Parameter	Message switching	Circuit switching	Packet switching
Information type	Data in the form of Morse, Baudot, ASCII codes.	Analog voice or PCM digital voice	Binary information
Transmission system	Digital data over different transmission media	Analog and digital data over different transmission media	Digital data over different transmission media.
Addressing scheme	Geographical addresses	Hierarchical numbering plan	Hierarchical address space
Routing scheme	Manual	Route selected during call setup.	Each packet is routed independently.
Multiplexing scheme	Character or message multiplexing	Circuit multiplexing.	Packet multiplexing shared media access networks.

Review Questions

Q. 1 Explain the term circuit switching. How is it differen from the packet switching ?

Q. 2 Explain the three phases related to the communication via circuit switching.

Q. 3 Write a short note on Space-Division switches.

Q. 4 Explain the time-division switches.

Q. 5 Write a short note on Time-space-Time switches.

Q. 6 Explain the routing system in circuit switching networks.

Q. 7 State the three switching methods.

Q. 8 Name different types of switches used in circu switching.

Q. 9 How is space division switching better than tim division switching ?

Q. 10 Explain the concept of datagram packet switching.

Q. 11 State the advantages and drawbacks of datagran packet switching.

Q. 12 Explain the delays in datagram switching.

□□□

CHAPTER 8

Unit II

Data Link Layer

Syllabus :

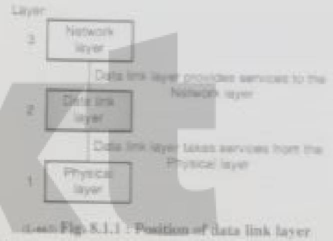
Introduction to data link layer, Nodes and links, Services, Two sub layers, Three types of addresses, Address Resolution Protocol (ARP), Error detection and correction, introduction, Types of errors, Redundancy, Detection versus correction.

8.1 Introduction :

- The physical layer deals with the transmission of signals over different transmission medias.
- A reliable and efficient communication between two adjacent machines can be achieved via the data link layer.
- This layer basically deals with frame formation, flow control, error control, addressing and link management.
- While sending data from source to destination errors may get introduced. The data communication circuits have only a finite data rate and there is non-zero propagation delay between the instant a bit is sent and the instant at which it is received.
- These limitations affect the efficiency of data transfer. The data link layer protocols used for communication take care of all these problems.
- Data link layer is the second layer in OSI reference model. It is above the physical layer.
- It is interesting to know that the TCP/IP suite does not define any protocol corresponding to data link layer and physical layer. These two layers are known as territories of network.
- These territorial networks can provide services to all the upper layers of TCP/IP suite. They can be either wired or wireless networks.
- We know that various types of networks are connected to each other for the Internet. For interconnecting different networks, the connecting devices such as routers or switches are used.
- The packet sent by a sender host has to travel through all these networks to reach the destination host.

8.1.1 Position of Data Link Layer :

- Fig. 8.1.1 shows the position of data link layer in the five layer Internet model. It is the second layer.

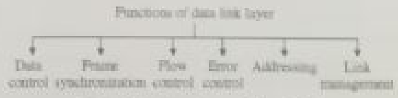

Layer
3
Network layer
Data link layer provides services to the Network layer
2
Data link layer
Data link layer takes services from the Physical layer
1
Physical layer

(L-660) Fig. 8.1.1 : Position of data link layer

- It receives services from the physical layer and provides services to the network layer.

8.2 Data Link Layer Design Issues (Functions of Data Link Layer) :

- The data link layer is supposed to carry out many specified functions.
- For effective data communication between two directly (physically) connected transmitting and receiving stations the data link layer has to carry out a number of specific functions as follows :



(L-664) Fig. 8.2.1 : Functions of data link layer

1. **Services provided to the network layer :**

   The data link layer provides a well defined service interface to the network layer. The principle service is transferring data from the network layer on sending machine to the network layer on destination machine. This transfer always takes place via the DLL.

2. **Frame synchronisation :**

   The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frames can be recognized by the destination machine.

3. **Flow control :**

   The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

4. **Error control :**

   The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

5. **Addressing :**

   When many machines are connected together (LAN), the identity of the individual machines must be specified while transmitting the data frames. This is known as addressing.

6. **Control and data on same link :**

   The data and control information is combined in a frame and transmitted from the source to destination machine. The destination machine must be able to separate out the control information from the data being transmitted.

7. **Link management :**

   The communication link between the source and destination is required to be initiated, maintained and finally terminated for effective exchange of data. It requires co-ordination and co-operation among all the involved stations. Protocols or procedures are required to be designed for the link management.

8.3 Nodes and Links :

- The type of communication taking place at the data link layer level is called as the **node to node communication.**
- A packet sent by a computer in the Internet will have to travel through different types of networks (LANs and WANs) before reaching the destination.
- All these LANs and WANs are connected to each other using routers.

Node :

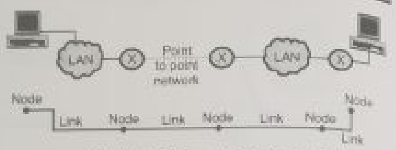
We can define a **node** as the two end hosts and the routers inbetween them.

Link :

The networks inbetween the two and hosts and the routers are called as **links.**

Source node and destination node :

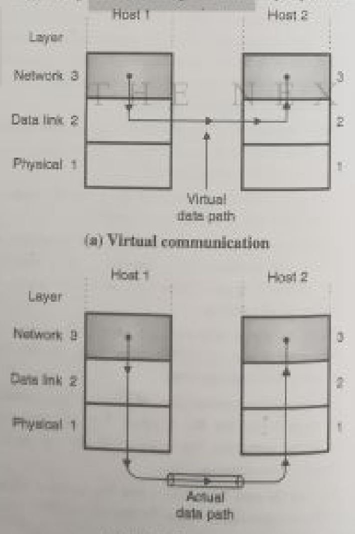
- The first node in the network is called as the source node while the last node is called as the destination node.
- Fig. 8.3.1, explains the concept of nodes and links.



(G-2873) Fig. 8.3.1 : Concept of nodes and links

8.4 Services Provided to Network Layer :

- Network layer is the layer above the data link layer in the OSI model. So it is supposed to provide services to the network layer.
- The main service to be provided is to transfer data from the network layer on the sending machine to the network layer of the receiving machine.
- The virtual path followed for such a communication is shown in Fig. 8.4.1(a). It is not the actual path.
- The actual path followed by the data from sending machine to destination is shown in Fig. 8.4.1(b) which is via all the layers below the network layer, then the physical medium, then layers 1, 2, 3 of receiving machine.
- However it is always easier to think that the communication is taking place through the data link layers (Fig. 8.4.1(a)) using a data link layer protocol.



(a) Virtual communication

(b) Actual data path

(G-667) **Fig. 8.4.1**

8.4.1 Types of Services Provided :

- Data link layer can be designed to offer different types of services. Some of them are as follows :
  1. Unacknowledged connectionless service.
  2. Acknowledged connectionless service.
  3. Acknowledged connection oriented service.

8.4.2 Unacknowledged Connectionless Service :

- In this type of service, the destination machine does not send back any acknowledgement after receiving frames.
- It is a connectionless service. So no connection is established before communication or released after it is over.
- If a frame is lost due to channel noise, then there are no attempts made to recover it.
- So this service is suitable only if the error rate is low. It is suitable for real time traffic such as speech. This type of service is highly unreliable.

8.4.3 Acknowledged Connectionless Service :

- This is the next step to improve reliability.
- In this service, there are no connections established for data transfer but for each frame received, the receiver sends an acknowledgement to the sender.
- If a frame is not received within some specified time it is assumed to be lost and the sender will retransmit it.
- This service is suitable for communication over unreliable channels such as wireless channels.

8.4.4 Acknowledged Connection Oriented Service :

- This is the most sophisticated one.
- The source and destination machines establish a connection before transferring the data.
- A specific number is given to each frame being sent and the data link layer guarantees that each transmitted frame is received.
- All the frames are guaranteed to be received in the same order as the order of transmission. Each received frame will be acknowledged individually by the destination machine.
- The data transfer takes place by following three distinct phases given below :
  1. Connection is established.
  2. The data frames are actually transmitted.
  3. The connection is released after completion of data transfer.

8.5 Two Sublayers :

8.5.1 Two Categories of Links :

- The medium which connects two nodes physically can be a cable or air. But the important point here is that the function of data link layer is to control how the medium is used.
- We can have a DLL which can utilise the capacity of the medium either fully or partially.
- A partially used medium is called as a **point to point link** whereas a fully used medium is called as the **broadcast link.**

8.5.2 Two Sublayers :

- We can divide the data link layer into two sublayers, in order to have a better understanding of its functionality and services provided by it.
- The two sublayers are as follows :
  1. Data link control sublayer (DLC)
  2. Media access control sublayer (MAC)
- The two sublayers are as shown in Fig. 8.5.1. The DLC sublayer is supposed to handle all the issues common to the point to point as well as broadcast links.
- However the MAC sublayer is supposed to handle the issues related only to broadcast links.

DLC sublayer
MAC sublayer
Data link layer

Fig. 8.5.1 : Two sublayers in data link layer

8.6 Three Types of Addresses :

- There are some data link layer protocols which define the following three types of addresses :
  1. Unicast address
  2. Multicast address
  3. Broadcast address

8.6.1 Unicast Address :

- The meaning of the word **unicast** is **one-to-one** communication. A unicast address is assigned to each host or each interface of a router.
- Therefore if a frame is having a unicast destination address, then it is destined to go to only one entity in the link.
- The example of a unicast address is the LAN address. Ethernet addresses are 48 bit in length (six bytes) which is written as 12 hexadecimal digits separated by colons.
- The example of a link layer unicast address of a computer is as shown in Fig. 8.6.1(a).

A4 36 43 12 94 E1

Fig. 8.6.1(a) : A unicast address

8.6.2 Multicast Address :

- There are some protocols, which define multicast addresses.
- The meaning of the word **multicasting** is **one-to-many** communication. However the communication is local i.e. inside the link.
- The multicast link layer addresses are very commonly used in LANs. Ethernet. They are 48 bit

(6 bytes) long and are written as 12 hexadecimal digits separated by colons as shown in Fig. 8.6.1(b).

- Note that in the multicast address, the second digit should be an even number in hexadecimal.

A2 : 36 : 47 : 15 : 92 : B1

Fig. 8.6.1(b) : Multicast address

8.6.3 Broadcast Address :

- There are some protocols, which define the broadcast addresses.
- The meaning of the word **broadcasting** is **one-to-all** communication.
- If a frame has a destination broadcast address, then it will be sent to all the entities connected in the link.
- The broadcast address are very commonly used in LANs, Ethernets. They are 48 bit (6 bytes) long with all the bits equal to 1.
- They are written as 12 hexadecimal digits separated by colons as shown in Fig. 8.6.1(c).

FF : FF : FF : FF : FF : FF

Fig. 8.6.1(c) : Broadcast address

8.7 ARP (Address Resolution Protocol) :

- An internet consists of various types of networks and the connecting devices like routers.
- A packet starts from the source host, passes through many physical networks and finally reaches the destination host.
- At the network level, the hosts and routers are recognised by their IP addresses.

IP address :

- An IP address is an internetwork address. It is a universally unique address.
- Every protocol involved in internetworking requires IP addresses.

MAC address :

- The packets from source to destination hosts pass through physical networks. At the physical level the IP address is not useful but the hosts and routers are addressed by their MAC addresses.
- A MAC address is a local address. It is unique locally but it is not unique universally.
- The IP and MAC address are two different identifiers and both of them are needed, because a physical network can have two different protocols operating at the network layer at the same time.
- Similarly a packet may travel through different physical networks.
- So to deliver a packet to a host or a router, we require addressing to take place at two levels namely IP addressing and MAC addressing.
- Most importantly we should be able to map the IP address into a corresponding MAC address.

8.7.1 Mapping of IP Address into a MAC Address :

- We have seen the need of mapping an IP address into a MAC address.
- Such a mapping can be of two types :
  1. Static mapping and 2. Dynamic mapping.

1. **Static mapping :**
   - In static mapping a table is created and stored in each machine. This table associates an IP address with a MAC address.
   - If a machine knows the IP address of another machine then it can search for the corresponding MAC address in its table.
   - The limitation of static mapping is that the MAC addresses can change. These changed MAC addresses must be updated periodically in the static mapping table.
2. **Dynamic mapping :**
   - In dynamic mapping technique a protocol is used for finding the other address when one type of address is known.
   - There are two protocols used for carrying out the dynamic mapping. They are :
     1. Address Resolution Protocol (ARP).
     2. Reverse Address Resolution Protocol (RARP)
   - The ARP is used for mapping an IP address to a MAC address whereas the RARP is used for mapping a MAC address to an IP address.

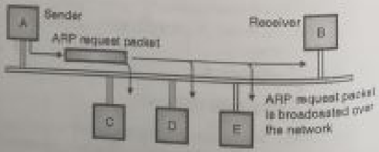
8.7.2 ARP Operation :

ARP is used for mapping an IP address to its MAC address. For a LAN, each device has its own physical or station address as its identification. This address is stored on the NIC (Network Interface Card) of that machine.

How to find the MAC address ?

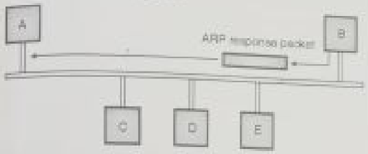
When a router or a host (A) needs to find the MAC address of another host (B) the sequence of events taking place is as follows :

1. The router or host A who wants to find the MAC address of some other router, sends an ARP request packet. This packet consists of IP and MAC addresses of the sender A and the IP address of the receiver (B).
2. This request packet is broadcasted over the network as shown in Fig. 8.7.1(a).



(G-878)Fig. 8.7.1(a) : ARP request is broadcast

3. Every host and router on the network will receive the ARP request packet and process it. But only the intended receiver (B) will recognize its IP address in the request packet and will send an ARP response packet back to A.
4. The ARP response packet has the IP and physical addresses of the receiver (B) in it. This packet is delivered only to A (unicast) using A's physical address in the ARP request packet. This is shown in Fig. 8.7.1(b). Thus host A has obtained the MAC address of B using ARP.



(G-876) Fig. 8.7.1(b) : ARP response unicast

8.7.3 ARP Packet Format :

The ARP message format is as shown in Fig. 8.7.2. The various fields in it are as follows :

1. **HTYPE (Hardware Type) :** This 16 bit field defines the type of network on which ARP is being run. ARP is capable of running on any physical network.
2. **PTYPE (Protocol Type) :** This 16 bit field is used to define the protocol using ARP. Note that we can use ARP with any higher-level protocol such as IPv4.
3. **HLEN (Hardware length) :** It is an 8 bit field which is used for defining the length of the physical address in bytes. For example, this value is 6 for Ethernet.

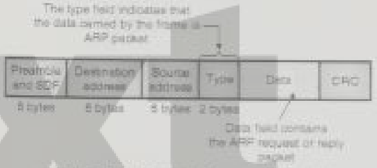
<table>
<tr><td colspan="2">Hardware Type (16 bits)</td><td>Protocol type (16 bits)</td></tr>
<tr><td>Hardware length</td><td>Protocol length</td><td>Operation request 1, Reply 2</td></tr>
<tr><td colspan="3">Sender hardware address</td></tr>
<tr><td colspan="3">Sender protocol address</td></tr>
<tr><td colspan="3">Target hardware address</td></tr>
<tr><td colspan="3">Target protocol address</td></tr>
</table>

Fig. 8.7.2 : ARP message format

4. **PLEN (Protocol Length) :** This field is 8 bit long and it defines the length of the IP address in bytes. For IPv4 this value is 4.
5. **OPER (Operation) :** It is a 16 bit field which defines the type of packet. The two possible types of packets are : ARP request (1) and ARP reply (2).
6. **SHA (Sender Hardware Address) :** This field is used for defining the physical address of the sender. The length of this field is variable.
7. **SPA (Sender Protocol Address) :** This field defines the logical address of the sender. The length of this field is variable.
8. **THA (Target Hardware Address) :** It defines the physical address of the target. It is a variable length field. This field contains all zeros for the ARP request packet, because the receivers physical address is not known to the sender.
9. **TPA (Target Protocol Address) :** This field defines the logical address of the target. It is a variable length field.

8.7.4 Encapsulation :

- An ARP packet (request or reply) is inserted directly into the data link frame. Such an insertion is known as encapsulation.
- Fig. 8.7.3 shows an example of encapsulation in which an ARP packet being encapsulated in an Ethernet frame. The type field shows that the data carried by the frame is an ARP request or reply packet.


The type field indicates that the data carried by the frame is ARP packet
Preamble and SDF
Destination address
Source address
Type
Data
CRC
8 bytes
6 bytes
6 bytes
2 bytes
Data field contains the ARP request or reply packet

(G-879)Fig. 8.7.3 : Encapsulation of ARP packet

8.7.5 Operation of ARP on Internet :

The services of ARP can be used under the following working conditions when it is being operated on internet :

1. The sender is a host and wants to communicate with another host which is on the same network.
2. The sender is a host and wants to communicate with a host on another network.
3. The sender is a router. It has received a datagram with a destination address of a host on another network.
4. The sender is a router. It has received a datagram which is meant for a host in the same network.

- Now let us see how ARP works on the internet.

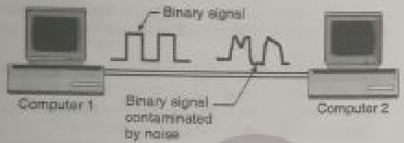
Operation :

1. The sender (host or router) knows the IP address of the target.
2. IP orders ARP to create an ARP request message. The request packet consists of senders physical and IP addresses plus the IP address of the target but the physical address of the target is not known.
3. This ARP request packet is sent to the data link layer. Here the ARP request packet is inserted in a frame.
4. Every router or host receives this frame because it is broadcast. All the machines except the target drop this packet as discussed earlier.
5. The target machine sends back a reply packet which contains the target's physical address. This reply is unicast and addressed only to the sender.
6. The sender receives the reply packet. Hence the physical address of the target has been obtained.

7. The IP datagram carrying data for the target machine is inserted in a frame and the frame is unicast to the target machine.

8.8 Introduction to Error Control Coding :

- When transmission of digital signals takes place between two systems such as computers as shown in Fig. 8.8.1, the signal get contaminated due to the addition of "Noise" to it.



(L-302)Fig. 8.8.1 : Noise contaminates the binary signal

- The noise can introduce an error in the binary bits travelling from one system to the other. That means a 0 may change to 1 or a 1 may change to 0.
- These error can become a serious threat to the accuracy of the digital system. Therefore it is necessary to detect and correct the errors.

8.8.1 Need of Error Control Coding :

- In data communication, errors are introduced during the transmission of data from the transmitter to receiver due to noise or some other reasons.
- The reliability of data transmission will be severely affected due to these errors.
- In order to improve the reliability of data transmission, the designer will have to increase the signal power or reduce the noise spectral density N_o so as to maximize the ratio E_b / N_o.
- But practically there is a limitation on the maximum value of the ratio E_b / N_o. We cannot increase the ratio beyond this limit. **Hence for a fixed value of E_b / N_o, we have to use some kind of "coding" in order to improve the quality of the transmitted signal.**
- Another advantage of using coding is that we can reduce the required value of E_b /N_o if the error rate is predecided and remains fixed at that value. This will inturn reduce the required transmitted power and the size of antenna.

How to detect and correct errors ?

- For the detection, and / or correction of these errors, one or more than one extra bits are added to the data bits at the time transmitting.
- These extra bits are called as parity bits. They allow the detection or sometimes correction of the errors.
- The data bits alongwith the parity bits form a code word.

Error control techniques :

- The error control techniques can be divided into two types :
  1. Error detection techniques.
  2. Error correction techniques.
- The error detecting techniques are capable of only detecting the errors. They cannot correct the errors.
- The error correcting techniques are capable of detecting as well as correcting the errors.

8.8.2 Types of Errors :

The errors introduced in the data bits during their transmission can be categorised as :

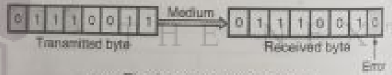
1. Content errors 2. Flow integrity errors.

- The content errors are nothing but errors in the contents of a message e.g. a "0" may be received as "1" or vice versa. Such errors are introduced due to noise added into the data signal during its transmission.
- Flow integrity errors means missing blocks of data. It is possible that a data block may be lost in the network possibly because it has been delivered to a wrong destination.
- Depending on the number of bits in error we can classify the errors into two types as :

1. Single bit error 2. Burst errors.

1. Single bit error :

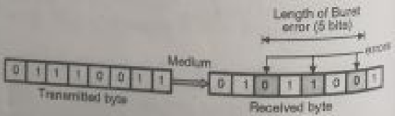
- The term single bit error suggests that only one bit in the given data unit such as byte is in error.
- That means only one bit in a transmitted byte will change from 1 to 0 or 0 to 1, as shown in Fig. 8.8.2.



(G-188) Fig. 8.8.2 : Single bit error

2. Burst errors :

- If two or more bits from a data unit such as a byte change from 1 to 0 or from 0 to 1 then burst errors are said to have occurred.
- Refer Fig. 8.8.3 in which the shaded bits in the received byte have been the erroneous bits. These are 3 bits but the length of the burst is shown to be of 5 bits.



(G-189) Fig. 8.8.3 : Burst errors

- The length of the burst error extends from the first erroneous bit to the last erroneous bit. Even though some of the bits in between have not been corrupted. The length of the burst error is shown to be 5 bits.
- Burst errors are illustrated in Fig. 8.8.3.

Disadvantages of coding :

Some of the disadvantages of the coding technique are :

1. An increased transmission bandwidth is required in order to transmit the encoded signal. This is due to the additional bits (redundancy) added by the encoder.
2. Use of coding make the system complex.

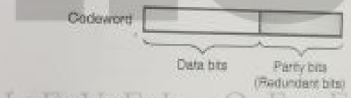
8.8.3 Disadvantages of Coding :

Some of the disadvantages of the coding technique are :

1. An increased transmission bandwidth is required in order to transmit the encoded signal. This is due to the additional bits (redundancy) added by the encoder.
2. Use of coding make the system complex.

8.8.4 Redundancy :

- Redundancy involves transmission of extra bits alongwith the data bits. These extra bits actually do not contain any data or information but they ensure the detection and correction of errors introduced during the data travel from sender to receiver.
- As these extra bits do not contain any information, they are known as redundant bits.
- The redundant bits are also known as **parity check** bits. They are produced from the data bits using some predecided rules.
- The data bits and redundant bits together form a code word as shown in Fig. 8.8.4.



(L-303)Fig. 8.8.4 : Structure of a transmitted code word

8.9 Detection Versus Correction :

- Detection and correction of errors are the two most important aspects of error control in data communication.
- The correction of errors is more difficult as compared to their detection. The process of error detection is much easier because we have to simply find if error is present or absent in the received code word.
- In **error detection** we are not interested even in the number of errors. The only question to be answered is whether an error has occurred or not.
- In **error correction,** multiple processes are involved such as detecting the errors, knowing their number, the location of errors and then correcting the erroneous bits.

Review Questions

Q. 1 State the various design issues for the data link layer.

Q. 2 State and explain the various services provided to the Network layer.

Q. 3 Define node and link.

Q. 4 Define node to node communication.

Q. 5 State three types of addresses.

Q. 6 Explain unicast and multicast addresess.

Q. 7 State the name of sublayers in data link layer.

Q. 8 Explain burst errors.

Q. 9 Explain the need, advantages and disadvantages of coding.

Q. 10 Explain the purpose of ARP.

Q. 11 Why is ARP request broadcast but ARP reply unicast ?

❑❑❑