Q.1	Error Detection
Ans.	**Error Detection** Error detection is the process of detecting the error during the transmission between the sender and the receiver. Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted. Types of error detection • Parity checking • Cyclic Redundancy Check (CRC) • Checksum **Priority Check:** One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity. The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even.If the number of 1s is odd, to make it even a bit with value 1 is added.  **CRC:** CRC is a different approach to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.

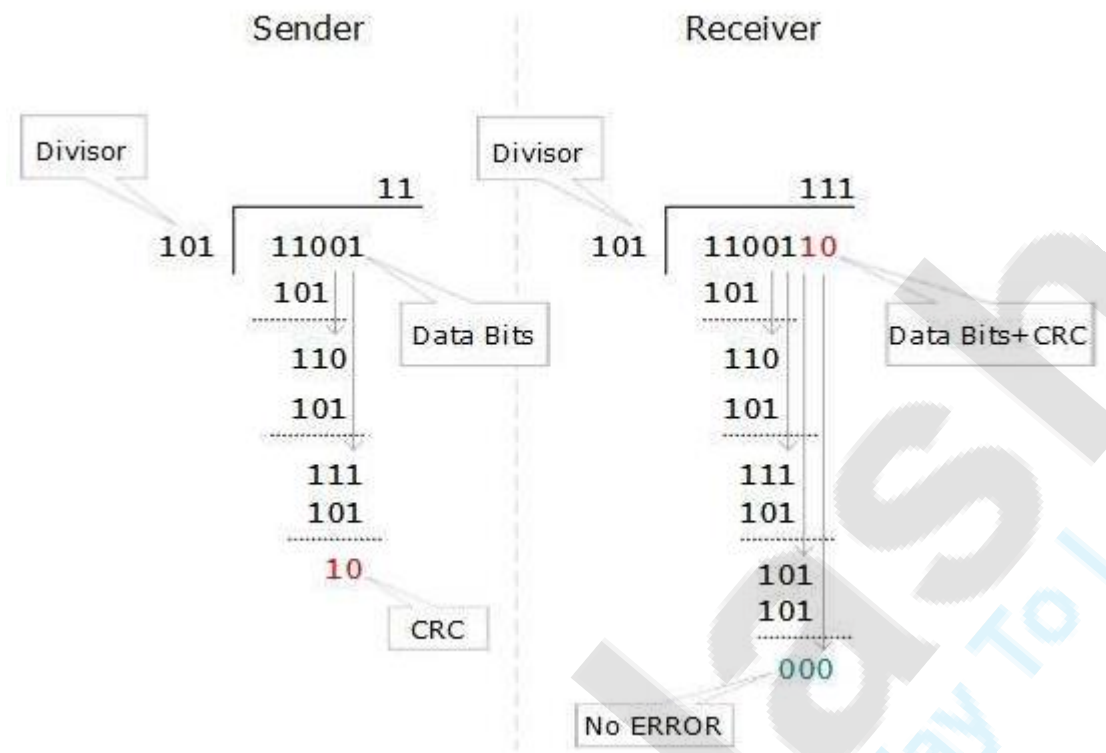
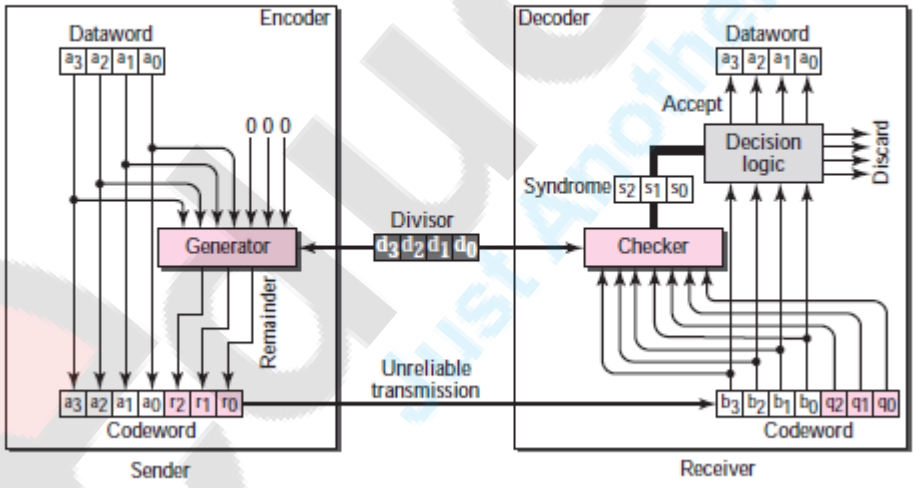


Figure C.6 *CRC encoder and decoder*

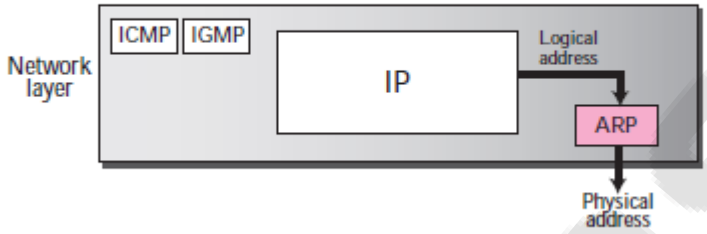


Checksum:
Check sum is the third method for error detection mechanism. Checksum is used in the upper layers, while Parity checking and CRC is used in the physical layer. Checksum is also on the concept of redundancy.

Q2.	ARP protocol
Ans.	**ARP:** Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an

address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a Media Access Control or MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

Figure 8.1 *Position of ARP in TCP/IP protocol suite*



Anytime a host, or a router, needs to find the physical address of another host or router on its network, it sends an ARP query packet. The packet includes the physical and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the physical address of the receiver, the query is broadcast over the network
(see Figure 8.2).
Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet. The response packet contains the recipient's IP and physical addresses. The packet is unicast directly to the inquirer using the physical address received in the query packet.
In Figure 8.2a, the system on the left (A) has a packet that needs to be delivered to another system (B) with IP address 141.23.56.23. System A needs to pass the packet to its data link layer for the actual delivery, but it does not know the physical address ofthe recipient. It uses the services of ARP by asking the ARP protocol to send a broadcast ARP request packet to ask for the physical address of a system with an IP address of 141.23.56.23.

Q.3	Point to point protocol
Ans.	**PPP:** PPP was devised by IETF (Internet Engineering Task Force) to create a data link protocol for point to point lines that can solve all the problems present in SLIP. • PPP is most commonly used data link protocol. It is used to connect the Home PC to the server of ISP via a modem. • This protocol offers several facilities that were not present in SLIP. Some of these facilities are: 1. PPP defines the format of the frame to be exchanged between the devices. 3.It defines how network layer data are encapsulated in data link frame.

4. PPP provides error detection.

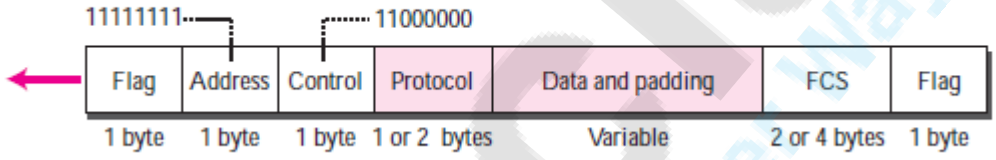
5. Unlike SLIP that supports only IP, PPP supports multiple protocols.

6. PPP allows the IP address to be assigned at the connection time i.e. dynamically. Thus a temporary IP address can be assigned to each host.

7. PPP provides multiple network layer services supporting a variety of network layer protocol. For this PPP uses a protocol called NCP (Network Control Protocol).

8. It also defines how two devices can authenticate each other.

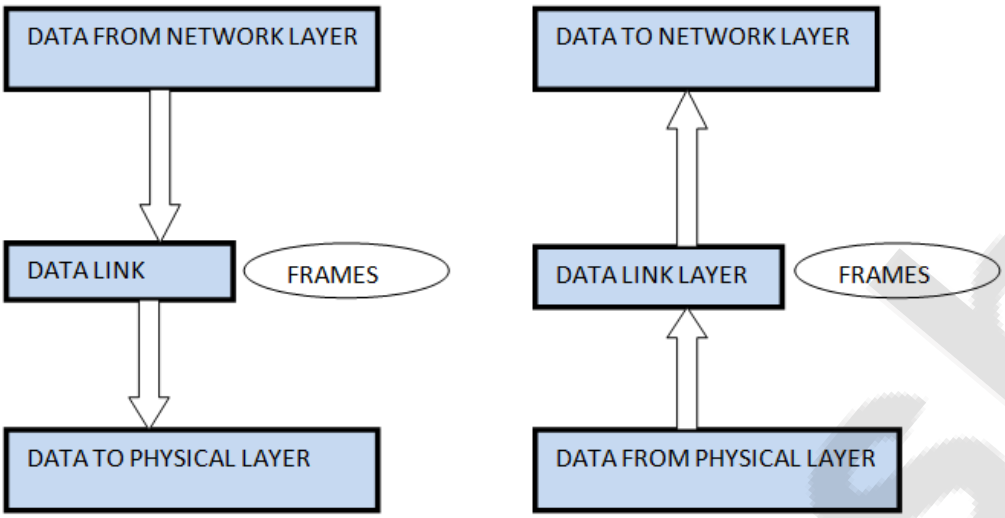
Figure 3.31 *PPP frame*



The descriptions of the fields are as follows:

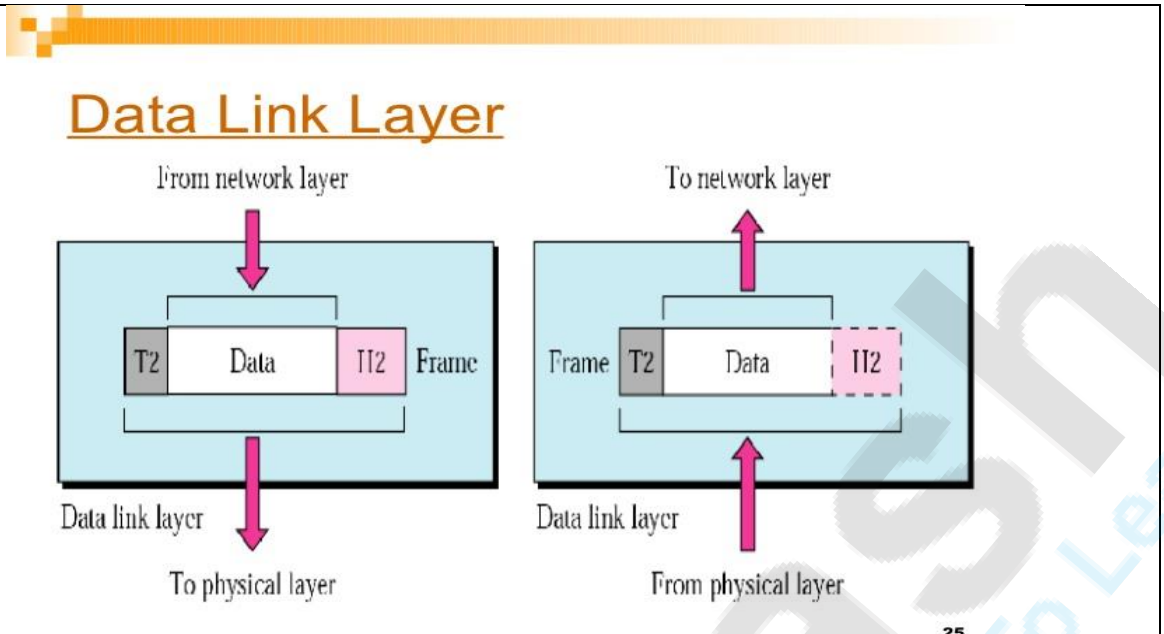
1. Flag field. The flag field identifies the boundaries of a PPP frame. Its value is 01111110.
2. Address field. Because PPP is used for a point-to-point connection, it uses the broadcast address used in most LANs, 11111111, to avoid a data link address in the protocol.
3. Control field. The control field is assigned the value 11000000 to show that, as in most LANs, the frame has no sequence number; each frame is independent.
4. Protocol field. The protocol field defines the type of data being carried in the data field: user data or other information.
5. Data field. This field carries either user data or other information.
6. FCS. The frame check sequence field is simply a 2-byte or 4-byte CRC used for error detection.

Q.4	Error Correction
Ans.	**Error Correction :**Send additional information so incorrect data can be corrected and accepted. Error correction is the additional ability to reconstruct the original, error-free data. There are two basic ways to design the channel code and protocol for an error correcting system : • Automatic Repeat-Request (ARQ) : The transmitter sends the data and also an error detection code, which the receiver uses to check for errors, and request retransmission of erroneous data. In many cases, the request is implicit; the receiver sends an acknowledgement (ACK) of correctly received data, and the transmitter re-sends anything not acknowledged within a reasonable period of time. • Forward Error Correction (FEC) : The transmitter encodes the data with an error-correcting code (ECC) and sends the coded message. The receiver never sends any messages back to the transmitter. The receiver decodes what it receives into the "most likely" data. The codes are designed so that it would take an "unreasonable" amount of noise to trick the receiver into misinterpreting the data.
Q.5	Data Link Layer
Ans.	Data link layer is most reliable node to node delivery of data. It forms frames from the packets that are received from network layer and gives it to physical layer. It also synchronizes the information which is to be transmitted over the data. Error controlling is easily done. The encoded data are then passed to physical. Error detection bits are used by the data link layer. It also corrects the errors. Outgoing messages are assembled into frames. Then the system waits for the acknowledgements to be received after the transmission. It is reliable to send message. **FUNCTIONS OF DATA LINK LAYER:** • Framing: Frames are the streams of bits received from the network layer into manageable data units. This division of stream of bits is done by Data Link Layer. • Physical Addressing: The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network. • Flow Control: A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side. • Error Control: Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames. • Access Control: Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.



The Data-Link layer contains two sublayers that are described in the IEEE-802 LAN standards:

Media Access Control (MAC)
Logical Link Control (LLC)
The Data-Link layer ensures that an initial connection has been set up, divides output data into data frames, and handles the acknowledgements from a receiver that the data arrived successfully. It also ensures that incoming data has been received successfully by analyzing bit patterns at special places in the frames.



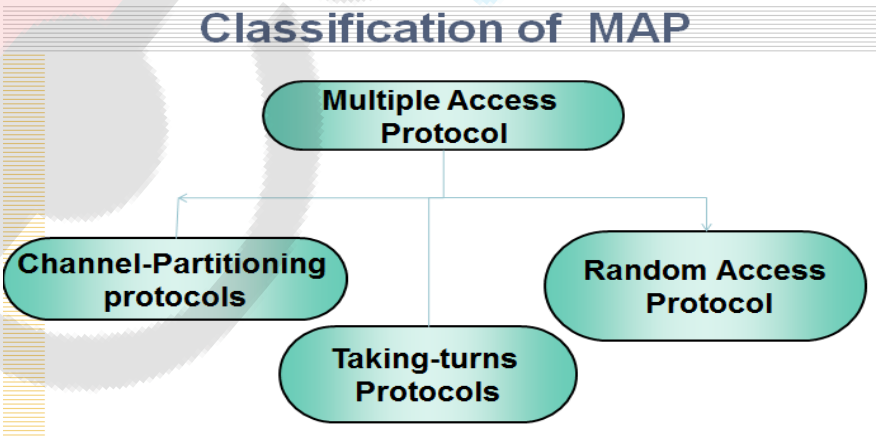
Q.6 Multiple Access Protocol

Q. Multiple access protocol is used to coordinate access to the link.
Nodes can regulate their transmission onto the shared broadcast channel by using Multiple access protocol.
It is used both wired and wireless local area network and satellite network.
All nodes are capable of transmitting frame, more than two nodes can transmit frames at the same time.
If so, the transmitted frames collide at all of the receivers.

When there is a collision, none of the receiving nodes can make any sense of any of the frames that were transmitted;

In a sense, the signals of the colliding frames become inextricably tangled together.

Thus, all frames involved in the collision are lost, and the broad cast channel as wasted during the collision interval.
To rectify this problem Multiple access protocol was implemented



	Channel Partitioning Protocols Techniques used to partition a broadcast channel's are, Time-division multiplexing Frequency-division multiplexing For example, if the channel send N nodes and that the transmission rate of the channel is R bps. TDM divides time into time frames and further divides each time frame into N time slots. Each slot time is then assigned to one of the N nodes. whenever a node has a packet to send, it transmits the packet's bits during its assigned time slot in the revolving TDM frame. **RANDOM ACCESS PROTOCOL** When node has packet to send Sense the channel. If it is busy, wait for **random** amount of time and then retry. no ***a prior*** coordination among nodes. All nodes use the same time, frequency and code. Two or more transmitting nodes ➜ "collision" Random access MAC protocol specifies how to recover from collisions -> Exponential backoff. Examples of random access MAC protocols: **CSMA, CSMA/CA, CSMA/CD** **Taking Turns MAC protocols:** (a) Polling: Master "invites" slaves Request/Clear overhead, latency, single point of failure (b) Token passing: token is passed from one node to the next Reduce latency, improve fault tolerance elaborate procedures to recover from lost token.
Q.7	Ethernet standards – IEEE 802.3, 802.5, FDDI, 802.6.
	802 Standards. IEEE 802.2, 802.3, 802.5, 802.11 The Institute of Electrical and Electronics Engineers is a standards setting body. Each of their standards is numbered and a subset of the number is the actual standard. The 802 family of standards is ones developed for computer networking. In this section, you will learn: - What the 802.2, 802.3, 802.5, 802.11 standards encompass; - Features, topology, and network cabling for each of these standards. First, let's discuss 802. IEEE, or Institute of Electrical and Electronics Engineers, is a standards setting body. They create standards for things like networking so products can be compatible with one another. You may have heard of IEEE 802.11b - this is the standard that IEEE has set (in this example, wireless-b networking). In this section, we will look at several networking technologies: 802.2, 802.3, 802.5, 802.11, and FDDI. Each of these is just a standard set of technologies, each with its own characteristics.

802.3 Ethernet

Now that we have an overview of the OSI model, we can continue on these topics. I hope you have a clearer picture of the network model and where things fit on it.

802.3 is the standard which Ethernet operates by. It is the standard for CSMA/CD (Carrier Sense Multiple Access with Collision Detection). This standard encompasses both the MAC and Physical Layer standards.

CSMA/CD is what Ethernet uses to control access to the network medium (network cable). If there is no data, any node may attempt to transmit, if the nodes detect a collision, both stop transmitting and wait a random amount of time before retransmitting the data.

The original 802.3 standard is 10 Mbps (Megabits per second). 802.3u defined the 100 Mbps (Fast Ethernet) standard, 802.3z/802.3ab defined 1000 Mbps Gigabit Ethernet, and 802.3ae define 10 Gigabit Ethernet.

Commonly, Ethernet networks transmit data in packets, or small bits of information. A packet can be a minimum size of 72 bytes or a maximum of 1518 bytes.

The most common topology for Ethernet is the star topology.

802.5 Token Ring

As we mentioned earlier when discussing the ring topology, Token Ring was developed primarily by IBM. Token ring is designed to use the ring topology and utilizes a token to control the transmission of data on the network.

The token is a special frame which is designed to travel from node to node around the ring. When it does not have any data attached to it, a node on the network can modify the frame, attach its data and transmit. Each node on the network checks the token as it passes to see if the data is intended for that node, if it is; it accepts the data and transmits a new token. If it is not intended for that node, it retransmits the token on to the next node.

The token ring network is designed in such a way that each node on the network is guaranteed access to the token at some point. This equalizes the data transfer on the network. This is different from an Ethernet network where each workstation has equal access to grab the available bandwidth, with the possible of a node using more bandwidth than other nodes.

Originally, token ring operated at a speed of about 4 Mbps and 16 Mbps. 802.5t allows for 100 Mbps speeds and 802.5v provides for 1 Gbps over fibber.

Token ring can be run over a star topology as well as the ring topology.

There are three major cable types for token ring: Unshielded twisted pair (UTP), Shielded twisted pair (STP), and fibber.

	Token ring utilizes a Multi-station Access Unit (MAU) as a central wiring hub. This is also sometimes called a MSAU when referring to token ring networks. **IEEE 802.6** is a standard governed by the ANSI for Metropolitan Area Networks (MAN). It is an improvement of an older standard (also created by ANSI) which used the Fiber distributed data interface (FDDI) network structure. The FDDI-based standard failed due to its expensive implementation and lack of compatibility with current LAN standards. The IEEE 802.6 standard uses the Distributed Queue Dual Bus (DQDB) network form. This form supports 150 Mbit/s transfer rates. It consists of two unconnected unidirectional buses. DQDB is rated for a maximum of 160 km before significant signal degradation over fiberoptic cable with an optical wavelength of 1310 nm. This standard has also failed, mostly for the same reasons that the FDDI standard failed. Most MANs now use Synchronous Optical Network (SONET) or Asynchronous Transfer Mode (ATM) network designs, with recent designs using native Ethernet or MPLS.