2 OSI Model

2.1. Introduction

In early days, the problem of getting a computer of one brand to accept data created by another manufacturer's machine has confronted users of these devices. At that time, only practical way to get around this barrier was to retype the data from the computer into the second. But this is a very time consuming process and has the chances of lot of errors.

As the computers proliferated, interfaces or adapters were invented that translated one machine's code into a form that others could understand, allowing a variety of computers to be hooked together in networks. But these interfaces ware expensive. Because a substantial number of them were needed to establish a large network. Moreover, each type of computer needed an interface of its own. Thus, there was little oportunity to spread the cost of developing the given interfaces by selling many copies of it.

About in 1977, the Geneva-based International Organization for Standardization set forth the *Open Systems Interconnection* (OSI) model. A master plan for computer-to-computer dialogue, the OSI model divides the communications process into seven layers. The model sets standards that permit a wide variety in the design of computer hardware and software. The model demands only that communication tasks remain in their assigned layers and that the output of each layer precisely matches the format established for it.

2.2. Standards

Standards are documents containing agreements reached by standards bodies responsible for that particular area of telecommunications. They are the result of study, discussion, and analysis. Standards may be endorsed at different levels—company, national, regional, and international—as appropriate.

The standards process works through agreement among relevant experts from across a spectrum of private and public sectors. These experts debate, contribute views, and investigate, often with a multitired political backdrop, to arrive at an agreed-upon specification. The process of getting a consensus from different experts after working through the technical issues almost always leads to a better specification in comparison to one developed by single vendor or govermment department. A consensus-based specification takes longer to produce than a single-party specification approach because

of the time-consuming nature of multiparty discussions. Although the process might be somewhat slower, it leads to a superior specificaton that will be supported by a wide base of manufactures—bringing with it interoperability.

The fact that Internet, wireless, and fixed-line standards are all being addressed by the SS7/C7 standards bodies is a sign of the central role that SS7/C7 plays in the convergence of today's voice and data networks. Until the early 1990s, largely separate worlds existed for telecommunications standards and for Internet standards. These two worlds are now intersecting, creating the need for additional standards to address new architectures, protocols and features.

Test specifications are used to facilitate the standards process by helping validate that equipment conforms to the documented standard(s). Testing is normally performed by an independent organization. Quite often this happens to be a department of an incumbent or private company that has been spun off.

2.3. Network Architectures

Network architectures deal with the physical connection, *i.e.* topologies, access methods and connection protocols. Some examples of network architectures are :

(a) Ethernet
(b) Token ring
(c) Apple Talk
(d) ARCNET
(e) ATM etc.

2.4. Protocol

By the term protocol, we mean the set of rules or standards designed to enable computers to be connected with one another and to exchange information among them with very little error. Protocol can describe low-level details of machine-to-machine interfaces (e.g. the order in which bits and bytes are sent across a wire) or high-level exchange between allocation programs (e.g. the way in which two programs transfer a file across the internet).

The following example makes the idea clear. Suppose ther are two people, one speaks Hindi and the other French. Since they have no common language, they each engage a translator whose common language in English. Thus, the person in Location A knows Hindi and wants to send a message "Mai samosa pasand karta hoon" ("I like samosa"). The translators use a common language say English. So the same is translated in English. He hands over the translated version to the secretary for faxing it to the other side. The secretary sends the message on Fax and the same is received in location B as a Fax message. The translator in this location B reads the English translated message and converts it into French language so that the Person in Location B can understant the message. In the above example, each protocol is totally independent of the other one, as

long as the interfaces are not changed. The translators can switch from English to Dutch or for that matter to any other language say Russian but both must agree for this. Similarly, the secretaries can send the message by e-mail instead of FAX. This is the basic philosophy of using multilayer protocol.

The protocol generally accepted for standardizing overall computer communications is a seven-layer set of hardware and software guidelines known as the OSI (Open System Inter-connection) model. Thus, the work protocol is used in reference to a multitude of standards affecting different aspects of communication. Some, such as the RS-232-C standard, affect hardware connections. Other standards govern data transmission. Among these are the parameters and handshaking signals used in modem communications. Other protocols, such as the widely used XMODEM, govern file transfer and yet others such as CSMA/CD, define the methods by which messages are passed around the stations on a LAN. Thus, taken as a whole, these various protocols represent attempts to ease the complex process of enabling computers of different makes to communicate with each other.

2.5. Layering the Communication Process

Protocols set standards that permit a wide variety in the design of computer hardware and software. Most of today's popular protocols are designed in a layered fashion. Layered approach divides communication tasks into layers. One should think of each layer as being logically connected to the same layer on a different computer on the network The connection established between these two layers is only logical; the physical communication occurs when packets of data are sent over a physical cable or wireless media.

The lower layers define the network's physical media and related tasks, such as putting data bits onto the network adapter cards and cable. The higher layers define how applications access communication services. The higher the layers, the more complex its task is. Each layer provides some service to action that prepares the data for delivery over the network to another computer. The layers are separated form each other by boundaries called interfaces. All requests are passed from one layer, through the interface to the next layer. Each layer builds upon the standards and activities of the layer below it. At each layer there is software that implements certain network functions according to a set of protocols.

At the sender's computer, before data is passed from one layer to another is broken into packets. Where a packet is a unit of information transmitted as a whole from one device to another on a network.

Each layer adds some header information to the data packet. This information includes additional formatting or addressing to the packet which it needs, to be successfully transmitted across the network.

This data packet is then put on the physical wire of the transmitting computer. The data packet (along with the header information added by the layers) travels along the wire. When the packet reaches the receiving computer, it passes up the layers, there. Each layer, in the process, reads the header information sent by its peer layer in the sending computer. This header is stripped off before the packet is passed to the upper layer. Finally, the packet reaches the particular application software which can process the data.

2.5.1. Need for Layered Solutions

Layered approach provides the following advantages :

(a) Each layer needs to know and worry only about the functions in its domain. Functioning of other layers are hidden from it. For example, a layer called presentation layer need not worry about how the data will be fragmented and routed along the network. These are the functions of another layer, namely the network layer.

(b) Each layer performs a functions independent of the other layers. This enables software developers to develop a software component for a particular layer. The software component so developed should conform to the standard to be followed at that particular layer. By following the standards, the component will be able to communicate and work with software components in other layers. This can be done no matter which vendor has manufactured which component. Thus, layered approach helps in standardizing the whole process, in a simple manner.

(c) A layer can be modified, if needed, without affecting other layers.

(d) Software packages conforming to the standards of a particular layer are able to use the softwares at other layers to communicate with each other. Thus, programmers at Application layer only need to concentrate on the main logic of the software and not on details such as how messages shall be broken down, to which router they should be sent to, what LAN technology the receiver is using, etc.

2.6. OSI Reference Model

Open System Interconnection (OSI) model, an ISO standard for worldwide communication Networks that defines a networking framework for implementing protocols in seven layers. Open Systems Interconnection (OSI) model is developed by ISO (International organization for standardization) in 1984. ISO is the organization dedicated to defining global communication and standards.

This model is called Open System Interconnection (OSI) because this model allows any two different systems to communicate regardless of their underlying architecture. Therefore OSI reference model allows open communication between different systems without requiring changes' to the logic of the underying hardware and software.

The International standard organization (ISO), in an effort to encourage open networks, developed an open systems interconnect reference model. The model logically groups the functions and sets rules, called protocols, necessary to establish and conduct communication between two or more parties. The model consists of seven functions, often referred to as layers.

OSI reference model is a logical framework for standards for the network communication. OSI reference model is now considered as a primary standard for internetworking and inter computing. Today many network communication protocols are based on the standards of OSI model. In the OSI model the network/data communication is defined into seven layers. The seven layers can be grouped into three groups-Network, Transport and Application.

2.7. Basics of OSI Model

The ISO (International Standards Organization) has created a layered model called the OSI (Open Systems Interconnect) model to describe defined layers in a network operating system. The purpose of the layers is to provide clearly defined functions to improve internet work connectivity between "computer" manufacturing companies. Each layer has a standard defined input and a standard defined output.

Understanding the function of each layer is instrumental in understanding data communication within networks whether Local, Metropolitan or Wide.

This is a top-down explanation of the OSI Model, starting with the user's PC and what happens to the user's file as it passes through the different OSI Model layers. The top-down approach was selected specifically (as opposed to starting at the Physical Layer and working up to the Application Layer) for ease of understanding of how the user's files are transformed through the layers into a bit stream for transmission on the network.

There are 7 Layers of the OSI model and they are always presented in this manner starting with layer 7 :

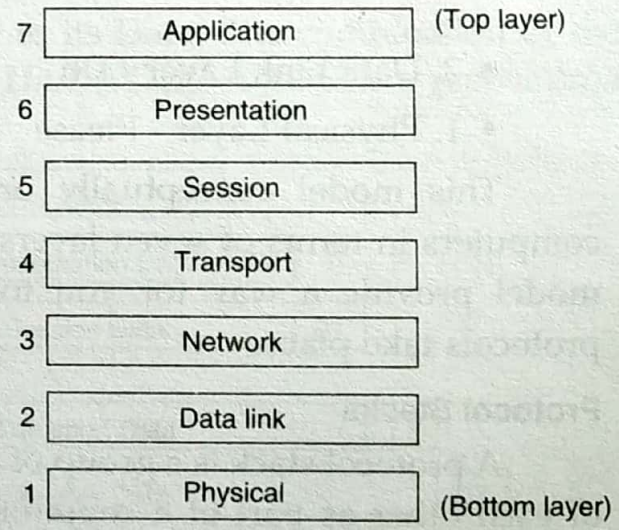


Fig. 2.1. The OSI model

There are a few ways of remembering the OSI layers, one is the phrase "Please Do Not Take Salami Pizza Away".

- 7. Application Layer - Away
- 6. Presentation Layer - Pizza
- 5. Session Layer - Salami
- 4. Transport Layer - Take
- 3. Network Layer - Not

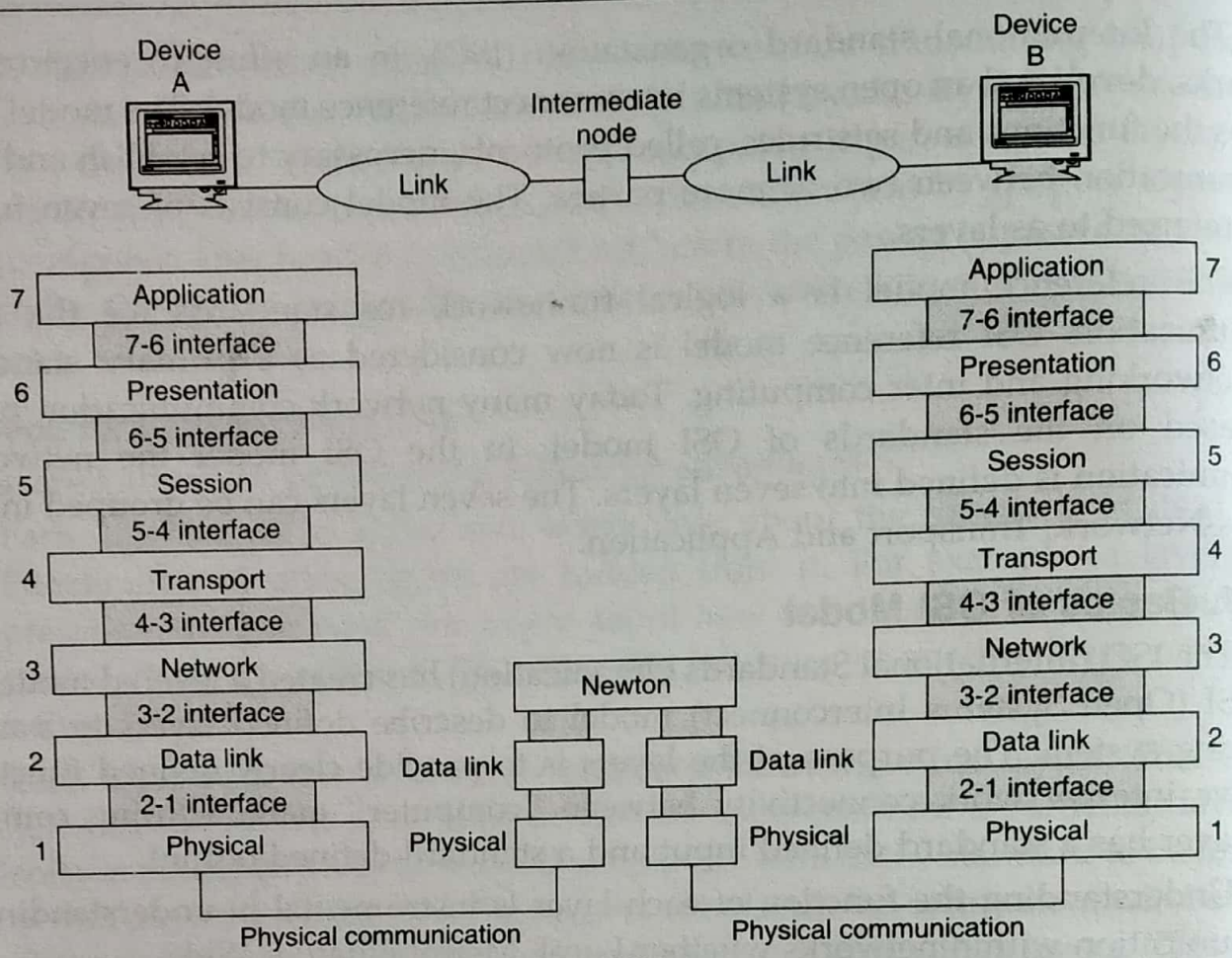


Fig. 2.2. OSI layers

- 2. Data Link Layer - Do
- 1. Physical Layer - Please

This model conceptually organizes the process of communications between computers in terms of seven layers called Protocol Stacks. The seven layers of the OSI model provide a way for you to understand how communications across various protocols take place.

Protocol Stacks

A protocol stack is a group of rules or procedures called protocols arranged on top of each other as part of a communication process. Every layer of the OSI model has different protocols associated with it.

When more than one protocol is needed to complete a communication process, the protocols are grouped together in a stack. A popular protocol stack is TCP/IP, which is widely used for UNIX and the Internet. Each layer in the protocol stack receives services from the layer below it and provides services to the layer above it. That means, layer N uses the services of the layer below it (layer N – 1) and provides services to the layer above it (layer N + 1). For two computers to communicate, the same protocol stacks must be running on each computer.

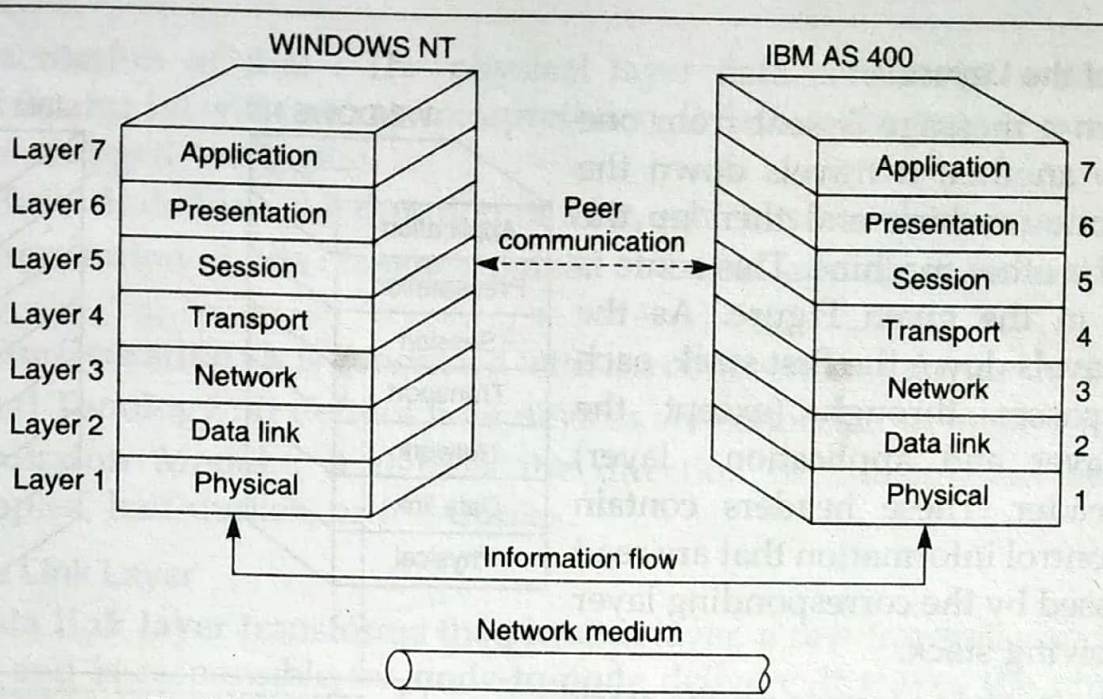
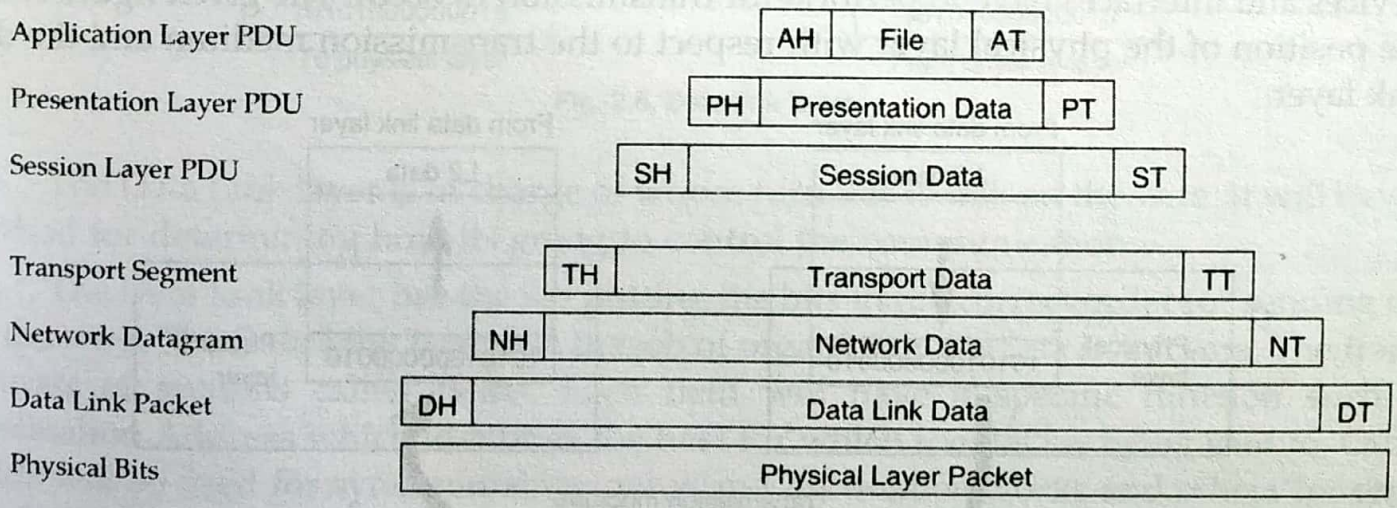


Fig. 2.3. Peer to peer communication between two computers

The computers can have different operating systems and still be able to communicate if they are running the same protocol stacks. For instance , a WINDOWS NT machine running TCP/IP protocol stack can communicate with an IBM AS400 machine running TCP/IP.

2.8. Layer Specific Communication

Each layer may add a Header and a Trailer to its Data. The combination of the header, data and trailer is called a ***Protocol Data Unit*** (PDU). A PDU is a *generic term* that is applied to a layer's data structure.



The header is information that precedes the data and the trailer is information that follows the data. Usually the header will contain source and destination addresses and some control information used to manage the communication. The trailer usually contains information such as error checking or a field to indicate the end of the PDU. The Application Header is indicated by the letters AH. The Application Trailer is indicated by the letters AT in the above figure.

Functions of the Layers

When a message is sent from one machine to another, it travels down the layers on one machine and then up the layers on the other machine. This route is illustrated in the given Figure. As the message travels down the first stack, each layer it passes through (except the physical layer and application layer) adds a header. These headers contain pieces of control information that are read and processed by the corresponding layer on the receiving stack.

As the message travels up the stack of the other machine, each layer strips the header added by its peer layer.

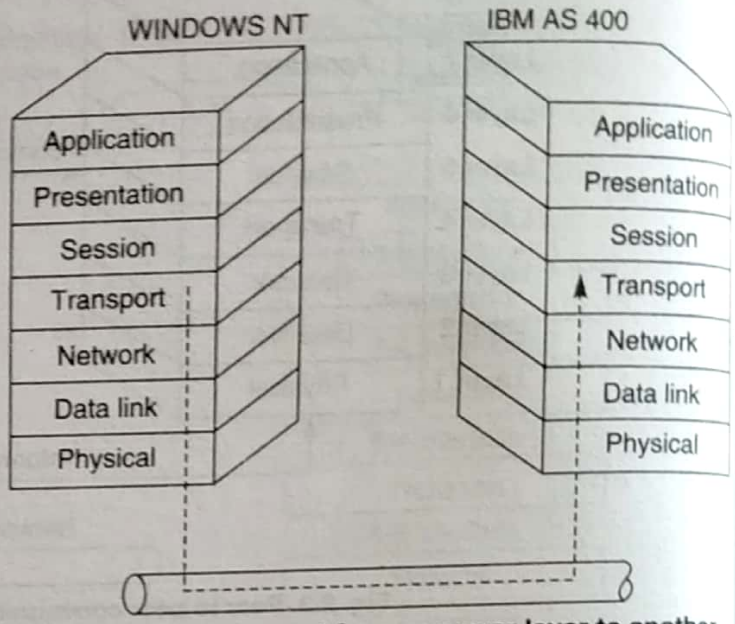


Fig. 2.4. A message sent from one peer layer to another peer layer

Let us now discuss the functions of each layer in the OSI model.

Layer 1- Physical Layer

The physical layer concerns itself with the transmission of bits and the network card's header interface to the network.

It coordinates the functions required to transmit a bit stream over a physical medium. It deals with both the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur. The given figure shows the position of the physical layer with respect to the transmission medium and the data link layer.

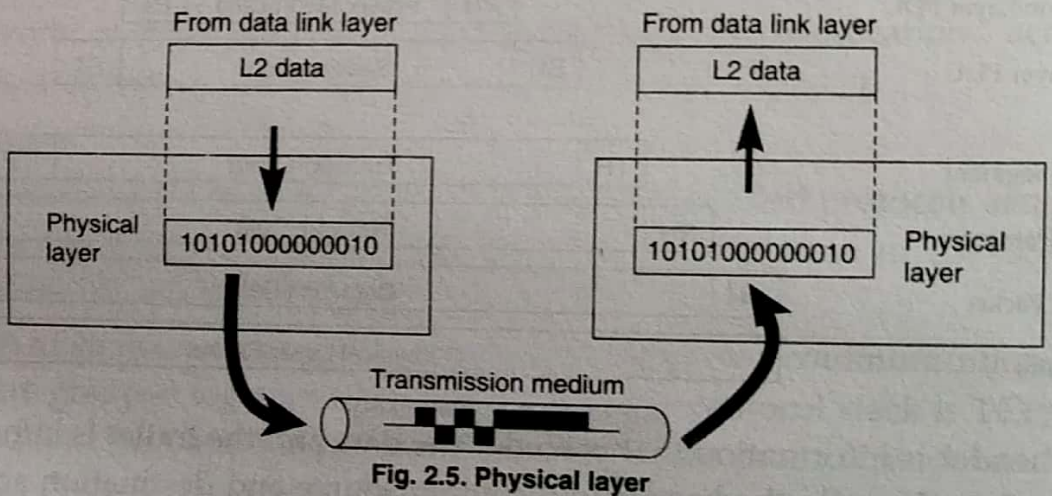


Fig. 2.5. Physical layer

The physical layer is concerned with the following responsibilities :

Physical characteristics of interfaces and media : It defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

Representation of Bits : The physical layer data consists of a stream of *bits* (sequence of 0s and 1s) without any interpretation. It defines the type of **encoding** (how 0s and 1s are changed to signals).

Data Rate : It defines the duration of a bit, which is how long it lasts.

Synchronization of bits : It synchronized at the bit level of sender and the receiver clocks.

Line Configuration : It is concerned with the connection of devices to the medium.

Physical Topology : It defines how devices are connected to make a network.

Transmission Model : It defines the direction of transmission between two devices; simplex, half-duplex, or full-duplex.

Layer 2- Data Link Layer

The **data link layer** transforms the physical layer, a raw transmission facility, to a reliable link and is responsible for **node-to-node** delivery. It makes the physical layer appear error free to the upper layer (network layer). The given figure shows the relationship of the data link layer to the network and physical layers.

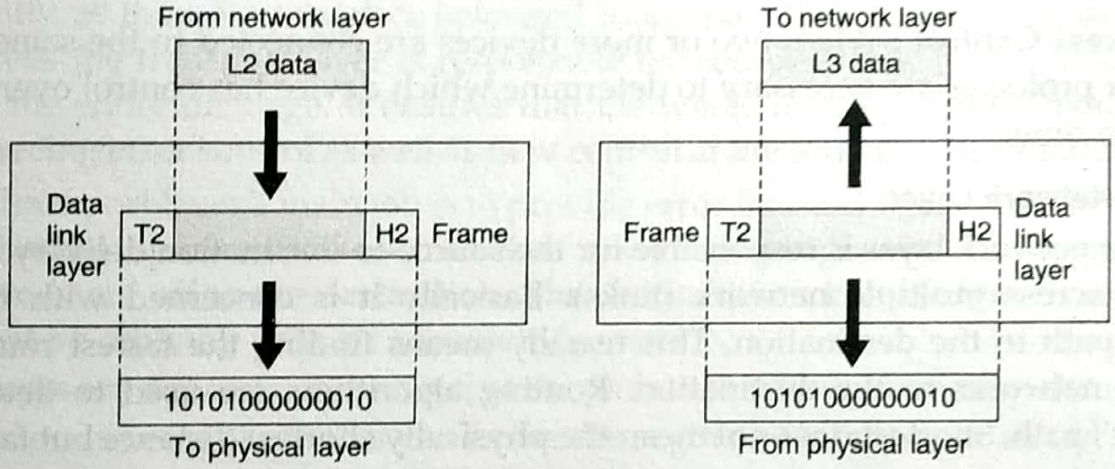


Fig. 2.6. Data link layer

The Data Link layer is in charge of whose turn it is to talk on the wire. It will have a method for determining how its going to control the communication.

The Data Link layer has the job putting the bits in the correct order for sending out on the wire. The Data Link layer has the job of organizing the data in a frame. The frame consists of sections called fields. Each field will have a specific function such as Destination Address which identifies the host for which the data is being sent to. Other fields will be used for synchronizing source and destination clocks and others for error checking.

The Data Link layer resides in the firmware layer of the network interface card. Firmware is software that is burnt into a read only memory. The node will have a unique address that identifies it from all other nodes. This address is called a hardware address because it is burnt into the firmware. Ethernet network interface cards' unique address is typically called a MAC address after a Data Link sub-layer called the Media Access Control (MAC) layer.

The Data Link layer takes the packets and puts them into frames of bits : 1s and 0s for transmission and assembles received frames into packets. The Data Link layer works at the bit level and is concerned about bit sequence. Error checking is at the bit level and frames with errors are discarded and a request for re-transmission is sent out.

Specific responsibilities of the data link layer include the following :

Framing : It divides the stream of bits received from the network layer into manageable data units called **frames.**

Physical Addressing : If frames are to be distributed to different systems on the network, then it adds a header to the frame to define the **physical address** of the sender **(source address)** and/or receiver **(destination address)** of the frame.

Flow Control : If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender, it imposes a flow control mechanism to prevent overwhelming the receiver.

Error Control : It adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames.

Access Control : When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Layer 3– Network Layer

The network layer is responsible for the source-to-destination delivery of a packet possibly across multiple network (links). Basically it is concerned with finding the shortest path to the destination. This usually means finding the fastest route through multiple networks to the destination. Routing algorithms are used to determine the "shortest" path. Shortest does not mean the physically shortest distance but fastest route.

The Network layer converts the segments into smaller protocol data units (PDUs) called packets that the network can handle. The Network layer is connectionless in that it does not guarantee that the packet will reach its destination. It is often referred to as "send and pray". The packet is sent out on the wire and we pray that is arrives.

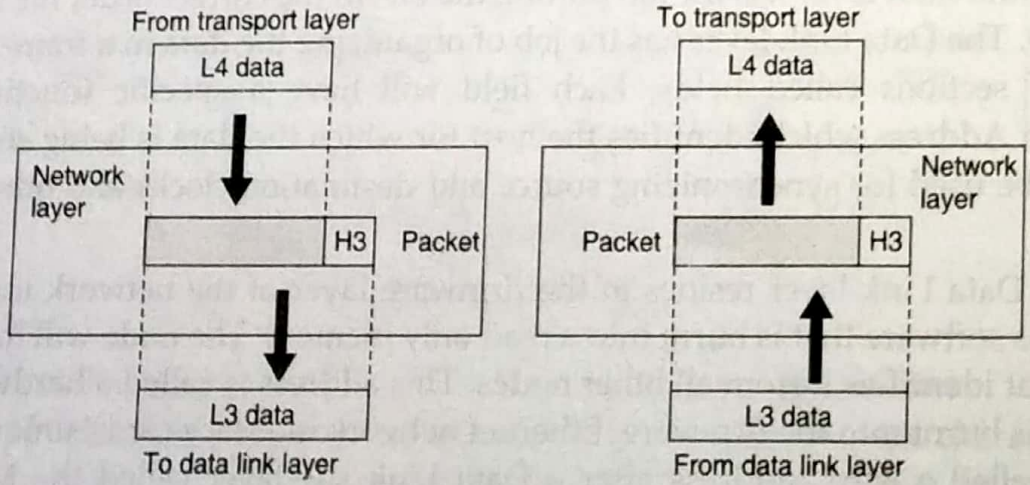


Fig. 2.7. Network layer

Network is identified by network addresses that are separate from node addresses. Since the Network layer is concerned with finding networks, it adds the source and destination addresses to the packet. The given figure shows the relationship of the network layer to the data link and transport layers.

Specific responsibilities of the network layer include the following :

Logical Addressing : The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. It adds a header to the packet coming from the upper layer that, among other things, includes the **logical addresses** of the sender and receiver.

Routing : When independent networks or links are connected together to create an *internetwork* (a network of networks) or a large network, the connecting devices (called *routers* or *gateways*) route the packets to their final destination.

Layer 4- Transport Layer

As we know the network layer oversees end-to-end delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. Whereas the transport layer is responsible for source-to-destination (end-to-end) delivery of the entire message. It ensures that the whole message arrives intact and in order, overseeing error control as well as flow control at the source-to-destination level.

The Transport layer's main job is to provide error free end to end delivery of data. The file is broken up into smaller sized data units called segments. The segments are numbered and sent off to the destination. The destination acknowledges receipt of the each segment by replying with an acknowledgement.

Networks are dynamic, meaning that the path to the destination may change while the information is being sent. This can cause the segments to arrive in an out of order sequence. Since there is no guarantee that the segments will arrive in the correct order, the Transport layer will correct out of order segments and put them in the correct order.

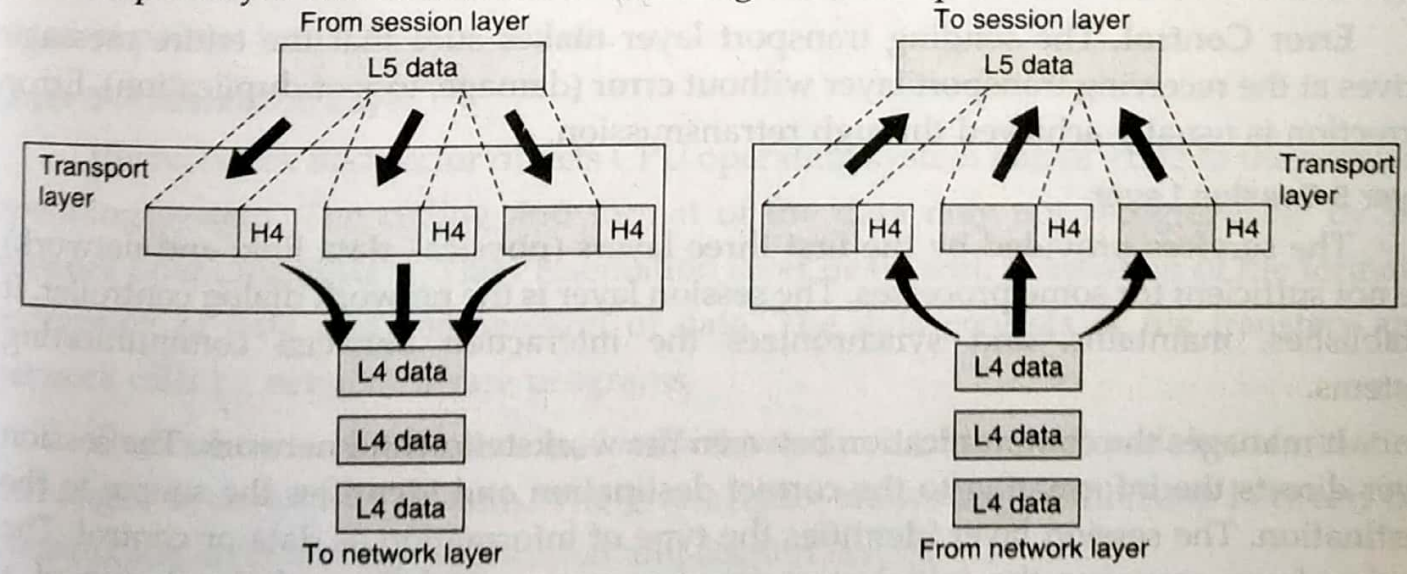


Fig. 2.8. Transport layer

If a segment that has been sent to the destination has not been acknowledged within a certain time period by the source. The transport layer will time out and resend the segment. If the destination does not receive or misses a segment in a sequence within a certain period of time, it will request that the missing segment be resent.

The Transport also provides error checking to make that data received hasn't been corrupted during transmission. The Transport layer guarantees an error-free host connection, it is not concerned with the path between machines. The given figure shows the relationship of the transport layer to the network and session layers.

The transport layer is concerned with the following responsibilities :

Service-point Addressing : Sometimes several programs run at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header therefore must include a type of address called a *service-point address* (or port address).

Segmentation and Reassembly : A message is divided into transmittable segments, each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in the transmission.

Connection Control : The transport layer can be either connectionless or connection-oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

Flow Control : Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.

Error Control. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without **error** (damage, loss or duplication). Error correction is usually achieved through retransmission.

Layer 5-Session Layer

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction between communicating systems.

It manages the communication between the workstation and network. The session layer directs the information to the correct destination and identifies the source to the destination. The session layer identifies the type of information as data or control. The session layer manages the initial start-up of a session and the orderly closing of a

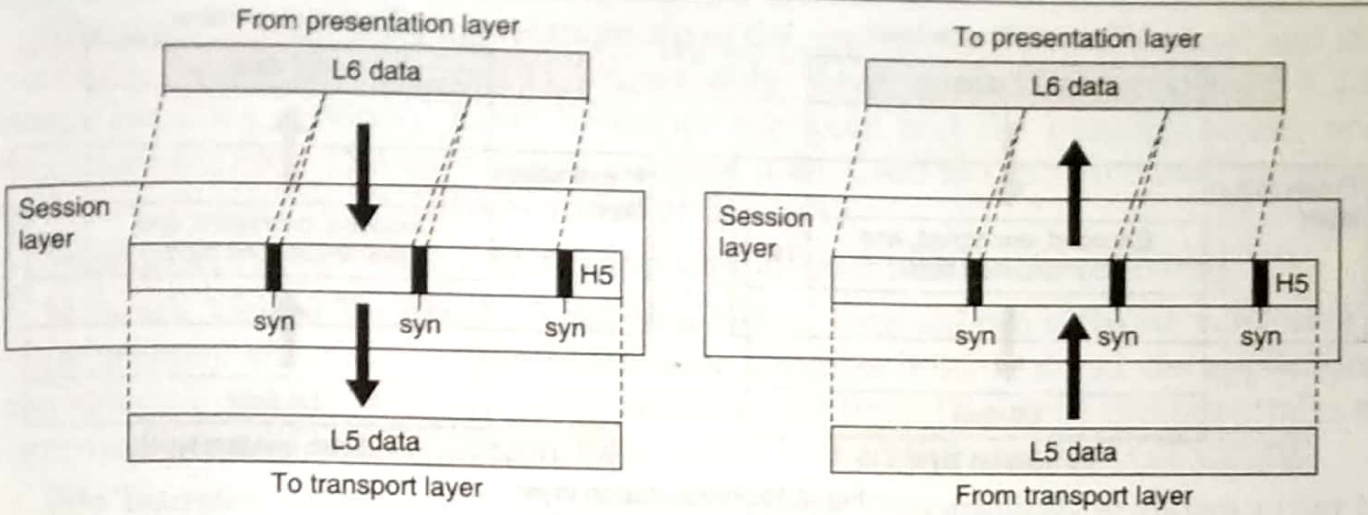


Fig. 2.9 Session layer

session. The Session layer also manages Logon procedures and Password recognition and permissions.

The session layer is concerned with managing the communication. Does the source have rights and permission to access the destination ? Is the destination alive and present ? The session layer will periodically check to see if the both source and destinations are still operating and will timeout if no communication has been seen for a while.

The given figure shows the relationship of the session layer to the transport and presentation layers.

The responsibilities of the session layer include the following :

Dialog Control : The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place either in half-duplex (one way at a time) or full-duplex (two ways at a time).

Synchronization : The session layer allows a process to add checkpoints (synchronization points) into a stream of data.

Layer 6-Presentation Layer

The Network Redirector directs CPU operating system native code to the network operating system. The coding and format of the data may not recognizeable by the network operating system. The Presentation layer deals with translation of file formats, encryption of data and compression of data. The data consists of file transfers and network calls by network aware programs.

Thus we can say it is concerned with the syntax and semantics of the information exchanged between two systems. The given figure shows the relationship between the presentation layer and the application and session layers.

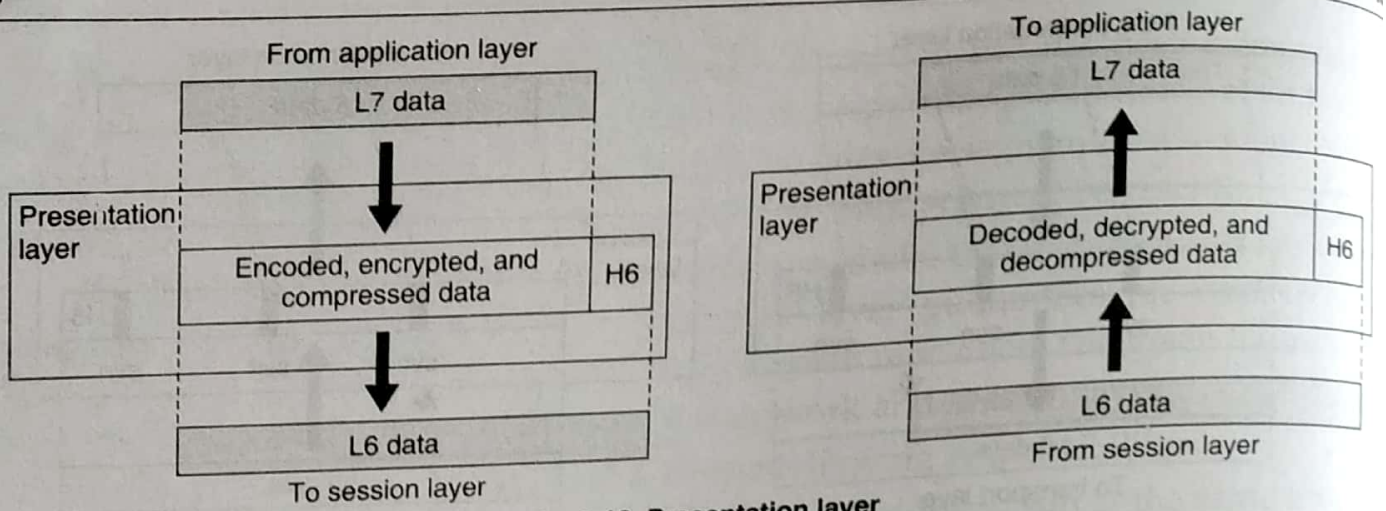


Fig. 2.10. Presentation layer

The responsibilities of the presentation layer include the following :

Translation : The processes (running programs) in two systems are usuall exchanging information in the form of character strings, numbers, and so on. Th information should be changed to bit streams before being transmitted. Becaus different computers use different encoding systems, the presentation layer is responsibl for interoperability between these different encoding methods.

Encryption : Encryption means that the sender transforms the original informatio to another form and sends the resulting message out over the network. Decryptio reverses the original process to transform the message back to its original form.

Compression : Data compression reduces the number of bits to be transmitted Data compression becomes particularly important in the transmission of multimedi such as text, audio and video.

Layer 7-Application Layer

The **application layer** enables the user, whether human or software, to access th network. It provides user interfaces and support for services such as electronic mail remote file access and transfer, shared database management, and other types o distributed information services.

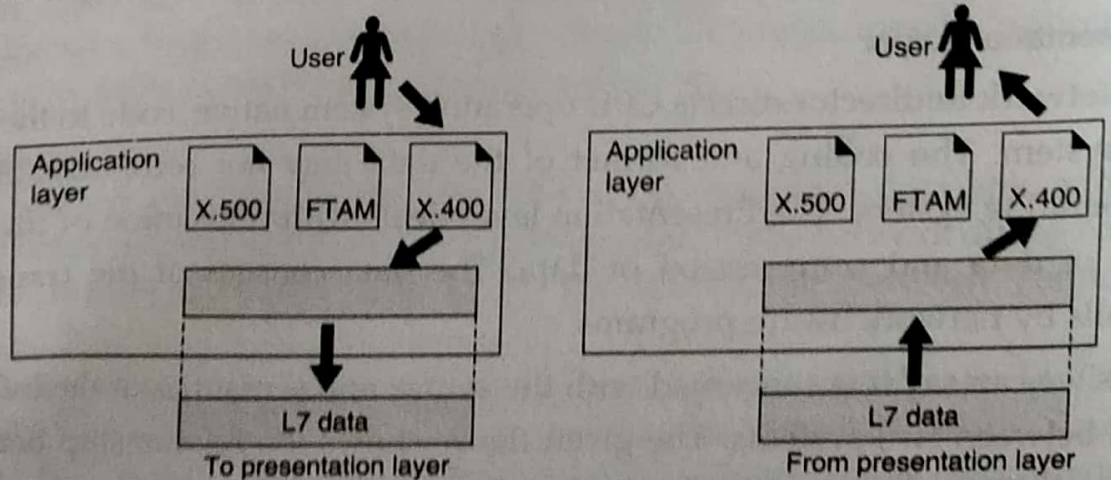


Fig. 2.11. Application layer

The given figure shows the relationship of the application layer to the user and the presentation layer. The figure 2.11 shows only three application services : X.400 (message-handling services); X.500 (directory services); and file transfer, access, and management (FTAM). The user in this example uses X.400 to send an e-mail message. Note that no headers or trailers are added at this layer.

Specific services provided by the application layer include the following :

Network Virtual Terminal : A network virtual terminal is a software version of a physical terminal and allows a user to log on to a remote host. To do so, the application creates software emulation of a terminal at the remote host. The user's computer talks to the software terminal, which, in turn, talks to the host and vice-versa.

File Transfer, Access and Management (FTAM) : This application allows a user to access files in a remote computer; and to manage or control files in a remote computer.

Mail Services : This application provides the basis for e-mail forwarding and storage.

Directory Services. This application provides distributed database sources and access for global information about various objects and services.

2.9. Functions Performed by Different Layers

The given table shows a summary of functions performed by different layers in the OSI model.

Table 2.1.

Layer Number	Layer Name	Description
7	Application layer	Interfaces user applications with network functionality, controls how applications access the network, and generates error messages. Protocols at this level include HTTP, FTP, SMTP and NFS.
6	Presentation layer	Translates data to be transmitted by applications into a format suitable for transport over the network. Redirector software, such as the workstation service for Microsoft Windows NT, is located at this level. Network shells are also defined at this layer.
5	Session layer	Defines how connections can be established, maintained, and terminated. Also performs name resolution functions.
4	Transport layer	Sequences packets so that they can be ressembled at the destination in the proper order. Generates acknowledgments and retransmits packets. Assembles packets after they are received.

3	Network layer	Defines logical host addresses such as IP addresses, creates packet headers, and routes packets across an internetwork using routers and Layer 3 switches. Strips the headers from the packets at the receiving end.
2	Data-link layer	Specifies how data bits are grouped into frames, and specifies frame formats. Responsible for error correction, flow control, hardware addressing (such as MAC addresses), and how devices such as hubs, bridges, repeaters, and layer 2 switches operate. The Project 802 specifications divide this layer into two sublayers, the logical link control (LLC) layer and the media access control (MAC) layer.
1	Physical layer	Defines network transmission media, signaling methods, bit synchronization, architecture (such as Ethernet or token ring), and cabling topologies. Defines how network interface cards (NICs) interact with the media (cabling). You can think of each layer as being logically connected to the same layer on a different computer on the network. For example, the application layer on one machine communicates with the application layer on another machine. But this communication is logical only; physical communication occurs when packets of data are sent down from the application layer of the transmitting computer, encapsulated with header information by each lower layer and then put on the wire at the physical layer of the transmitting computer. After traveling along the wire, the packets are picked up by the physical layer of the receiving computer, passed up the seven layers while each layer strips off its associated header information, and then passes to the application layer of the receiving computer, where the receiving application can process the data.

2.10. Enhancements to the OSI Model

The bottom two OSI layers, the Physical layer and the Data Link layer, define how multiple computers can simultaneously use the network without interfering with each other.

The IEEE 802 project worked with the specifications in those two layers to create specifications which have defined the dominant LAN environments.

The 802 Standards Committee decided that more detail was needed at the Data Link layer. They divided the Data Link layer into two sublayers :

(a) Logical Link Control (LLC)—error and flow control
(b) Media Access Control (MAC)—access control

Logical Link Control Sublayer

The LLC manages data-link communication and defines the use of logical interface points, called service access points (SAPs). Other computers can refer to and use SAPs to transfer information from the LLC sublayer to the upper OSI layer. These standards are defined by 802.2.

Media Access Control Sublayer

The figure given below indicates the media access control sublayer is the lower of the two sublayers, providing shared access for the computer's network adapter cards to the Physical layer. The Media Access Control layer communicates directly with the network adapter card and is responsible for delivering error-free data between two computers on the network. Categories 802.3, 802.4, 802.5 and 802.12 define standards for both the is sublayer and OSI layer 1, the Physical Layer consider the given figure.

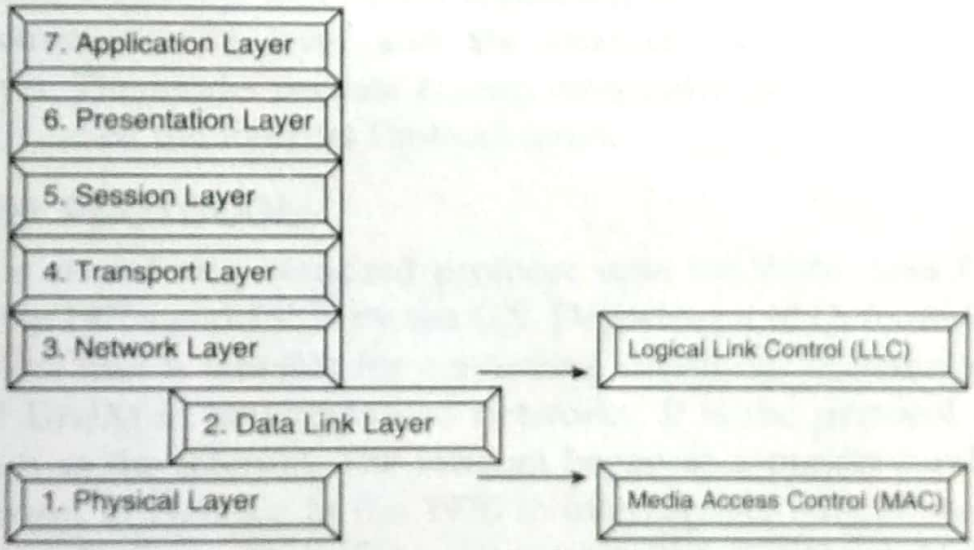


Fig. 2.12 Sub-layers of Datalink layer

Logical Link Control (LLC)

802.1 OSI Model and network Management
802.2 Logical Link Control
Media Access Control (MAC)
802.3 CSMA/CD
802.4 TOKEN BUS
802.5 TOKEN RING
802.12 DEMAND PRIORITY

Fig. 2.13. Standards for LLC and MAC

EXERCISE

1. Define the term network architecture.
2. mention some network architecture.
3. Explain the brief protocol.
4. Describe the concept of layering in the communication process.
5. What are the advantages of applying layered approach?
6. What do you mean by OSI reference model? Explain in detail.
7. What are the seven layers of OSI model?
8. List and explain all the layers of OSI models.
9. Define the term protocol stack.
10. Write the functions of physical and data link layers of OSI model.
11. Differentiate between network and transport layer.
12. Describe the functions of application layer.