# Krupanidhi Degree College

# Sessional 2 Question Bank

# Data Communications and Network

**2 MARKS QUESTIONS**

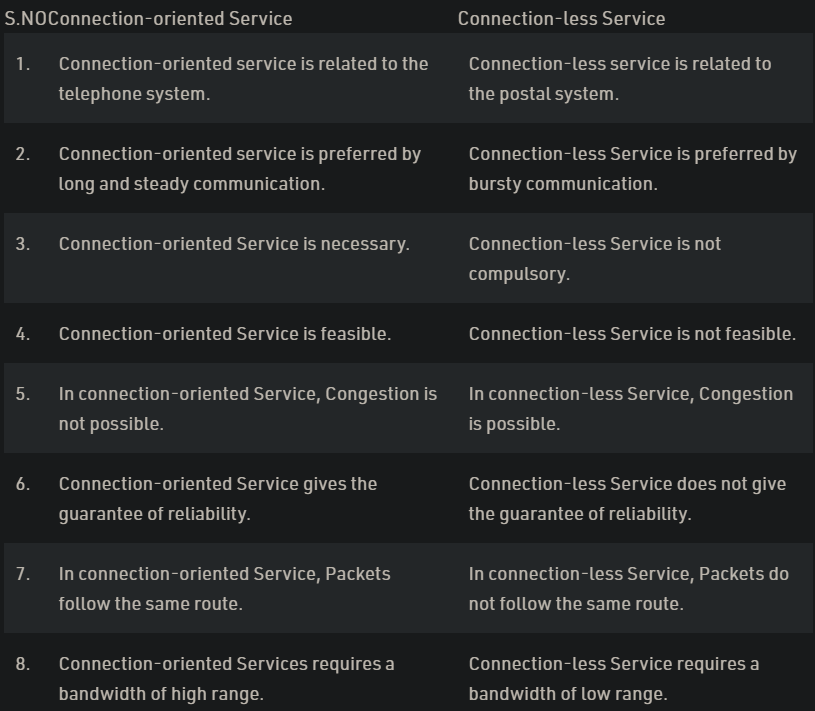
1. Define pipelining. - pipelining is the method of sending multiple data units without waiting for an acknowledgment for the first frame sent. Pipelining ensures better utilization of network resources and also increases the speed of delivery, particularly in situations where a large number of data units make up a message to be sent.
2. Define framing. - Framing is a point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits.
3. Define ALOHA. List its types. - ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. There are two types -
   1. Pure ALOHA
   2. Slotted ALOHA
4. Define packet switching. - Packet switching is a connectionless network switching technique. The message is divided and grouped into a number of units called packets that are individually routed from the source to the destination. There is no need to establish a dedicated circuit for communication.
5. Mention various types of bridges.

* **Transparent bridge**—A transparent bridge is invisible to the other devices on the network.
* **Translational bridge**—A translational bridge can convert from one networking system to another. As you might have guessed, it translates the data it receives.
* **Source-route bridge**—Source-route bridges were designed by IBM for use on Token Ring networks. The source-route bridge derives its name from the fact that the entire route of the frame is embedded within the frame

1. Define random access protocols. List them - Random access protocols assign uniform priority to all connected nodes. Any node can send data if the transmission channel is idle. No fixed time or fixed sequence is given for data transmission. The four random access protocols are−
   1. ALOHA
   2. Carrier sense multiple access (CMSA)
   3. Carrier sense multiple access with collision detection (CMSA/CD)
   4. Carrier sense multiple access with collision avoidance (CMSA/CA)
2. Define controlled access protocols. List them. - Controlled access protocols allow only one node to send data at a given time. Before initiating transmission, a node seeks information from other nodes to determine which station has the right to send. This avoids collision of messages on the shared channel. The station can be assigned the right to send by the following three methods−
   1. Reservation
   2. Polling
   3. Token Passing
3. Define piggy backing - In two-way communication, whenever a frame is received, the receiver waits and does not send the control frame back to the sender immediately. The receiver waits until its network layer passes in the next data packet. The delayed acknowledgement is then attached to this outgoing data frame. This technique of temporarily delaying the acknowledgement so that it can be hooked with next outgoing data frame is known as piggybacking.
4. Define FDDI - Fiber Distributed Data Interface, or FDDI, is a high-speed network technology which runs at 100 Mbps over fiber-optic cabling, often used for network backbones in a local area network (LAN) or metropolitan area network (MAN).

[Extra explanation: Fiber Distributed Data Interface (FDDI) is usually implemented as a dual token-passing ring within a ring topology (for campus networks) or star topology (within a building). The dual ring consists of a primary and secondary ring. The primary ring carries data. The counter-rotating secondary ring can carry data in the opposite direction, but is more commonly reserved as a backup in case the primary ring goes down.]

1. Define multiple access communication -
2. Mention the functions of packet switching. - Packet Switching uses Store and Forward technique while switching the packets; while forwarding the packet each hop first store that packet then forward. This technique is very beneficial because packets may get discarded at any hop due to some reason. More than one path is possible between a pair of source and destination. Each packet contains Source and destination address using which they independently travel through the network.
3. Compare connection-oriented and connectionless service. -



1. Expand FDDI and CSMA -
   1. Fiber Distributed Data Interface
   2. Carrier Sense Multiple Access
2. Define Ethernet - Ethernet is a family of wired computer networking technologies commonly used in local area networks, metropolitan area networks and wide area networks.
3. Expand HDLC and PPP -
   1. High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.
   2. Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds. Since it is a data link layer protocol, data is transmitted in frames.
4. Define polling - couldn’t find proper definition
5. Define reservation - Reservation protocols are the class of protocols in which the stations wishing to transmit data broadcast themselves before actual transmission. These protocols operate in the medium access control (MAC) layer and transport layer of the OSI model.
6. Define stop and wait ARQ - Stop-and-wait ARQ, also referred to as alternating bit protocol, is a method to send information between two connected devices. It ensures that information is not lost due to dropped packets and that packets are received in the correct order.
7. Define CSMA and CDMA/CD –

CSMA/CD stands for Carrier Sense Multiple Access/Collision Detection. It is a widely used MAC protocol. Its specifications have been standardized by the IEEE 802.3 standard.

Code Division Multiple Access (CDMA) is a sort of multiplexing that facilitates various signals to occupy a single transmission channel. It optimizes the use of available bandwidth. The technology is commonly used in ultra-high-frequency (UHF) cellular telephone systems, bands ranging between the 800-MHz and 1.9-GHz.

1. Mention the advantages of CDMA - CDMA has a soft capacity. The greater the number of codes, the more the number of users. It has the following advantages −
   1. CDMA requires a tight power control, as it suffers from near-far effect. In other words, a user near the base station transmitting with the same power will drown the signal latter. All signals must have more or less equal power at the receiver
   2. Rake receivers can be used to improve signal reception. Delayed versions of time (a chip or later) of the signal (multipath signals) can be collected and used to make decisions at the bit level.
   3. Flexible transfer may be used. Mobile base stations can switch without changing operator. Two base stations receive mobile signal and the mobile receives signals from the two base stations.
   4. Transmission Burst − reduces interference.
2. Define Go-back-N ARQ protocol. - Go-Back-N ARQ is a specific instance of the automatic repeat request protocol, in which the sending process continues to send a number of frames specified by a window size even without receiving an acknowledgement packet from the receiver.
3. Define HDLC with Frame format - High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.

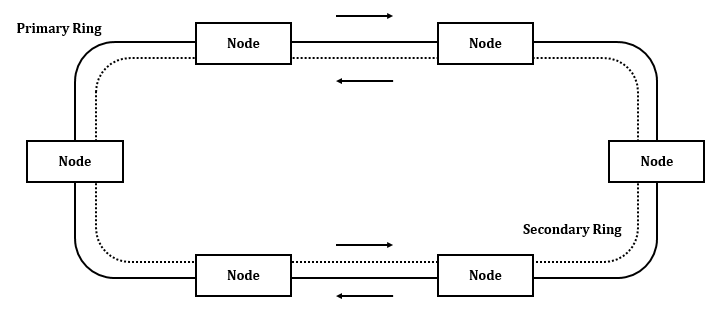
**5 OR 10 OR 15 MARKS QUESTIONS:**

1. **Explain FDDI with neat diagram.**

Fiber Distributed Data Interface (FDDI) is a set of ANSI and ISO standards for transmission of data in local area network (LAN) over fiber optic cables. It is applicable in large LANs that can extend up to 200 kilometers in diameter.

## Features

* FDDI uses optical fiber as its physical medium.
* It operates in the physical and medium access control (MAC layer) of the Open Systems Interconnection (OSI) network model.
* It provides high data rate of 100 Mbps and can support thousands of users.
* It is used in LANs up to 200 kilometers for long distance voice and multimedia communication.
* It uses ring based token passing mechanism and is derived from IEEE 802.4 token bus standard.
* It contains two token rings, a primary ring for data and token transmission and a secondary ring that provides backup if the primary ring fails.
* FDDI technology can also be used as a backbone for a wide area network (WAN).



1. **Explain the working of packet switch network with neat diagram.**

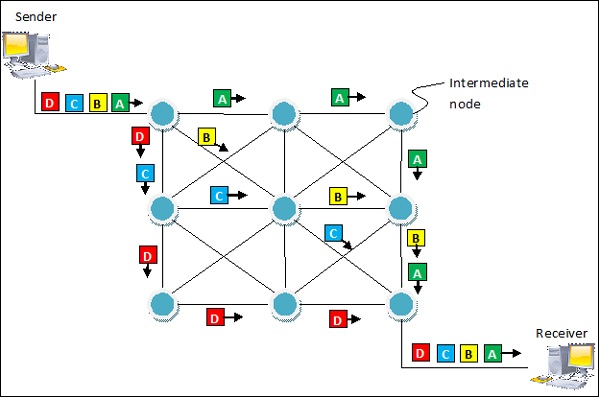
Packet switching is a connectionless network switching technique. Here, the message is divided and grouped into a number of units called packets that are individually routed from the source to the destination. There is no need to establish a dedicated circuit for communication.

## Process

Each packet in a packet switching technique has two parts: a header and a payload. The header contains the addressing information of the packet and is used by the intermediate routers to direct it towards its destination. The payload carries the actual data.

A packet is transmitted as soon as it is available in a node, based upon its header information. The packets of a message are not routed via the same path. So, the packets in the message arrives in the destination out of order. It is the responsibility of the destination to reorder the packets in order to retrieve the original message.

The process is diagrammatically represented in the following figure. Here the message comprises of four packets, A, B, C and D, which may follow different routes from the sender to the receiver.



## Advantages and Disadvantages of Packet Switching

## Advantages

* Delay in delivery of packets is less, since packets are sent as soon as they are available.
* Switching devices don’t require massive storage, since they don’t have to store the entire messages before forwarding them to the next node.
* Data delivery can continue even if some parts of the network faces link failure. Packets can be routed via other paths.
* It allows simultaneous usage of the same channel by multiple users.
* It ensures better bandwidth usage as a number of packets from multiple sources can be transferred via the same link.

## Disadvantages

* They are unsuitable for applications that cannot afford delays in communication like high quality voice calls.
* Packet switching high installation costs.
* They require complex protocols for delivery.
* Network problems may introduce errors in packets, delay in delivery of packets or loss of packets. If not properly handled, this may lead to loss of critical information.

1. **Explain Stop and wait ARQ with neat diagram.**

**Stop & Wait ARQ**

Stop & Wait ARQ is a **sliding window protocol**for flow control and it overcomes the limitations of Stop & Wait, we can say that it is the improved or modified version of Stop & Wait protocol.

Stop & Wait ARQ assumes that the communication channel is noisy (previously Stop & Wait assumed that the communication channel is not noisy). Stop & Wait ARQ also assumes that errors may occur in the data while transmission.

**Working of Stop & Wait ARQ**

Working of Stop & Wait ARQ is almost like Stop & Wait protocol, the only difference is that it includes some additional components, which are:

1. Time out timer
2. Sequence numbers for data packets
3. Sequence numbers for feedbacks

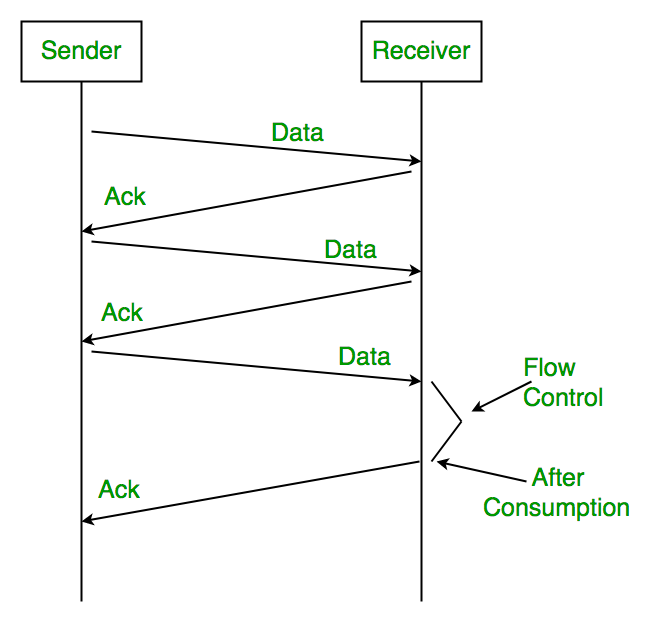
**Note:** If any sliding window protocol must work properly then, the available sequence numbers must be greater than or equal to the sum of sender window size and receiver window size.

**[available sequence numbers >= sender window size + receiver window size]**

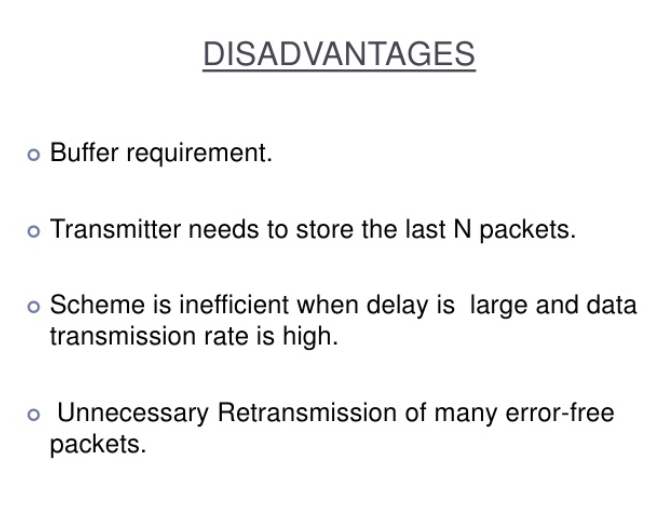
Stop & Wait ARQ is a 1-bit sliding window protocol where the size of the sender window as well as the receiver window is 1. Thus, in Stop & Wait ARQ technique, the minimum number of sequence numbers required is equal to the sum of sender window size & receiver window size

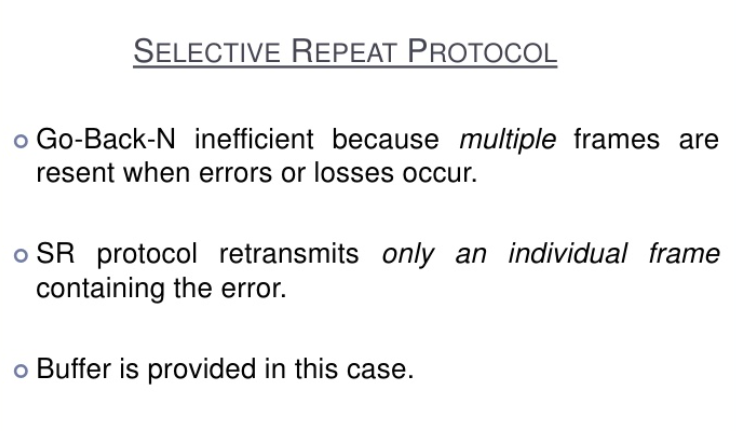
**[minimum number of sequence numbers required = sender window size + receiver window size]**

Thus, the minimum number of sequence numbers required in Stop & Wait ARQ is 2, which are 0 and 1.



1. **List the disadvantages of Go-back-N protocol and explain how it is overcome in selective repeat protocol.**





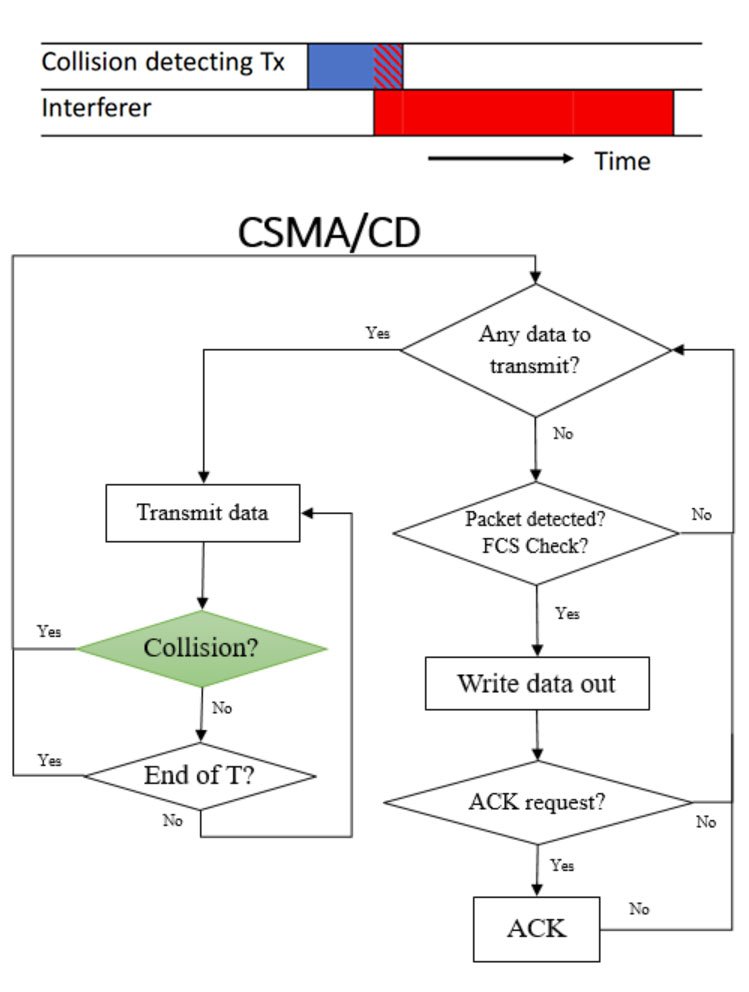
1. **Explain CSMA/CD protocol with neat diagram**.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. It senses or listens whether the shared channel for transmission is busy or not, and defers transmissions until the channel is free. The collision detection technology detects collisions by sensing transmissions from other stations. On detection of a collision, the station stops transmitting, sends a jam signal, and then waits for a random time interval before retransmission.

## Algorithms

The algorithm of CSMA/CD is:

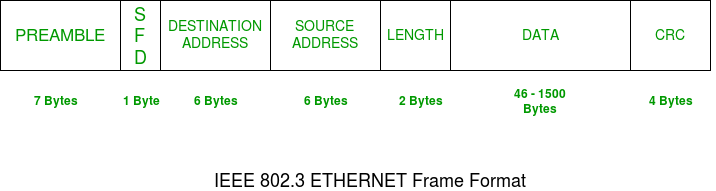
* When a frame is ready, the transmitting station checks whether the channel is idle or busy.
* If the channel is busy, the station waits until the channel becomes idle.
* If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision.
* If a collision is detected, the station starts the collision resolution algorithm.
* The station resets the retransmission counters and completes frame transmission.



1. **Explain IEEE 802.3 frame format with neat diagram.**

Basic frame format which is required for all MAC implementation is defined in **IEEE 802.3 standard**. Though several optional formats are being used to extend the protocol’s basic capability.  
Ethernet frame starts with Preamble and SFD, both works at the physical layer. Ethernet header contains both Source and Destination MAC address, after which the payload of the frame is present. The last field is CRC which is used to detect the error. Now, let’s study each field of basic frame format.

### Ethernet (IEEE 802.3) Frame Format –



* **PREAMBLE –**Ethernet frame starts with 7-Bytes Preamble. This is a pattern of alternative 0’s and 1’s which indicates starting of the frame and allow sender and receiver to establish bit synchronization. Initially, PRE (Preamble) was introduced to allow for the loss of a few bits due to signal delays. But today’s high-speed Ethernet don’t need Preamble to protect the frame bits.  
  PRE (Preamble) indicates the receiver that frame is coming and allow the receiver to lock onto the data stream before the actual frame begins.
* **Start of frame delimiter (SFD) –** This is a 1-Byte field which is always set to 10101011. SFD indicates that upcoming bits are starting of the frame, which is the destination address. Sometimes SFD is considered the part of PRE, this is the reason Preamble is described as 8 Bytes in many places. The SFD warns station or stations that this is the last chance for synchronization.
* **Destination Address –** This is 6-Byte field which contains the MAC address of machine for which data is destined.
* **Source Address –** This is a 6-Byte field which contains the MAC address of source machine. As Source Address is always an individual address (Unicast), the least significant bit of first byte is always 0.
* **Length –**Length is a 2-Byte field, which indicates the length of entire Ethernet frame. This 16-bit field can hold the length value between 0 to 65534, but length cannot be larger than 1500 because of some own limitations of Ethernet.
* **Data –** This is the place where actual data is inserted, also known as **Payload**. Both IP header and data will be inserted here if Internet Protocol is used over Ethernet. The maximum data present may be as long as 1500 Bytes. In case data length is less than minimum length i.e. 46 bytes, then padding 0’s is added to meet the minimum possible length.
* **Cyclic Redundancy Check (CRC) –**CRC is 4 Byte field. This field contains a 32-bits hash code of data, which is generated over the Destination Address, Source Address, Length, and Data field. If the checksum computed by destination is not the same as sent checksum value, data received is corrupted.

1. **Explain the types of aloha with neat diagrams**

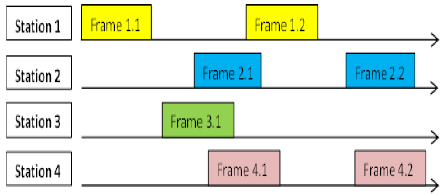
ALOHA one of the major thing needs to be remembered is the transmission of the data. Because whenever both sides or nodes transmits the data there will be data collision. This is a one-directional transmission, If node1 is transmitting the data then node2 should receive the data.

## **There are two types of ALOHA’s**

1. Pure ALOHA.
2. Slotted ALOHA.

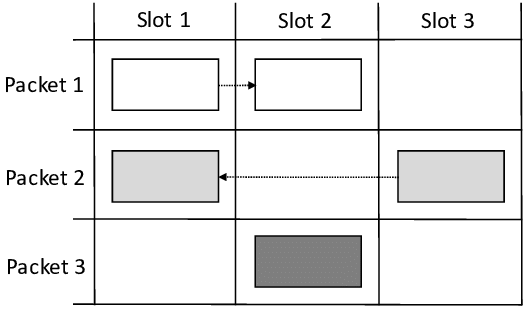
### **Pure ALOHA**

* Applicable to any shared transmission medium.
* When a station has a frame it sends at any time
* The station then listens for an amount of time equal to the Maximum possible round-trip propagation delay on the network plus small fixed time in requirement.
* It receives ACK.
* If not re-transmit it.
* If no ACK after repeated transmission gives up.



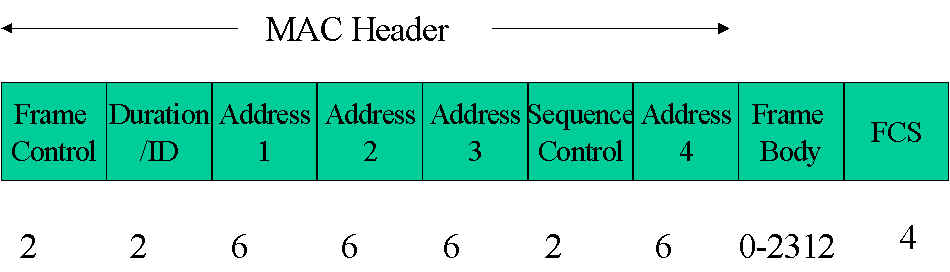
### **Slotted ALOHA**

* Slotted ALOHA was invented to improve the efficiency of pure aloha.
* Divide the time into slots of the frame time & force the station to send only at the beginning of the time slot.

.

1. **Explain IEEE 802.11 frame format with neat diagram.**

* The IEEE 802.11 MAC accepts MSDUs (MAC Service Data Unit) from higher layers in the protocol stack for the purpose of reliably sending those MSDUs to the equivalent layer of the protocol stack in another station.
* MAC adds information to the MSDU in the form of headers & trailers to create an MPDU (MAC Protocol Data Unit).
* MPDU is then passed on to the physical layer to be sent over the wireless medium to the other station.
* MAC may fragment MSDUs into several frames.
* The general IEEE 802.11 frame format is as shown below-



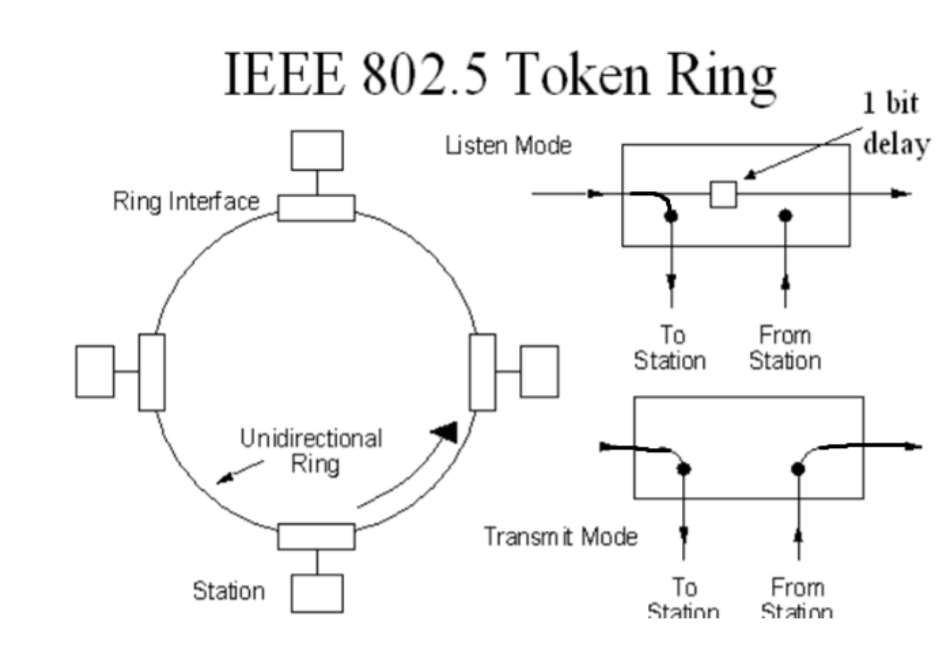
1. **Explain IEEE 802.5 frame format with neat diagram.**

IEEE 802.5 (Token Ring): Ring Topology

* + Shared ring medium: all nodes see all frames
  + Round Robin MAC Protocol: determines which station can transmit
  + A special 3-byte pattern, the token, circulates around the ring perpetually and represents the "right to transmit"
  + This establishes round-robin media access
  + Data flow is unidirectional
  + All data flows in a particular direction around the ring; nodes receive frames from their upstream neighbor and forward them to their downstream neighbor
  + Data rate: 4 or 16 Mbps

The token bit sequence circulates around the ring.

* + Each station forwards the token if it does not have a frame to transmit.
  + A station with data to send seizes the token (repeater now in transmit state) and begins sending it’s frame. It can transmit for length of time called the Token Hold Time (THT) = 10 mseconds.
  + Each station forwards the frame.
  + The destination station notices its address and saves a copy of the frame as it also forwards the frame.
  + When the sender sees its frame return, it drains it from the ring and reinserts a token. When the last bit of the returning frame has been drained, the repeater switches immediately to the listen state.

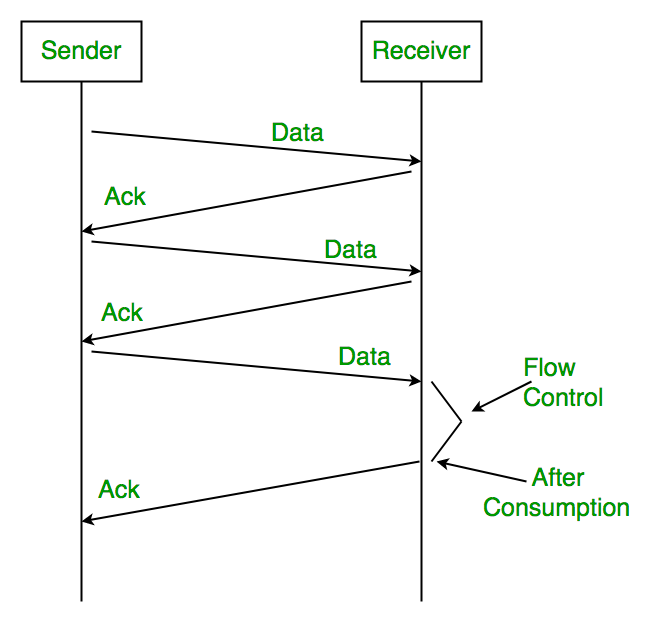


1. **Explain all ARQ protocols with neat diagrams.**

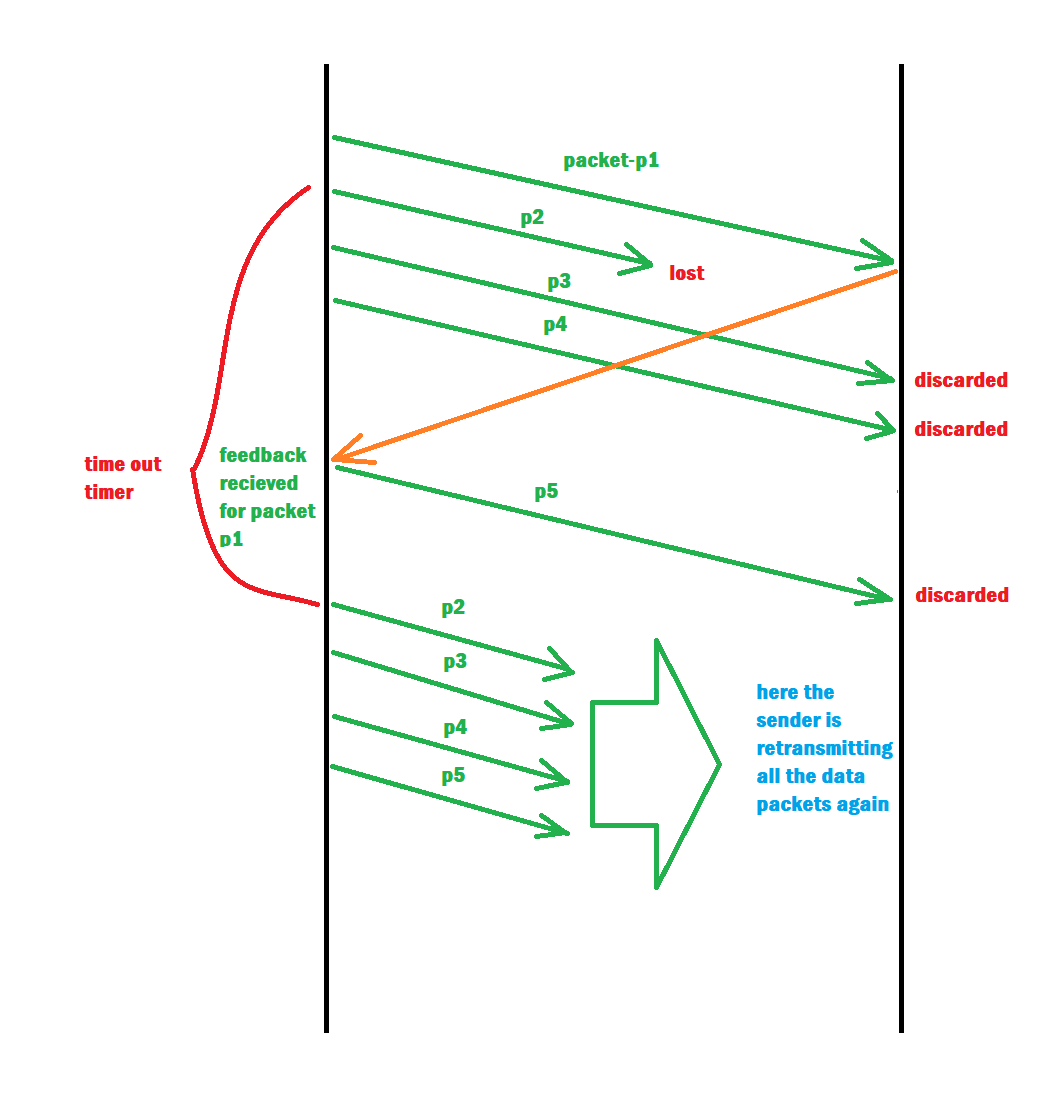
#### Types

There are several types of ways in which these protocols function in the data link layer :

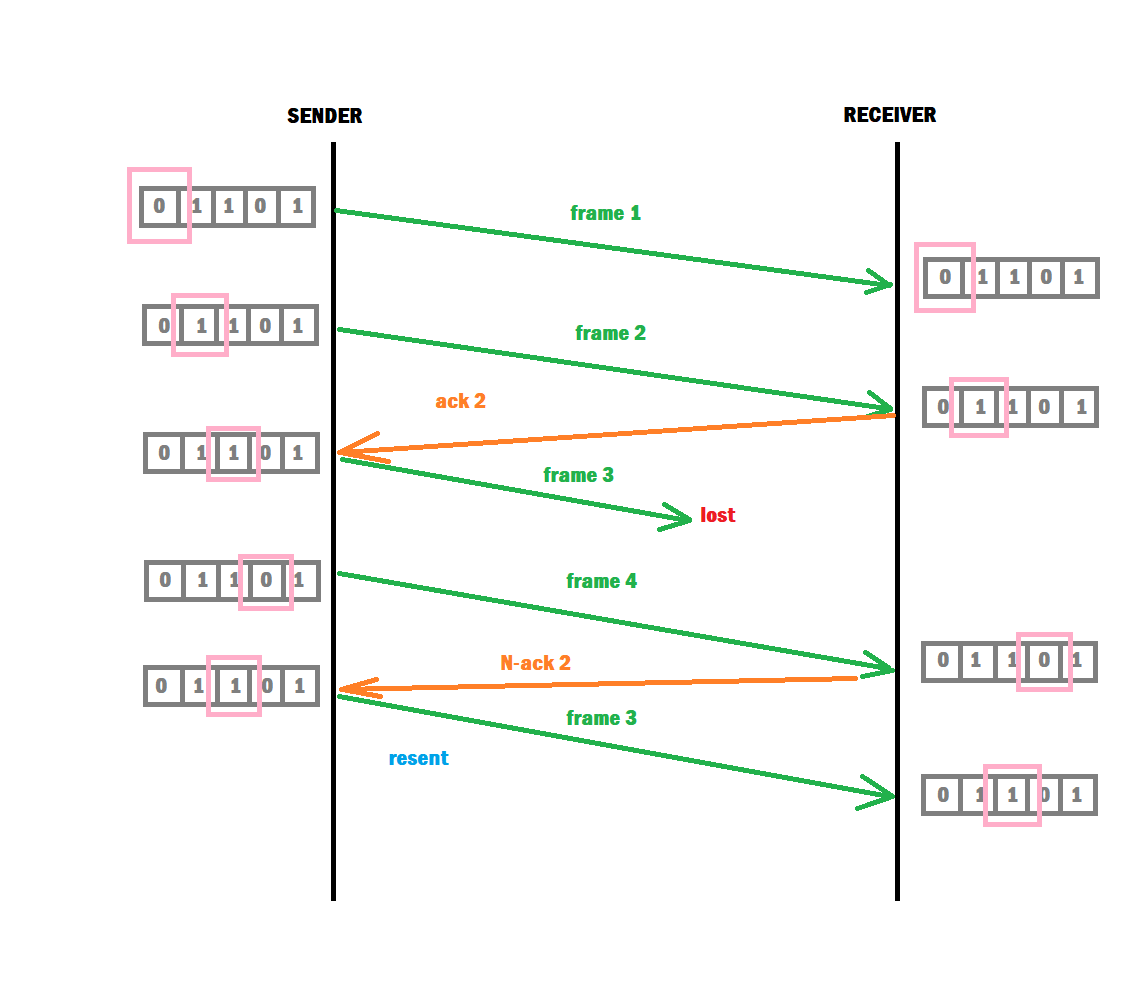
* [Stop And Wait ARQ](https://www.geeksforgeeks.org/stop-and-wait-arq/)**:**  
  Stop and wait ARQ is also referred to as the alternating protocol is a method used in two-way communication systems to send information between two connected devices (sender and a receiver). It is referred to as stop and wait ARQ because the function of this protocol is to send **one frame at a time**. After sending a frame or packet, the sender doesn’t send any further packets until it receives an acknowledgment from the receiver. Moreover, the sender keeps a copy of the sent packet. After receiving the desired frame, the receiver sends an acknowledgment. If the acknowledgment does not reach the sender before the specified time, known as the timeout, the sender sends the same packet again. The timeout is reset after each frame transmission. The above scenario depicts a Stop and wait situation, so this control mechanism is termed as Stop and wait ARQ.



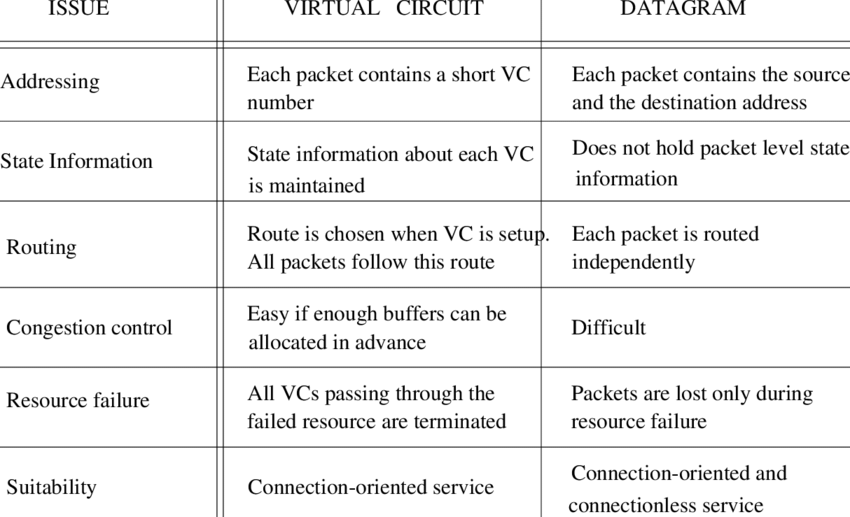
* **Go Back-N ARQ:**  
  Go-Back-N ARQ is a type of the ARQ protocol, in which the sending process continues to **send several frames or packets even without receiving an acknowledgment packet from the receiver**. The receiver process keeps track of the sequence number of the next packet it expects to receive and sends that sequence number with every acknowledgment to the sender. The receiver will remove any packet that does not have the desired sequence number it expects and will resend an acknowledgment for the last correct frame. There are only two possibilities that a frame won’t match the sequence number: it is either a duplicated frame of an existing frame or an out-of-order frame that needs to be sent later, the receiver recognizes this scenario and sends an acknowledgment signal accordingly. Once the sender has sent all of the frames in its window, it will identify that all of the frames since the first lost frame, and will **go back to the sequence number** of the last acknowledgment signal that it received from the receiver pr and continue the process over again. The only drawback of this type of system is that it results in sending packets multiple times: if any frame was lost or found to be corrupted, then that frame and all following frames in the send window will be re-transmitted.  
  This protocol is more efficient than Stop and wait ARQ as there is no waiting time.



* **Selective Repeat ARQ/Selective Reject ARQ:**  
  Selective Repeat ARQ/Selective Reject ARQ protocol mechanism is similar to the Go-Back-N protocol mechanism but in Selective Repeat ARQ the sending process continues even after a frame is found to be corrupt or lost. This is achieved: the receiver process keeps track of the sequence number of the earliest frame it has not received and sends the respective sequence number with the acknowledgment signal. If a frame is not received at the receiver end, the sender continues to send the succeeding frames until it has emptied its window. once this error-correction process has been done, the process continues where it left off. Unlike, Go back-N protocol this does not send a packet multiple times.



1. **List the difference between datagram and virtual circuits.**

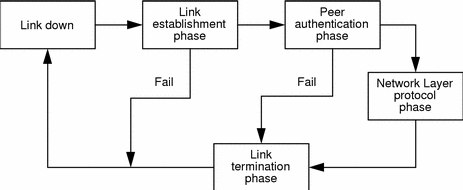


1. **Explain ppp phase diagram**

# PPP Phase Diagram

The process of establishing, maintaining, and terminating PPP links passes through several distinct phases, during which PPP frames are exchanged between the endpoints of the link.

* Link establishment phase
* Peer authentication phase (optional)
* Network layer protocol phase
* Link termination phase



## **Link Establishment Phase**

The Link Control Protocol (LCP) is used to configure the PPP link during the link establishment phase. The configuration parameters are negotiated by an exchange of LCP frames. If the negotiation converges, the link is established and either the authentication protocol or network layer protocol phase is started. If the endpoints fail to negotiate a common configuration for the link, it is closed immediately.

During the link establishment phase only LCP frames should be transmitted in the PPP frames. All other frames are discarded.

## **Peer Authentication Phase (optional)**

Optionally, one or both of the endpoints can request peer authentication. Solstice PPP supports peer authentication based on the Password Authentication Protocol (PAP) and the Challenge-Handshake Authentication Protocol (CHAP). If authentication is successful, the link remains up and the network layer protocol phase is started. If authentication fails, the link termination phase is started to close the link.

During the peer authentication phase only LCP and authentication frames should be transmitted in the PPP frames. All other frames are discarded.

## **Network Layer Protocol Phase**

The Network Control Protocols (NCP) are used to configure the appropriate network layer. Solstice PPP implements the Internet Protocol Control Protocol (IPCP) to configure IP over PPP.

Once the network layer is configured by an exchange of NCP frames, IP datagrams can be encapsulated for transmission across the link. LCP frames may be exchanged periodically to test and maintain the link.

During the network layer protocol phase, LCP, NPC, and IP frames should be transmitted in the PPP frames. All other frames are discarded.

## **Link Termination Phase**

The link may be terminated at any time, at the request of either endpoint. Termination may occur due to authentication failure, carrier loss, or the expiration of the inactivity timeout. Link control protocol (LCP) frames are exchanged to terminate the link.

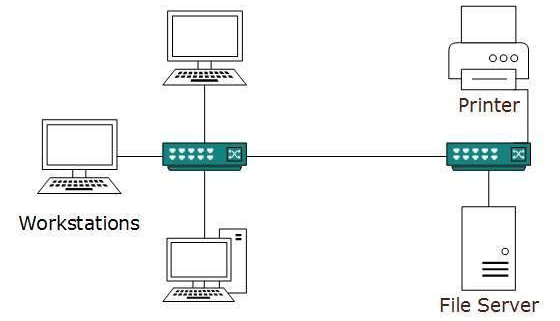
During the link termination phase only LCP frames should be transmitted in the PPP frames. All other frames are discarded.

1. **Summarize on LAN**

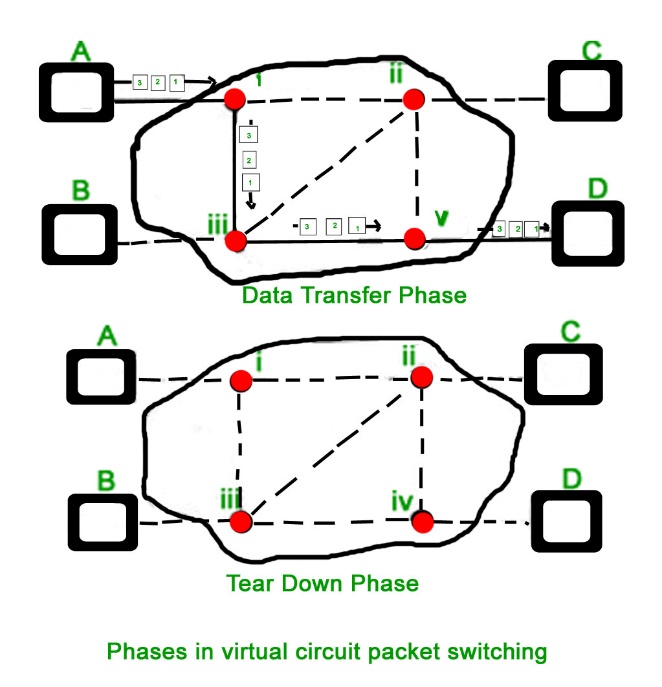
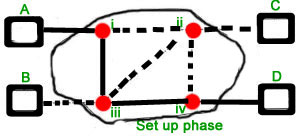
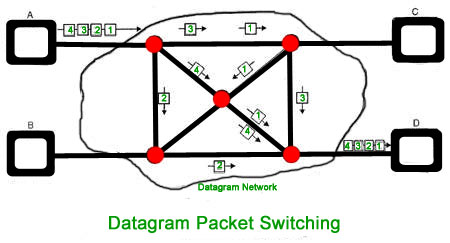
A Local Area Network (LAN) is a private network that connects computers and devices within a limited area like a residence, an office, a building or a campus. On a small scale, LANs are used to connect personal computers to printers. However, LANs can also extend to a few kilometers when used by companies, where a large number of computers share a variety of resources like hardware (e.g. printers, scanners, audiovisual devices etc), software (e.g. application programs) and data.

## The distinguishing features of LAN are

* Network size is limited to a small geographical area, presently to a few kilometers.
* Data transfer rate is generally high. They range from 100 Mbps to 1000 Mbps.
* In general, a LAN uses only one type of transmission medium, commonly category 5 coaxial cables.
* A LAN is distinguished from other networks by their topologies. The common topologies are bus, ring, mesh, and star.
* The number of computers connected to a LAN is usually restricted. In other words, LANs are limitedly scalable.
* IEEE 802.3 or Ethernet is the most common LAN. They use a wired medium in conjuncture with a switch or a hub. Originally, coaxial cables were used for communications. But now twisted pair cables and fiber optic cables are also used. Ethernet’s speed has increased from 2.9 Mbps to 400 Gbps.



1. **Explain types of packet switching with neat diagrams**

* **Connection-oriented Packet Switching (Virtual Circuit) :-** Before starting the transmission, it establishes a logical path or virtual connection using signalling protocol, between sender and receiver and all packets belongs to this flow will follow this predefined route. Virtual Circuit ID is provided by switches/routers to uniquely identify this virtual connection. Data is divided into small units and all these small units are appended with help of sequence number. Overall, three phases takes place here- Setup, data transfer and tear down phase.  
    
  All address information is only transferred during setup phase. Once the route to destination is discovered, entry is added to switching table of each intermediate node. During data transfer, packet header (local header) may contain information such as length, timestamp, sequence number etc.  
  Connection-oriented switching is very useful in switched WAN. Some popular protocols which use Virtual Circuit Switching approach are X.25, Frame-Relay, ATM and MPLS(Multi-Protocol Label Switching).
* **Connectionless Packet Switching (Datagram) :-** Unlike Connection-oriented packet switching, In Connectionless Packet Switching each packet contains all necessary addressing information such as source address, destination address and port numbers etc. In Datagram Packet Switching, each packet is treated independently. Packets belonging to one flow may take different routes because routing decisions are made dynamically, so the packets arrived at destination might be out of order. It has no connection setup and teardown phase, like Virtual Circuits.  
  Packet delivery is not guaranteed in connectionless packet switching, so the reliable delivery must be provided by end systems using additional protocols.  
  

1. **Explain LLC layer.**

### **The Logical Link Control Layer**

The Logical Link Control (LLC) layer provides the major interface between the hardware below and the software layers above. Because it sits between the protocols in the MAC layer that regulate access to transmission media and the rest of the protocol stack, the LLC layer lets the upper layers communicate with any form of transmission media in the same way.

The LLC layer receives an IP packet from the Internet layer and formats it into frames, the units that will be sent across the physical media. The organization of a frame, however, depends on the type of MAC protocol that will be used. This means that the LLC is hardware-dependent, unlike the upper layers in the protocol stack.

LLC layer protocols include specifications for the frames of many types of physical networks, including Ethernet, [Token Ring](https://www.sciencedirect.com/topics/computer-science/token-ring) (rarely used today because it has become nearly impossible to find parts to maintain the hardware), and FDDI (Fiber Distributed Data Interface).

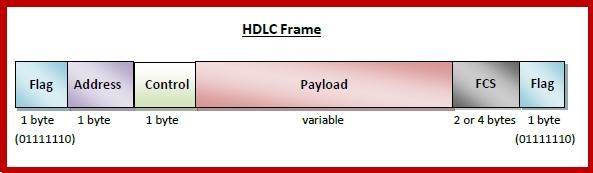
1. **Explain HDLC frame format**

High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.

## HDLC Frame

HDLC is a bit - oriented protocol where each frame contains up to six fields. The structure varies according to the type of frame. The fields of a HDLC frame are −

* **Flag** − It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
* **Address** − It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
* **Control** − It is 1 or 2 bytes containing flow and error control information.
* **Payload** − This carries the data from the network layer. Its length may vary from one network to another.
* **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



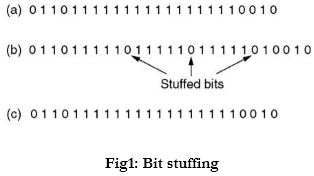
1. **Compare random access and scheduling approaches.**

* The two classes of medium access control schemes, random access and scheduling, differ in major ways, but they also share many common features. Their differences stem primarily from their very different points of departure. Scheduling techniques have their origins in reservation systems that attempt to emulate the performance of a centrally scheduled system such as a multiplexer. Random access techniques, on the other hand, have their origins in the ALOHA scheme that involves transmitting immediately, and subsequently at random times in response to collisions. The scheduling approach provides methodical orderly access to the medium, whereas random access provides a somewhat chaotic, uncoordinated, and unordered access. The scheduling approach has less variability in the delays encountered by packets and therefore has an edge in supporting applications with stringent delay requirements. On the other hand, when bandwidth is plentiful, random access systems can provide very small delays as long as the systems are operated with light loads.
* Both random access and scheduling schemes have the common feature that channel bandwidth is used to provide information that controls the access to the channel. In the case of rescheduling systems, the channel bandwidth carries explicit information that allows stations to schedule their transmissions. In the case of random access systems, channel bandwidth is used in collisions to alert stations of the presence of other transmissions and of the need to spread out their transmissions in time. Indeed, the contention process in CSMA-CD amounts to a distributed form of scheduling to determine which station should transmit next.

1. **Explain bit stuffing and byte stuffing.**

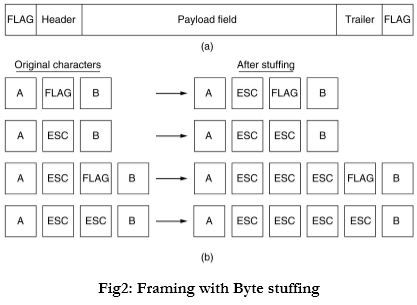
**Bit stuffing:**

* Allows frame to contain arbitrary number of bits and arbitrary character size. The frames are separated by separating flag.
* Each frame begins and ends with a special bit pattern, 01111110 called a flag byte. When five consecutive l's are encountered in the data, it automatically stuffs a '0' bit into outgoing bit stream.
* In this method, frames contain an arbitrary number of bits and allow character codes with an arbitrary number of bits per character. In his case, each frame starts and ends with a special bit pattern, 01111110.
* In the data a 0 bit is automatically stuffed into the outgoing bit stream whenever the sender's data link layer finds five consecutive 1s.
* This bit stuffing is similar to byte stuffing, in which an escape byte is stuffed into the outgoing character stream before a flag byte in the data.
* When the receiver sees five consecutive incoming i bits, followed by a o bit, it automatically destuffs (i.e., deletes) the 0 bit. Bit Stuffing is completely transparent to network layer as byte stuffing. The figure1 below gives an example of bit stuffing.
* This method of framing finds its application in networks in which the change of data into code on the physical medium contains some repeated or duplicate data. For example, some LANs encodes bit of data by using 2 physical bits.

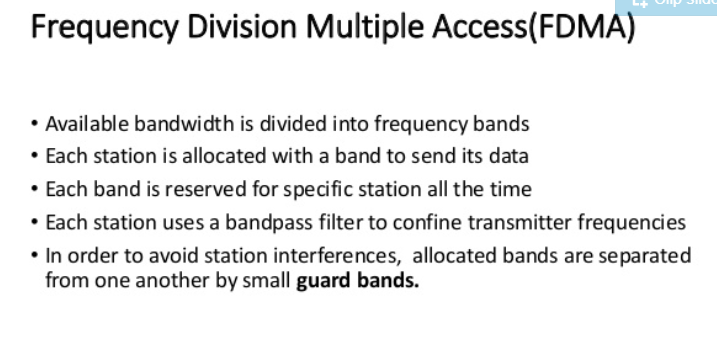


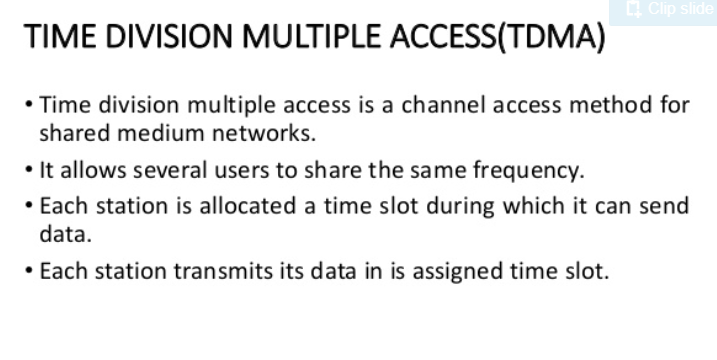
**Byte stuffing:**

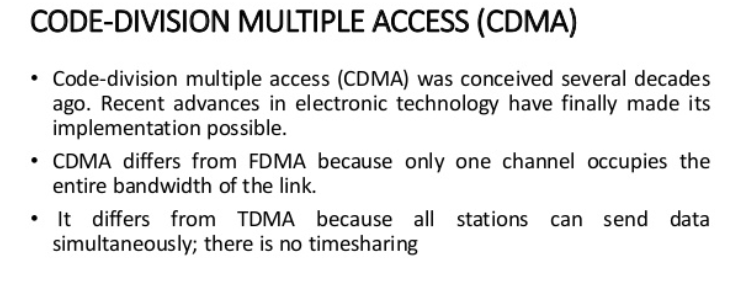
* In this method, start and end of frame are recognized with the help of flag bytes. Each frames starts with and ends with a flag byte. Two consecutive flag bytes indicate the end of one frame and start of the next one. The flag bytes used in the figure 2 used is named as “ESC” flag byte.
* A frame delimited by flag bytes. This framing method is only applicable in 8-bit character codes which are a major disadvantage of this method as not all character codes use 8-bit characters e.g. Unicode.
* Four example of byte sequences before and after stuffing:



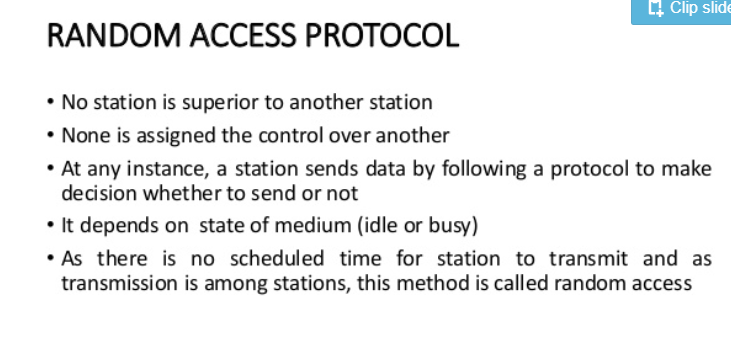
1. **Explain three types of channelization methods with neat diagrams.**

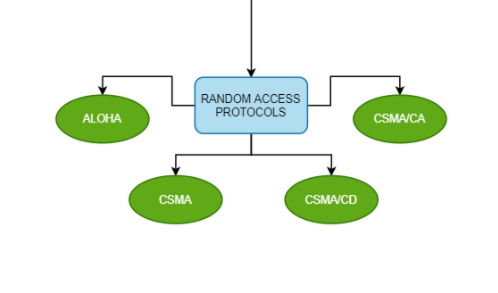






1. **Explain random access protocols with neat diagram.**





1. **Explain controlled/ scheduling approaches with neat diagrams**

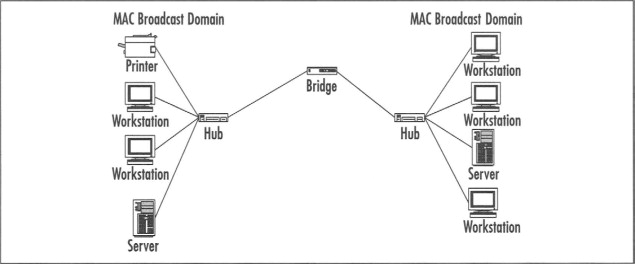
**Not sure**

1. **Explain types of bridges with neat diagram.**

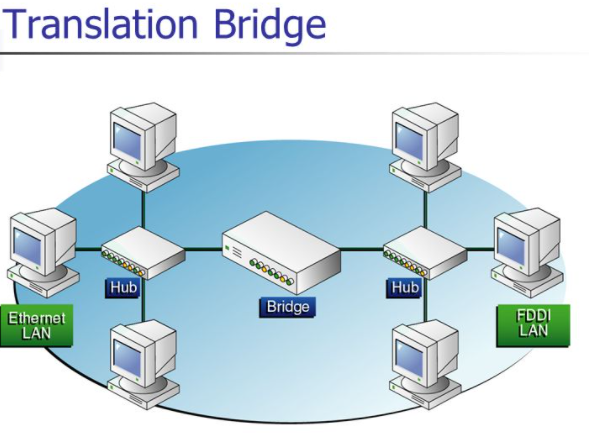
### Types of Bridges

Three types of bridges are used in networks. You don’t need detailed knowledge of how each bridge works, but you should have an overview:

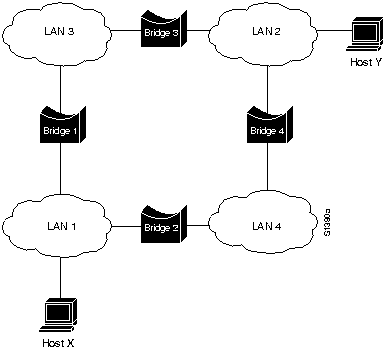
* **Transparent bridge**—A transparent bridge is invisible to the other devices on the network. Transparent bridges perform only the function of blocking or forwarding data based on the MAC address; the devices on the network are oblivious to these bridges’ existence. Transparent bridges are by far the most popular types of bridges.



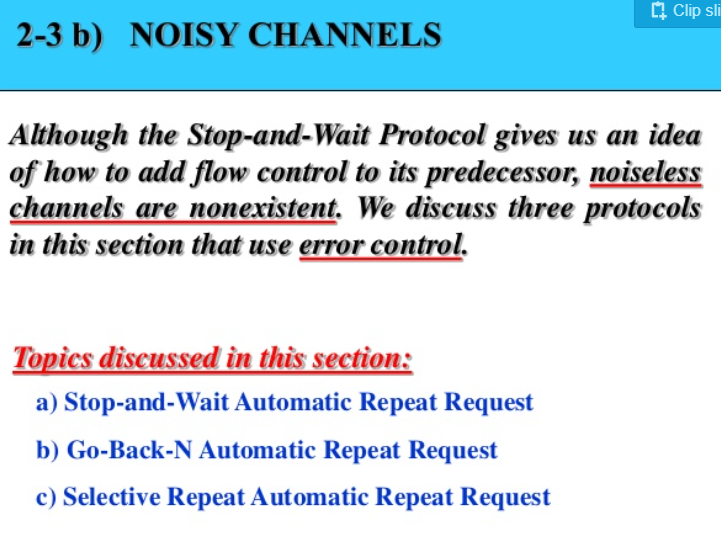
* **Translational bridge**—A translational bridge can convert from one networking system to another. As you might have guessed, it translates the data it receives. Translational bridges are useful for connecting two different networks, such as Ethernet and Token Ring networks. Depending on the direction of travel, a translational bridge can add or remove information and fields from the frame as needed.

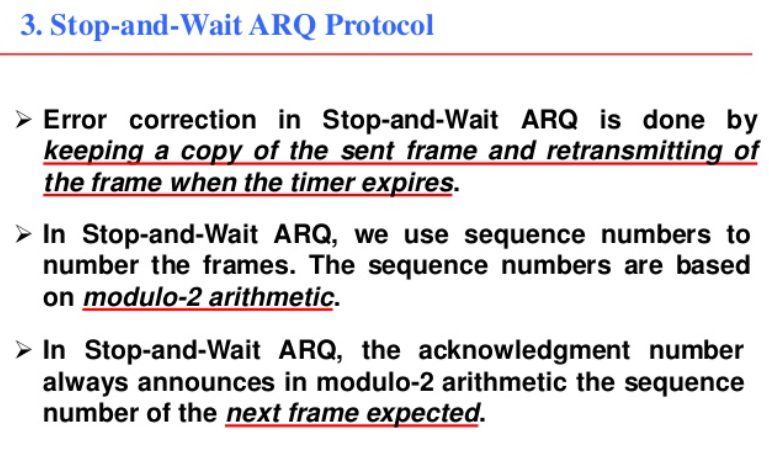


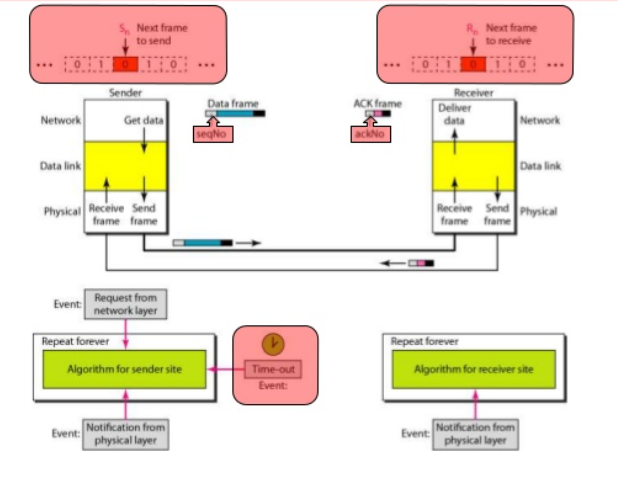
* **Source-route bridge**—Source-route bridges were designed by IBM for use on Token Ring networks. The source-route bridge derives its name from the fact that the entire route of the frame is embedded within the frame. This allows the bridge to make specific decisions about how the frame should be forwarded through the network. The diminishing popularity of Token Ring makes the chances that you’ll work with a source-route bridge very slim.

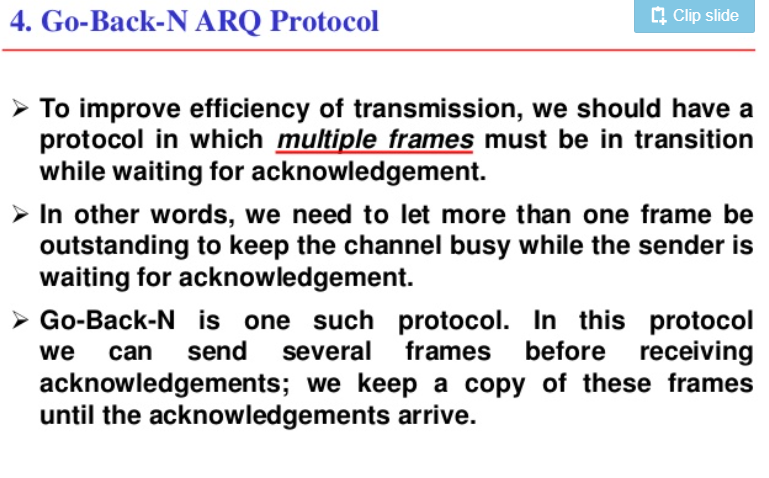


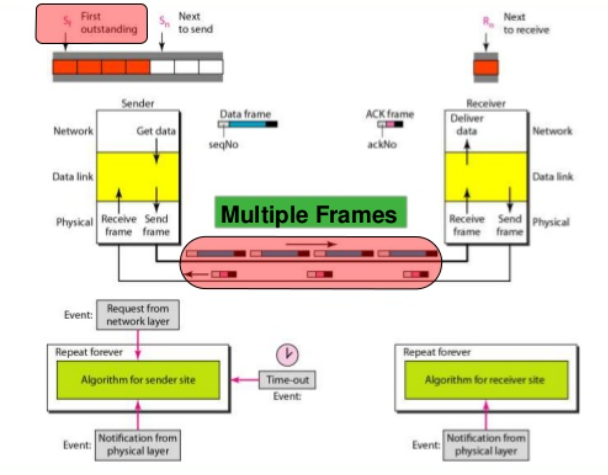
1. **Explain noisy channel protocols with neat diagrams.**

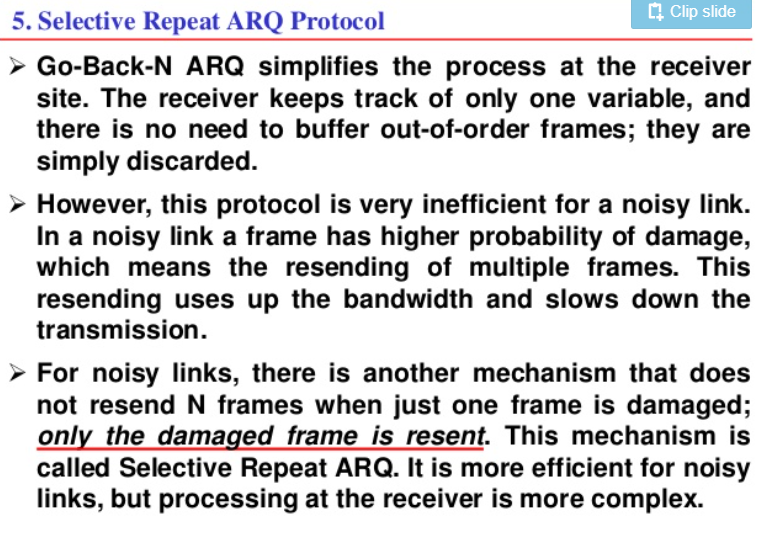


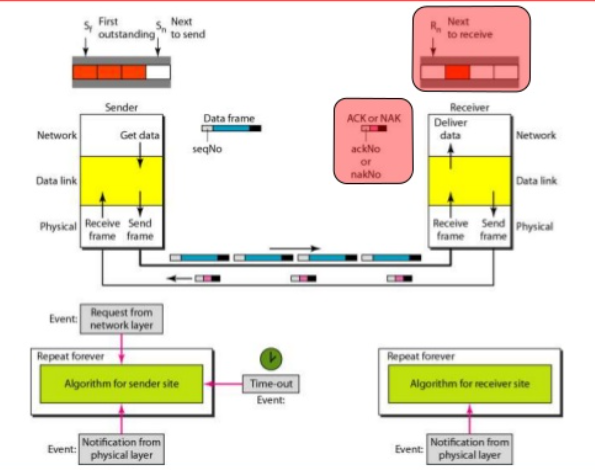












1. **Explain sliding window protocols.**

# **Sliding Window Protocol**

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in [TCP (Transmission Control Protocol)](https://www.javatpoint.com/tcp).

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

## **Types of Sliding Window Protocol**

Sliding window protocol has two types:

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

### **Go-Back-N ARQ**

Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.

### **Selective Repeat ARQ**

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