmitting data simultaneously.
4. Receiver mobility: If the receiver is mobile and moves out of range after sending the CTS frame, then the sender may not receive the CTS frame, leading to collisions with other hidden terminals that are transmitting data simultaneously.

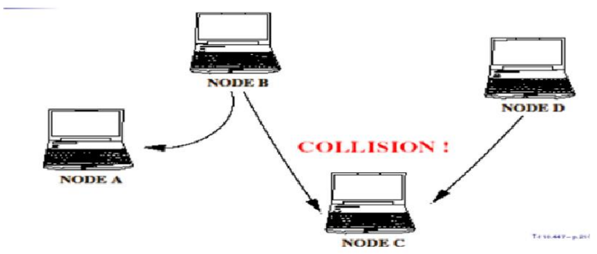
Failure Scenario 1



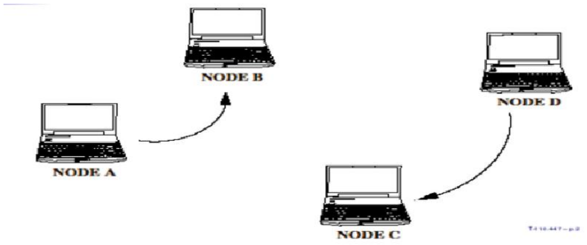
A sends RTS to B



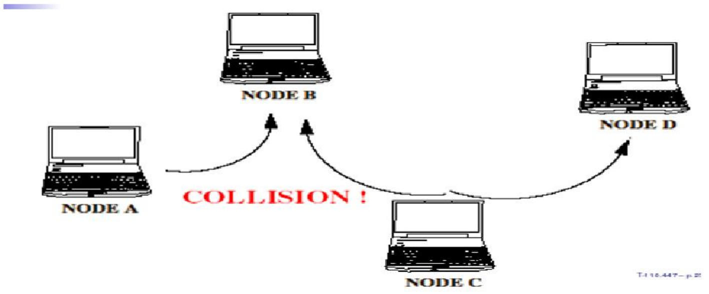
B broadcasts CTS &
D sends RTS to C (D can not receive CTS!!)



A sends DATA to B -
D sends RTS to C Again



A sends DATA to B -
C broadcasts CTS



In general, the effectiveness of the RTS-CTS handshaking process in resolving the hidden terminal problem depends on various factors, such as the network topology, traffic load, channel conditions, and mobility of the nodes. Network designers must consider these factors while designing and deploying wireless LAN networks to ensure efficient and reliable communication.

Q5. What is the difference between *CSMA/CD* and *CSMA/CA* MAC protocols? Describe the reasons why the Network Allocation Vector (NAV) is preferred than Physical carrier sending in *CSMA/CA* MAC protocol. ***q 2nd

- The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) and Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) are two popular Medium Access Control (MAC) protocols used in wired and wireless networks, respectively. Here are the basic differences between these two protocols:

- **Collision Detection vs. Collision Avoidance:** CSMA/CD detects collisions by sensing the carrier on the medium after it has started transmitting. In contrast, CSMA/CA avoids collisions by reserving the medium before transmitting data.
- **Wired vs. Wireless Networks**: CSMA/CD is used in wired networks, such as Ethernet, while CSMA/CA is used in wireless networks, such as Wi-Fi.
- **RTS/CTS Handshaking Process:** CSMA/CA uses an RTS/CTS handshaking process to reserve the medium before transmitting data, while CSMA/CD does not use any handshaking process.

- **Hidden Terminal Problem:** CSMA/CA uses an additional mechanism called the Network Allocation Vector (NAV) to avoid collisions caused by hidden terminals, while CSMA/CD does not have a specific mechanism to handle the hidden terminal problem.
- Delay and Overhead: CSMA/CA has more overhead than CSMA/CD due to the RTS/CTS handshaking process and the use of the NAV timer. This can lead to increased delay and reduced network throughput.

- CSMA/CD rule: Backoff after collision
- CSMA/CA rule: Backoff before collision

In summary, the main difference between CSMA/CD and CSMA/CA is the way they handle collisions and reserve the medium for data transmission. While CSMA/CD detects collisions and uses a simple backoff mechanism to avoid them, CSMA/CA avoids collisions by reserving the medium before transmitting data and using an RTS/CTS handshaking process.

The Network Allocation Vector (NAV) is a timer used in CSMA/CA to reserve the medium for a specific duration of time. The NAV timer is set by the receiver and is broadcast to all other nodes in the network. During the duration of the NAV timer, no other nodes can transmit data, even if the carrier is sensed to be idle. The NAV timer is preferred over physical carrier sending because of the following reasons:

1. **Hidden Terminal Problem:** The NAV timer helps to avoid collisions caused by hidden terminals, which is a major problem in wireless networks. Physical carrier sensing does not solve the hidden terminal problem.
2. **Efficiency:** Physical carrier sending involves transmitting a signal to reserve the medium, which increases the overhead and reduces network efficiency. The NAV timer, on the other hand, is a software-based mechanism that does not require any additional hardware or signaling.
3. **Flexibility:** The duration of the NAV timer can be adjusted dynamically based on network conditions, such as the number of active nodes and the amount of traffic. This allows for better utilization of the medium and higher network throughput.

In summary, the main difference between CSMA/CD and CSMA/CA is the way they handle collisions and reserve the medium for data transmission. While CSMA/CD detects collisions and uses a simple backoff mechanism to avoid them, CSMA/CA avoids collisions by reserving the medium before transmitting data and using an RTS/CTS handshaking process. The NAV timer is preferred over physical carrier sending in CSMA/CA because it helps to avoid collisions caused by hidden terminals, is more efficient, and offers greater flexibility.

Q. Differentiate between ATM and TDM. Why small cell is used in ATM technology? Write down some applications of ATM. ***q 3rd

The differentiating between ATM and TDM:

Feature	ATM (Asynchronous Transfer Mode)	TDM (Time Division Multiplexing)
Principle of Operation	Packet-switching using fixed-length cells (53 bytes)	Multiplexing technique dividing into fixed time slots
Bandwidth Allocation	Dynamically allocated based on requirements	Fixed time slots allocated to channels
Flexibility	Supports various types of traffic (voice, data, video)	Less flexible, suitable for fixed bandwidth allocation
Efficiency	Efficient bandwidth utilization	Fixed allocation regardless of utilization
Applications	Broadband networks, voice/video transmission	Traditional telephony, legacy systems

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.

Applications of ATM

To support any type of traffic:
- bursty data (to multi-megabit rates: files, images, multimedia)
- voice (sustained data rate, 64 kbps)
- video (sustained data rate, multi-megabit rates)

To support transactions that use data, voice, and video simultaneously

To provide bandwidth on demand (pay for use)
To support multicast operations (video conferencing)
To provide guaranteed Quality-of-Service

1. Broadband Networks: ATM was initially developed for high-speed broadband networks. It has been used in various applications such as broadband internet access, video streaming, and multimedia communication.

2. Voice and Video Transmission: ATM provides efficient support for real-time applications like voice and video. It offers quality of service guarantees and low latency, making it suitable for voice over ATM (VoATM) and video conferencing.

3. ATM Networks: ATM has been utilized in building wide area networks (WANs) and metropolitan area networks (MANs) where efficient multiplexing, high bandwidth, and QoS are required.

4. Local Area Networks (LANs): ATM has also been implemented in LAN environments to provide high-speed connectivity and support for multimedia applications within organizations.

5. Virtual Private Networks (VPNs): ATM can be used to create secure virtual private networks, enabling organizations to connect geographically dispersed locations with high-speed data transmission and privacy.

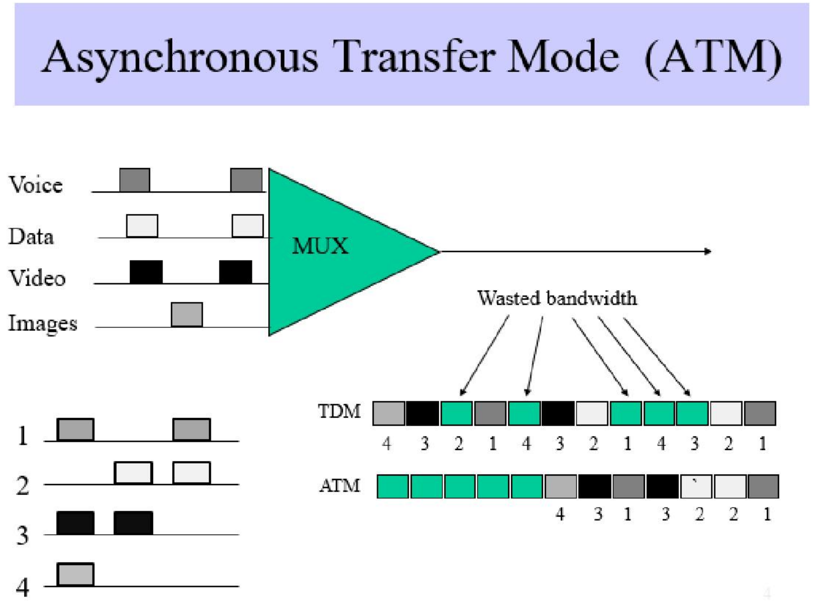
6. Mobile Networks: ATM has been explored for mobile network backhaul, where it can efficiently handle the high data rates and traffic demands of cellular networks.

Q. What is Asynchronous Transfer Mode (ATM) in data communication? How ATM resolves the wastage of bandwidth in TDMA? ***q 3rd

- Asynchronous Transfer Mode (ATM) is a high-speed, connection-oriented packet-switching technology used in telecommunications and computer networks. It is designed to support multiple types of traffic, including voice, data, and video, at high speeds over a wide range of transmission media.

- ✓ **Asynchronous** refers to the manner in which BW is allocated among connections and users. ATM is asynchronous in the sense that the recurrence of cells containing information from an individual user is not necessarily periodic.
- ✓ **ATM** uses statistical (asynchronous) time-division multiplexing i.e., the multiplexer fills a slot with a cell from any input channel that has a cell; the slot is empty if none of the channels has a cell to send.
- ✓ **Transfer mode** is a term intended to signify that it is a multiplexing and switching technique.

ATM resolves the wastage of bandwidth in Time Division Multiple Access (TDMA) by using a technique called cell switching. In TDMA, a fixed amount of time is allocated to each user for data transmission, even if there is no data to send. This results in a wastage of bandwidth, especially when the traffic is bursty.


Asynchronous Transfer Mode (ATM)

ATM is a packet-oriented (also connection oriented) transfer mode which allows multiple logical connections to be multiplexed over a single physical interface. The information flow on each logical connection is organized into fixed-size packets called cell.

In contrast, ATM uses cells of fixed length (53 bytes) for data transmission. Each cell consists of a 5-byte header and a 48-byte payload. The ATM switch examines the header of each cell and forwards it to the appropriate destination. Since the cells are of fixed length, the ATM switch can switch cells from different connections in a more efficient manner than the variable-length packets used in other protocols such as IP.

The use of cells also allows for statistical multiplexing, which means that the bandwidth is shared among multiple users dynamically based on their traffic requirements. This results in better utilization of the bandwidth and reduces wastage.

Another advantage of ATM is its ability to provide Quality of Service (QoS) guarantees for different types of traffic. ATM allows for the allocation of different levels of priority to different types of traffic, based on their requirements for delay, jitter, and bandwidth. This allows for better management of the network resources and ensures that high-priority traffic is given preferential treatment.

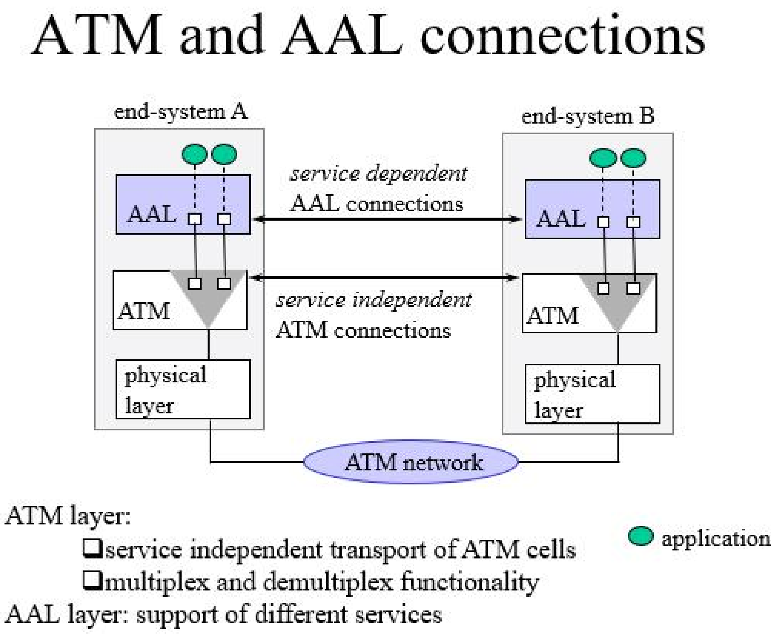
In summary, ATM is a high-speed, connection-oriented packet-switching technology that uses cells of fixed length for data transmission. It resolves the wastage of bandwidth in TDMA by using cell switching, statistical multiplexing, and providing QoS guarantees for different types of traffic.

Q. What are the function of Application Adaption Layer (AAL) in ATM based data communication? ***q 3rd

- The Application Adaptation Layer (AAL) in ATM-based data communication provides a way to adapt different types of data, such as voice, video, and data, to the fixed-size ATM cells for transmission over an ATM network. The AAL is responsible for ensuring that data from higher-layer protocols is properly segmented and reassembled into ATM cells and that it is transmitted with the appropriate quality of service (QoS) parameters.

The main functions of the AAL are as follows:

1. Segmentation and Reassembly (SAR): The AAL is responsible for segmenting the data from higher-layer protocols into ATM cells and reassembling them at the receiving end. The SAR function ensures that the data is properly segmented into fixed-size cells and that the cells are reassembled into their original format at the receiver.
2. Convergence Sublayer (CS): The AAL provides a convergence sublayer that is responsible for mapping the higher-layer protocols into ATM cells. The CS function ensures that the data from different protocols is properly formatted and that it is compatible with the ATM network.
3. Transmission and Reception: The AAL is responsible for transmitting and receiving data over the ATM network. It ensures that the data is transmitted with the appropriate QoS parameters, such as delay, jitter, and bandwidth, and that it is received correctly at the destination.
4. QoS Management: The AAL provides a mechanism for managing the QoS parameters of different types of data, such as voice, video, and data. It allows for the allocation of different levels of priority to different types of traffic, based on their requirements for delay, jitter, and bandwidth.



ATM and AAL connections

ATM layer:

- ❑service independent transport of ATM cells
- ❑multiplex and demultiplex functionality

AAL layer: support of different services

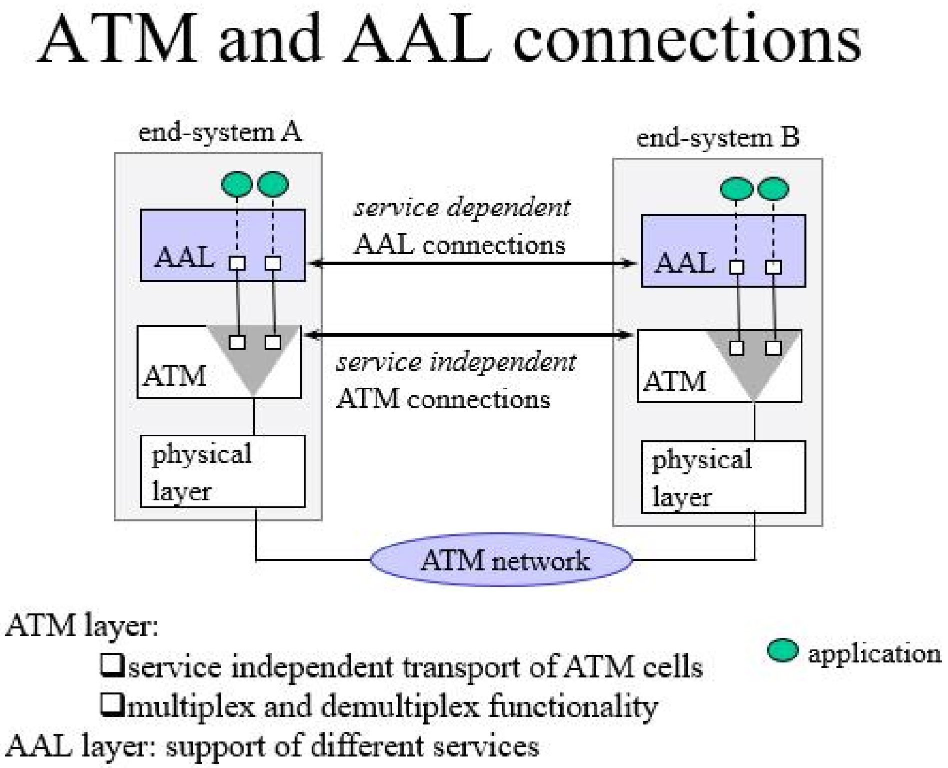
In summary, the Application Adaptation Layer (AAL) in ATM-based data communication provides a way to adapt different types of data to the fixed-size ATM cells for transmission over an ATM network. It ensures that the data is properly segmented and reassembled into ATM cells, that it is compatible with the ATM network, that it is transmitted and received correctly, and that it is provided with the appropriate quality of service (QoS) parameters.

Q. How does the Application Adaption Layer (AAL) support heterogeneous applications through ATM-based network? ***q 3rd

- The Application Adaptation Layer (AAL) in ATM-based networks supports heterogeneous applications by providing a common interface for various types of applications to interact with the ATM network. It adapts different types of data, such as voice, video, and data, to the fixed-size ATM cells for transmission over an ATM network. The AAL is responsible for ensuring that data from higher-layer protocols is properly segmented and reassembled into ATM cells and that it is transmitted with the appropriate quality of service (QoS) parameters.

The AAL supports heterogeneous applications through the following ways:

1. **Segmentation and Reassembly:** The AAL provides a mechanism for segmenting and reassembling data from different applications into ATM cells. This allows for the transmission of different types of data, such as voice, video, and data, over the same network.
2. **Convergence Sublayer:** The AAL provides a convergence sublayer that is responsible for mapping the different types of data from different applications into ATM cells. This ensures that the data is properly formatted and that it is compatible with the ATM network.
3. **QoS Management:** The AAL provides a mechanism for managing the QoS parameters of different types of data. It allows for the allocation of different levels of priority to different types of traffic, based on their requirements for delay, jitter, and bandwidth.
4. **Adaptation to Lower Layers:** The AAL provides an interface between the higher-layer protocols and the lower layers of the ATM network. This allows for the adaptation of different types of data to the fixed-size ATM cells for transmission over an ATM network.



ATM and AAL connections

ATM layer:

❑service independent transport of ATM cells

❑multiplex and demultiplex functionality

AAL layer: support of different services

In summary, the Application Adaptation Layer (AAL) in ATM-based networks provides a way to support heterogeneous applications by adapting different types of data to the fixed-size ATM cells for transmission over an ATM network. It provides mechanisms for segmentation and reassembly, convergence sublayer, QoS management, and adaptation to lower layers to ensure that data from different applications is properly formatted and transmitted with the appropriate QoS parameters.

Q3. Show that the Asynchronous Transfer Mode (ATM) is able to make the data communication in a service independent manner while it communicates data frames through Data Link Layer of a Local Area Network. ***q 3rd

- Asynchronous Transfer Mode (ATM) is a packet-switched network technology that operates at the Data Link Layer of the OSI model. ATM is designed to support different types of services, such as voice, video, and data, over the same network. It achieves service independence by using fixed-size cells that are 53 bytes long, which are more efficient than variable-length packets used in other network technologies.

The ATM cell consists of a 5-byte header and a 48-byte payload. The header contains information about the source and destination of the cell, as well as information about the quality of service (QoS) required for the cell. The payload contains the actual data that is being transmitted.

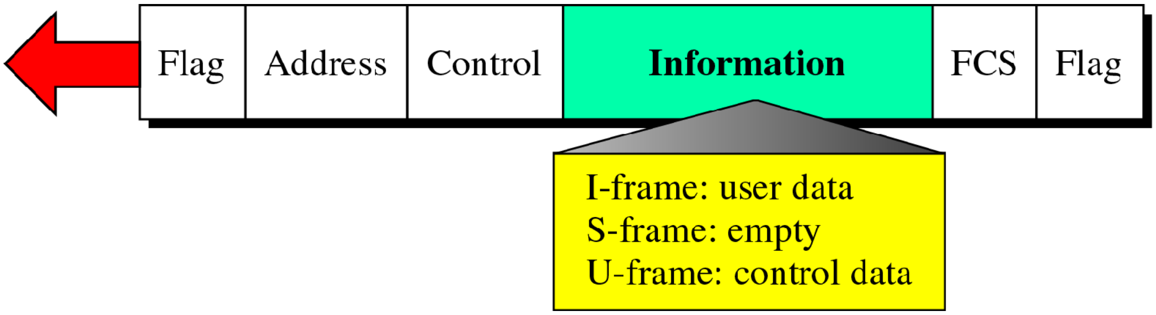
ATM is able to make data communication in a service independent manner through the following mechanisms:

1. Cell Switching: ATM uses cell switching to transmit data over the network. Cells are switched based on the information in the cell header, which includes the destination address and the QoS parameters. This allows ATM to provide a consistent level of service for different types of traffic, regardless of the type of application or service.
2. Virtual Channels and Virtual Paths: ATM uses virtual channels and virtual paths to provide a connection-oriented service that is independent of the underlying network technology. A virtual channel is a logical connection between two endpoints that is used to transmit data. A virtual path is a group of virtual channels that are used to transmit data between two endpoints.
3. Quality of Service (QoS): ATM provides different levels of QoS for different types of traffic. The QoS parameters are specified in the cell header and are used to ensure that data is transmitted with the appropriate level of priority and bandwidth.
4. AAL: The Application Adaptation Layer (AAL) in ATM is responsible for adapting different types of data to the fixed-size ATM cells for transmission over the network. The AAL supports different types of applications, such as voice, video, and data, by providing a common interface for these applications to interact with the ATM network.

Q15. In Link Access Procedure, Balanced (LAPB), how many types of data frames are conventionally used? Explain them clearly. ***q 4th

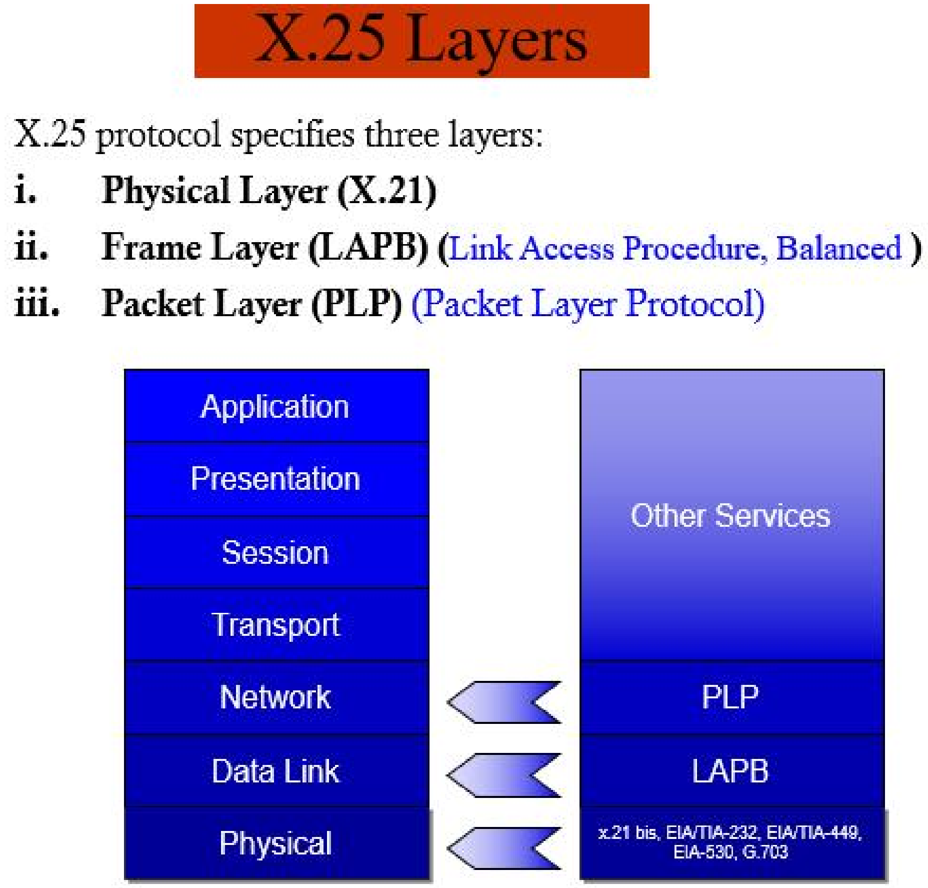
In Link Access Procedure, Balanced (LAPB), there are three types of data frames that are conventionally used:

- 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.



Q. Sketch the X.25 protocol layers and compare it with the Open System Interconnection (OSI) model. ***q 4th

X.25 Protocol Layers:
The X.25 protocol is a widely used protocol suite for packet-switched networks. It consists of three main layers:



X.25 Layers

X.25 protocol specifies three layers:

i. Physical Layer (X.21)

ii. Frame Layer (LAPB) (Link Access Procedure, Balanced)

iii. Packet Layer (PLP) (Packet Layer Protocol)

1. Physical Layer (X.21): The physical layer of the X.25 protocol deals with the physical transmission of data over the network medium. It defines the electrical, mechanical, and functional specifications for the physical connections between devices. It includes aspects such as voltage levels, timing, and physical connectors.

2. Data Link Layer (Frame Layer -LAPB): Link Access Procedure, Balanced (LAPB) is The data link layer in X.25 is responsible for the reliable transmission of data between adjacent nodes in the network. It ensures error-free and ordered delivery of data frames. The data link layer also handles flow control and error detection and correction.

3. Network Layer (Packet Layer -PLP): Packet Layer Protocol (PLP) is The network layer is responsible for addressing and routing data packets between different networks or nodes. It handles the logical addressing of packets and determines the best path for data transmission. The X.25 network layer uses virtual circuits for establishing connections between nodes.

Comparison with the OSI Model:

The X.25 protocol predates the OSI model but can be mapped to its general architecture. Here's a comparison of the X.25 protocol layers with the OSI model:

1. Physical Layer, X.21: The X.25 physical layer corresponds to the OSI physical layer. Both layers handle the physical transmission of data, including the specifications for the physical medium.

2. Data Link Layer (Frame Layer -LAPB): Link Access Procedure, Balanced (LAPB) is The X.25 data link layer combines aspects of both the OSI data link layer and network layer. It incorporates functions related to error detection and correction (similar to OSI data link layer) and also handles aspects like flow control and reliable data delivery (similar to OSI network layer).

3. Network Layer (Packet Layer -PLP): Packet Layer Protocol (PLP) is The X.25 network layer corresponds to the OSI network layer. Both layers are responsible for addressing, routing, and logical connectivity between nodes. The X.25 network layer uses virtual circuits for establishing connections, which is similar to the OSI concept of virtual circuits in the network layer.

It's important to note that the X.25 protocol predates the OSI model and was developed independently. Therefore, the layering in X.25 does not align perfectly with the OSI model. Nonetheless, the X.25 protocol can be roughly mapped to the OSI model's layers based on their functional similarities.

Q19. Make a clear comparison between frame relay and X.25 MAC technologies. ***q 4th

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.

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. ***q 5th

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.

Q. What is quantization error? Can we reduce the quantization error anyway? Show that average quantization error is $a^2/12$; where a is the quantization interval. ***q 5th

Quantization error is the difference between the actual analog input value and the nearest quantization level. It is a deterministic error that is introduced when an analog signal is converted to a digital signal. The quantization error is proportional to the size of the quantization interval, which is the smallest possible difference between two digital values. The higher the resolution of the digital signal, the smaller the quantization interval and the lower the quantization error.

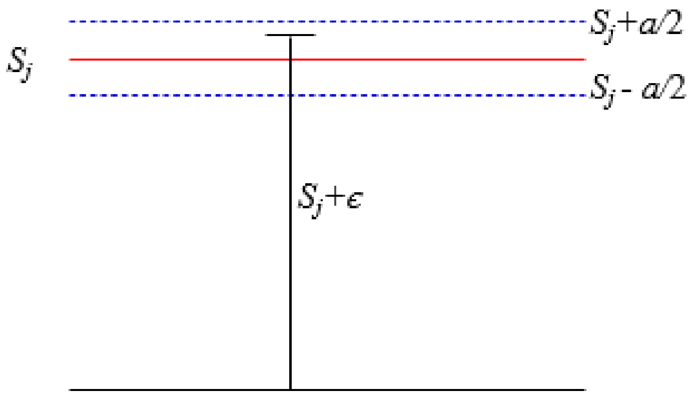


Fig. 5: Quantization error

The quantization error can be reduced by increasing the resolution of the digital signal. This can be done by using a higher-order analog-to-digital converter (ADC). However, increasing the resolution of the ADC also increases the cost and complexity of the system.

The average quantization error can be calculated as follows:
E = a^2 / 12

$$E(\in^2) = \frac{1}{a}\int_{-a/2}^{a/2} \in^2 \; d\in = \frac{a^2}{12} \qquad \text{Where} \qquad -\frac{a}{2} \le \in \le \frac{a}{2}$$

where:

- E is the average quantization error
- a is the quantization interval

This equation can be derived by considering the probability distribution of the quantization error. The quantization error can be positive or negative, and the probability of a positive error is equal to the probability of a negative error. The average quantization error is therefore equal to the square of the quantization interval divided by 12.

There are a number of ways to reduce the quantization error, including:

- Using a higher-order ADC
- Using a dither signal
- Using noise shaping

Using a higher-order ADC is the most effective way to reduce the quantization error, but it also increases the cost and complexity of the system. Using a dither signal is a less expensive way to reduce the quantization error, but it does not reduce the error as much as using a higher-order ADC. Noise shaping is a technique that can be used to reduce the quantization error without increasing the cost or complexity of the system.

Q. Draw the figure for above/below equation and show the significance of it by mentioning input signal bandwidth, guard band and signal filtering. ***q 5th

$$= dX(\omega) + d \sum_{n=-\infty, n\neq 0}^{\infty} X(\omega - n\omega_c)\,\text{sin}\,c(nd) = d\sum_{n=-\infty}^{\infty} X(\omega - n\omega_c)\,\text{sin}\,c(nd)$$

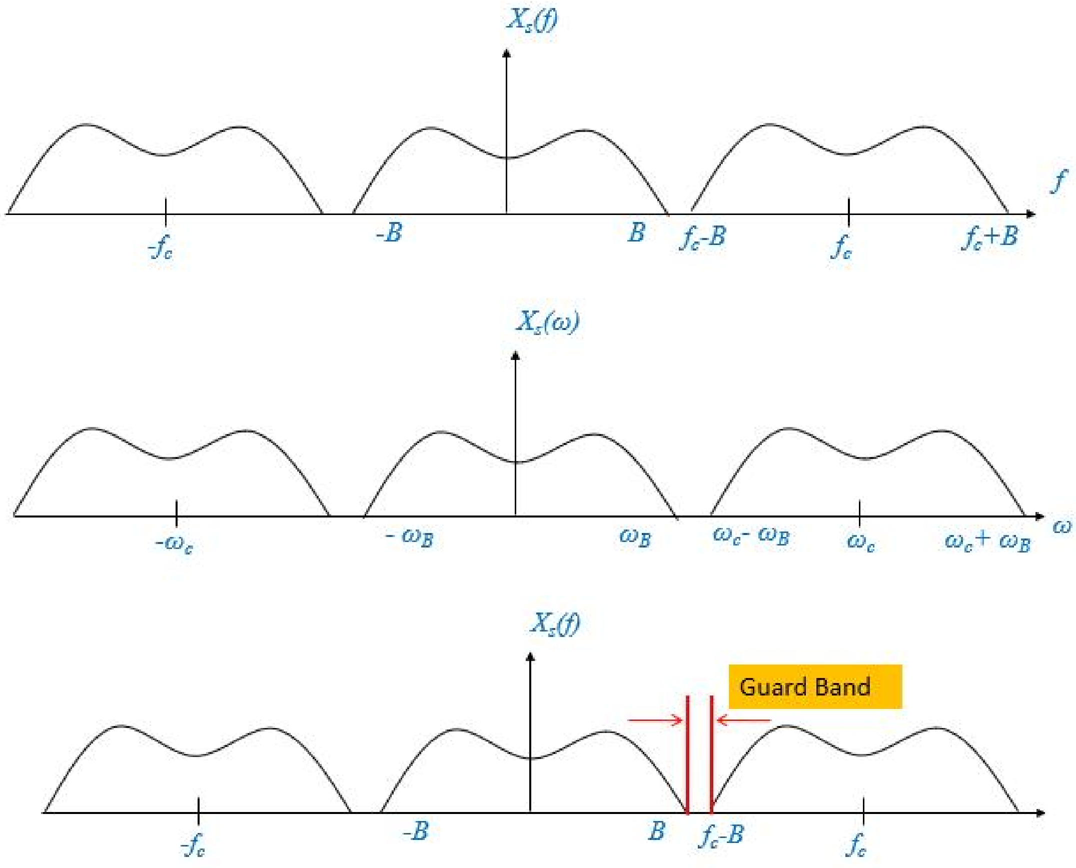


Fig. The condition $f_c \geq 2B$ is called Nyquist sampling rate.

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

Q. Why zigzag is introduced in the delta modulation output? What is optimum step size? How does the optimum step size remove the slop overload distortion? *** q6

The zigzag pattern is introduced in the delta modulation output to reduce the average quantization error. The quantization error is the difference between the original analog signal and the quantized digital signal. The zigzag pattern helps to distribute the quantization error more evenly across the signal, which reduces the overall distortion.

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.

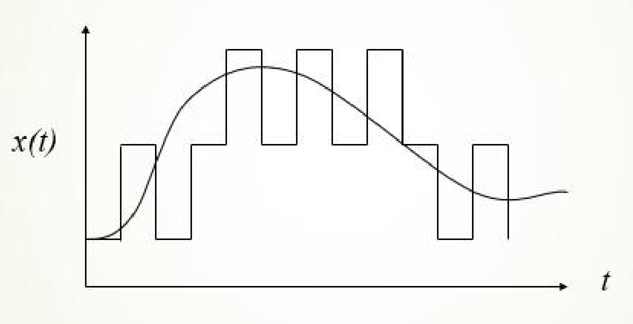


Fig. 21: Output of the demodulator for larger step size

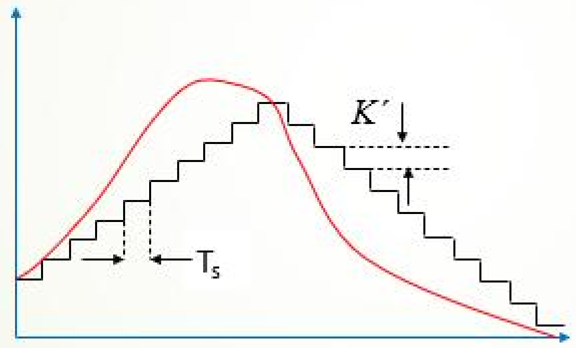


Fig. 22: Output of the demodulator for smaller step size

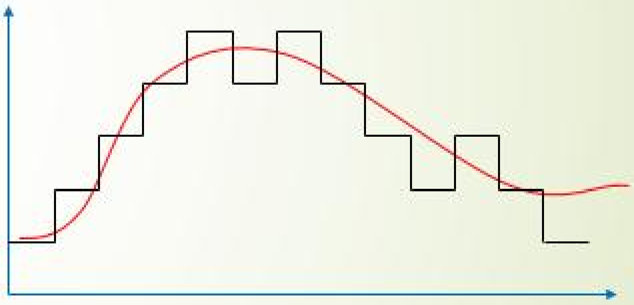


Fig. 23: Output of the demodulator for optimum step size

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. *** q6

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(θ) = K/T_s = kf_s = k8000

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

Q. With an appropriate figure, describe the Delta Modulation Technique. How the predictor circuit plays a major role in modulation process? *** q6

- ✓ Delta modulation is a simple form of analog-to-digital conversion that uses a one-bit quantizer to represent the difference between consecutive samples of an analog signal. The technique involves comparing the input signal with the predicted value and encoding the difference as either a positive or negative change.
- ✓ When sample to sample difference is expressed by a single bit then the modulation scheme is called ***delta modulation*** is considered as an special case of DPCM.

Major components of transmitter and receiver of delta modulation are *sampler*, *predictor*, *quantizer*, *adder* and *smoothing filter* shown in Fig. 18. In transmitter, the analog baseband signal *x(t)* is sampled and a difference signal, is generated. Here is j^{th} sampled pulse of *x(t)* is x_j and g_j is j^{th} predicted pulse.

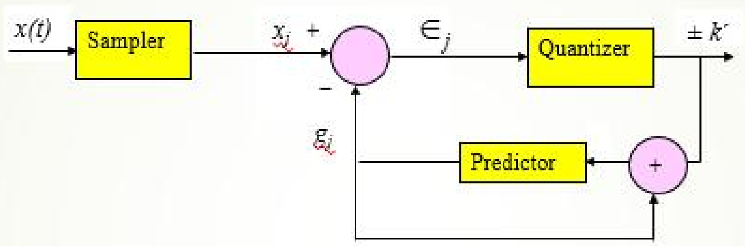


Fig. 18(a): Delta modulator

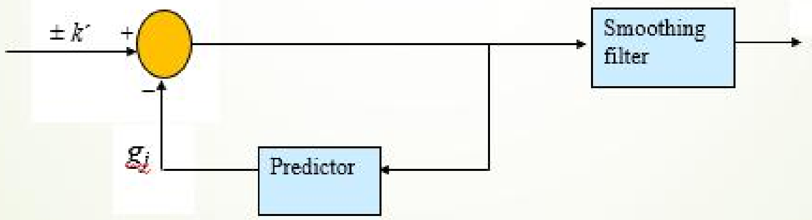


Fig. 18(b): Delta demodulator

Predicted pulse is determined from linear combination of some previous sampled pulses shown in Fig. 19 is expressed as,

$$g_j = \sum_{s=1}^{k} h_s \hat{x}_{j-s}$$

where $\hat{x}_j$ is the jth estimated sample determined as, $g \pm k'$

Based on difference signal $\in_j$ a pulse of amplitude k' is generated by a quantizer like,

$$P_j = \begin{cases} k' & if \in_j \ is \ positive \\ -k' \, if \in_j & is \ negative \end{cases}$$

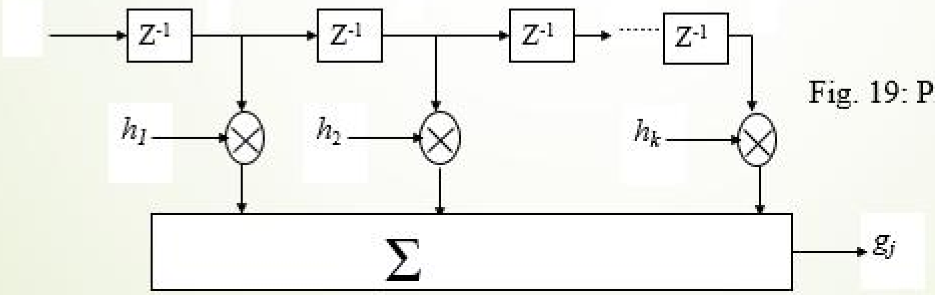


Fig. 19: Predictor circuit

Q. Write down the name of different digital modulation technique. Why do we prefer digital modulation in data transmission process? *** q8

There are several different digital modulation techniques used in data transmission. Some of the commonly used ones include:

1. **Amplitude Shift Keying (ASK):** This modulation technique varies the amplitude of the carrier signal to represent digital data.
2. **Frequency Shift Keying (FSK):** FSK modulates the carrier signal by varying its frequency to encode digital information.
3. **Phase Shift Keying (PSK):** PSK alters the phase of the carrier signal to represent different digital symbols.
4. **Quadrature Amplitude Modulation (QAM):** QAM combines amplitude and phase modulation, allowing multiple bits to be transmitted simultaneously.
5. **Orthogonal Frequency Division Multiplexing (OFDM):** OFDM divides the data into multiple narrowband subcarriers, each carrying a portion of the information.

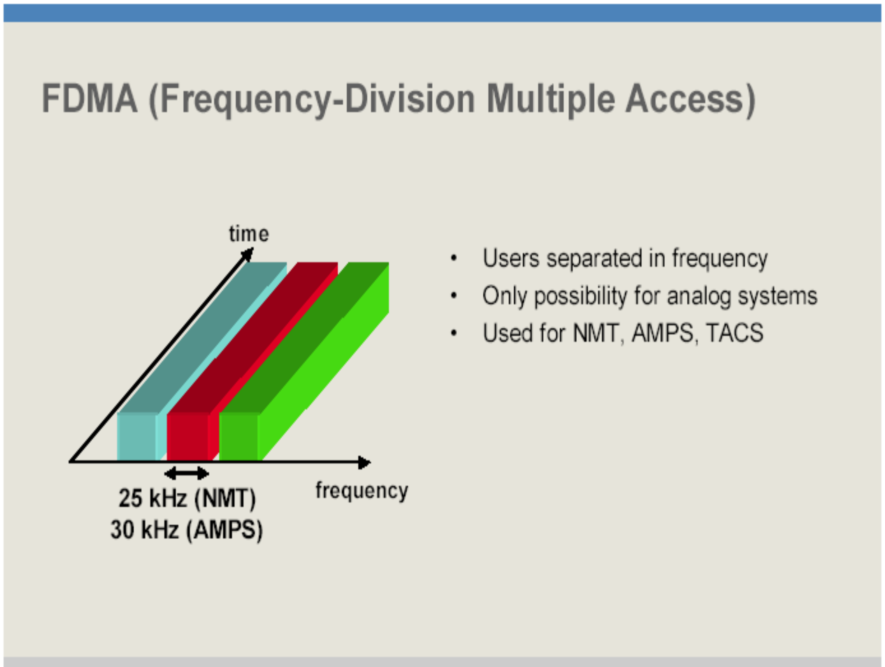
Digital modulation is preferred in data transmission for several reasons:

1. **Noise Immunity:** Digital modulation techniques are more resilient to noise and interference compared to analog modulation. Digital signals can be easily detected and decoded, allowing for more reliable transmission in noisy environments.
2. **Error Detection and Correction:** Digital modulation allows the implementation of error detection and correction techniques, such as error-correcting codes. These techniques enable the receiver to detect and correct errors introduced during transmission, ensuring high data integrity.
3. **Data Compression:** Digital modulation enables the use of data compression techniques, which reduce the amount of bandwidth required for transmission. This is particularly beneficial in scenarios where limited bandwidth is available or where efficient utilization of the available bandwidth is desired.
4. **Multiplexing:** Digital modulation allows for efficient multiplexing of multiple signals on a single channel. Techniques like time-division multiplexing (TDM) and frequency-division multiplexing (FDM) can be easily implemented with digital modulation, enabling simultaneous transmission of multiple data streams.
5. **Flexibility and Compatibility:** Digital modulation techniques are highly flexible and can accommodate various data formats, including voice, video, and data. They can be easily integrated with different types of networks and communication systems, making them compatible with a wide range of devices and applications.

Overall, digital modulation offers improved reliability, error detection and correction capabilities, efficient bandwidth utilization, and compatibility with various data formats. These advantages make it a preferred choice in modern data transmission processes.

Q. Give a comparative study among FDMA, TDMA and CDMA. With necessary Figures, describe the working principle of FDM technique. *** q8

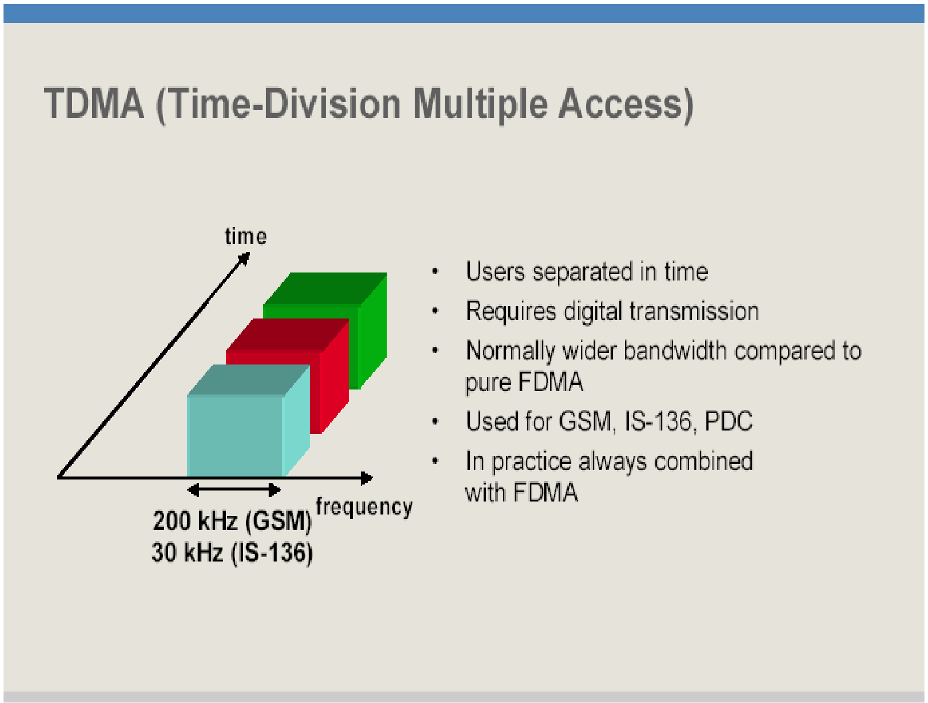
Frequency-division multiple access (FDMA): In FDMA, each user is assigned a unique frequency band. This ensures that no two users will interfere with each other. FDMA is a good choice for applications where there are a limited number of users and each user needs a large amount of bandwidth.



FDMA (Frequency-Division Multiple Access)

- Users separated in frequency
- Only possibility for analog systems
- Used for NMT, AMPS, TACS

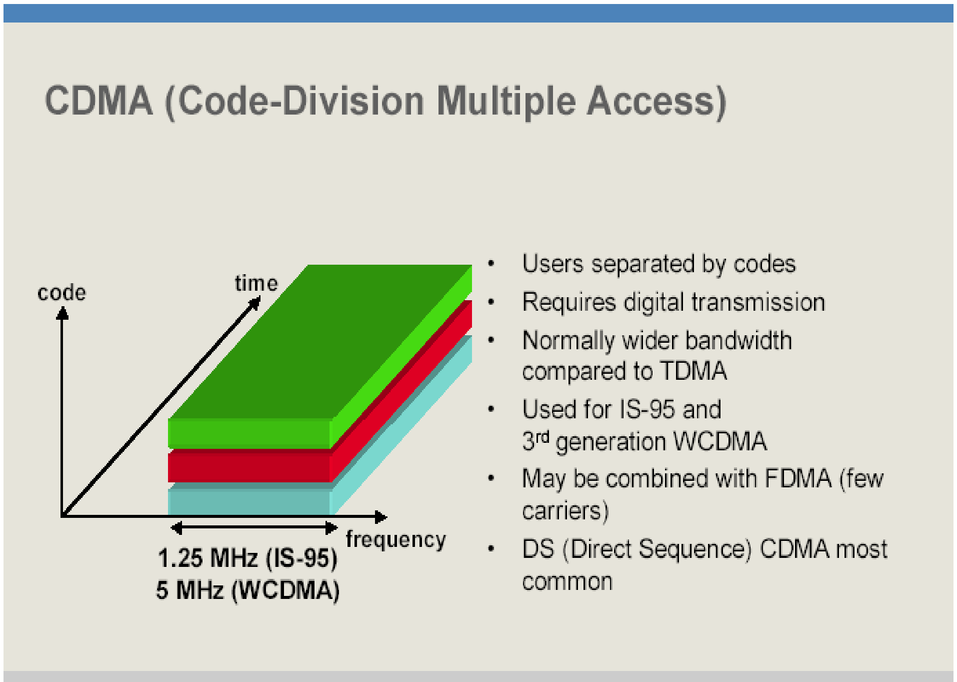
Time-division multiple access (TDMA): In TDMA, each user is assigned a unique time slot. This ensures that no two users will transmit at the same time. TDMA is a good choice for applications where there are a large number of users and each user only needs a small amount of bandwidth.



TDMA (Time-Division Multiple Access)

- Users separated in time
- Requires digital transmission
- Normally wider bandwidth compared to pure FDMA
- Used for GSM, IS-136, PDC
- In practice always combined with FDMA

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.



CDMA (Code-Division Multiple Access)

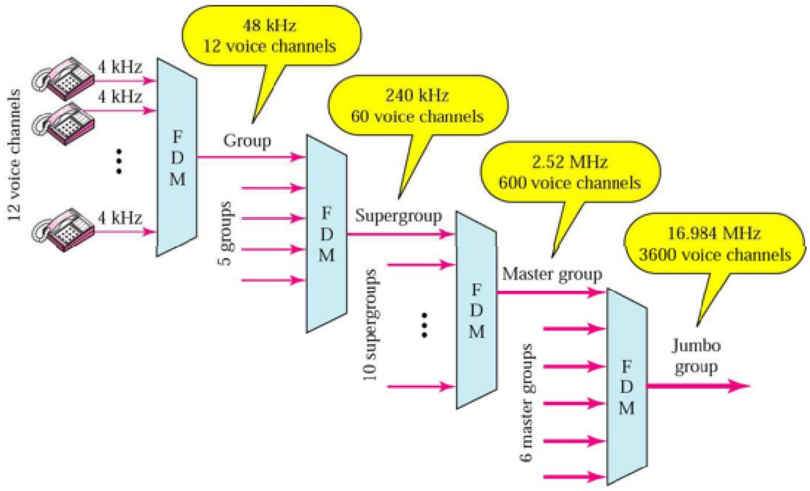
- Users separated by codes
- Requires digital transmission
- Normally wider bandwidth compared to TDMA
- Used for IS-95 and 3rd generation WCDMA
- May be combined with FDMA (few carriers)
- DS (Direct Sequence) CDMA most common

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

Frequency Division Multiplexing

- In telecommunications, **frequency Division multiplexing** (**FDM**) is a technique by which the total bandwidth available in a communication medium is divided into a series of non-overlapping frequency sub-bands, each of which is used to carry a separate signal.



Frequency Division Multiplexing

Examples of FDM

- As an example of an FDM system, Commercial broadcast radio (AM and FM radio) simultaneously transmits multiple signals or "stations" over the airwaves. These stations each get their own frequency band to use, and a radio can be tuned to receive each different station.
- Another good example is cable television, which simultaneously transmits every channel, and the TV "tunes in" to which channel it wants to watch.

Q. How does the scrambling technique avoid the bandwidth wastage? In which type of data communication, the scrambling technique is a must and why? *** q7

Scrambling is a technique used to alter the original data signal in a controlled manner. This is done by applying a pseudo-random sequence to the data signal. The scrambling process ensures that the data signal is spread out evenly across the available bandwidth. This helps to avoid bandwidth wastage, which can occur when the data signal is concentrated in a narrow band of frequencies.

Scrambling is a must in some types of data communication, such as digital cellular networks. This is because the data signals in these networks are very narrowband and can easily be interfered with by other signals. Scrambling helps to spread out the data signals and make them less susceptible to interference.

Here are some of the benefits of scrambling:

- Avoids bandwidth wastage
- Makes the data signal less susceptible to interference
- Improves the security of the data signal

Here are some of the drawbacks of scrambling:

- Increases the complexity of the system
- Can introduce some distortion to the data signal

Overall, scrambling is a useful technique that can be used to improve the performance of data communication systems.

Here are some examples of data communication systems that use scrambling:

- Digital cellular networks
- Satellite communications
- Data links
- Military communications

In digital cellular networks, scrambling is used to spread the data signals across the available bandwidth. This helps to avoid interference from other signals and improves the quality of the received signal.

In satellite communications, scrambling is used to protect the data signals from unauthorized access. This is done by using a secret scrambling code that is known only to the authorized users.

In data links, scrambling is used to improve the security of the data signals. This is done by using a scrambling code that is known only to the sender and receiver.

In military communications, scrambling is used to protect the data signals from enemy interception. This is done by using a scrambling code that is known only to the authorized users.