CHAPTER 2

Unit I

Network Models

Syllabus :

Network models, Protocol layering, Scenarios, Principle of protocol layering, Logical connections, TCP/IP protocol suite, Layered architecture, Layers in TCP/IP protocol suite, Encapsulation and Decapsulation, Addressing, Multiplexing and Demultiplexing, Detailed introduction to physical layer, Detailed introduction to data link layer, Detailed introduction to the network layer, Detailed introduction to the transport layer, Detailed introduction to application layer.

2.1 Network Models :

- This chapter is the base for the remaining book. In this chapter the idea of network model has been discussed first and then the TCP/IP protocol suite has been discussed in detail.
- In order to define the computer network operations, two models have been derived. They are as follows :
  1. TCP/IP protocol suite.
  2. OSI model.
- The International Standards Organisation (ISO) covers all aspects of network communication in the Open Systems Interconnection (OSI) model.
- An OSI model is a layered framework for the design of network systems that allows for communication across all types of computer systems.
- The purpose of each layer is to offer certain services to the higher layers.
- Layer n on one machine (source) will communicate with layer n on another machine (destination).
- The rules and conventions used in this communication are collectively known as the layer n protocol.
- Basically a protocol is an agreement between the two communicating machines about how the communication link should be established, maintained and released.

2.2 Protocol Layering :

Protocol :

A protocol in data communication and networking is designed to define certain rules which are to be followed by both sender and the receiver and all the intermediate devices, so as to make the communication effective.

Protocol layering :

- For a simple type of communication, we need to use only one simple protocol.
- However for a complex type of communication, we need to divide the tasks among various layers. At each layer we need to use a protocol to carry out a specific task. This is known as **protocol layering.**

2.2.1 Scenarios :

Need of protocol layering :

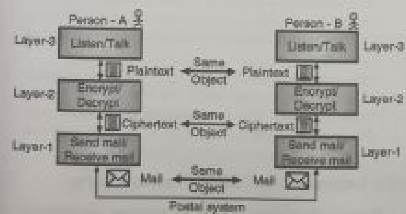
In order to understand the need of protocol layering, let us develop two simple scenarios as follows :

1. **First scenario :**
   - In the first scenario, the communication between the source and destination is very very simple. Therefore only **one layer** will be sufficient to carry it out successfully.
   - Assume that A and B are neighbours staying next to each other in the same building. They speak the same language and can talk face to face very easily and frequently.
   - Therefore the communication between A and B can take place in one layer as shown in Fig. 2.2.1(a).

(G-2062) **Fig. 2.2.1(a) : A single layer protocol**

   - Even in the simple single layer scenario, a set of rules must be followed. The set of rules which should be followed by both A and B are as follows :
     1. Both A and B should greet each other.
     2. They must choose proper words for communication.
     3. If A is speaking, B should remain silent and listen to A and vice versa.
     4. Both know that the communication should be bidirectional (dialog) and not unidirectional (monolog).
     5. They should say goodbye while leaving.

2. **Second scenario :**
   - Now let us discuss the second scenario, in which person A has been offered a high-level position in his company and therefore he needs to relocate himself to company's another branch which is located in a city which is far away from person B.
   - But A and B being very good friends wish to continue their communication about an innovative project to start a new business after their retirement.
   - They choose the conventional mail through post office as their way of communication. But they do not want to reveal their ideas to anyone in case their mails are intercepted. Therefore both of them agree upon using the technique of **encryption and decryption.**
   - Thus the sender encrypts the letter so that any intruder won't be able to read and understand the contents of the letter.
   - Only the receiver knows how to decrypt it. So he will decrypt the received letter and understand its contents.
   - From this discussion we conclude that the communication between A and B takes place in three layers as shown in Fig. 2.2.1(b). Let us assume that both persons A and B have three different machines or robots to perform the tasks specified at each layer.
   - Refer Fig. 2.2.1(b) and imagine that person A sends the first letter to B. For this A talks to the robot at layer-3 as if it is person B.
   - The layer-3 robot (or machine) listens to what A says and converts it into the **plaintext** i.e. a letter written in English. This letter is then sent to the robot or machine present at layer-2.
   - This **plaintext** is encrypted by the machine at layer-2 to create the **ciphertext** which is sent to the machine present at layer-1.
   - The robot/machine present at layer-1 will take the ciphertext, puts it in an envelope, write the addresses of sender and receiver over it and mails the envelope.



(G-2063) **Fig. 2.2.1(b) : A three layer protocol**

   - At **person B's place,** the letter from the mailbox is picked up by the robot/machine at layer-1, the letter in the **ciphertext** is taken out of the envelope and gives it to the machine/robot at layer-2.
   - The machine at layer-2, decrypts the ciphertext to obtain the **plaintext** and hands it over to the machine at layer-3.
   - Finally the machine/robot present at layer-3 reads the plaintext as if person A is talking to person B.

Advantages of protocol layering :

1. It allows us to divide a complex task into many simpler tasks.
2. It allows us to separate the services from the implementation.
3. In practice, the communication does not always take place directly between the two end systems (A and B) but there are intermediate systems which need only some layers. Without the protocol layering the intermediate systems will be as complex as the two and system, thus making the entire system very complex and expensive.
4. It simplifies the design process as the function of each layer is well defined.
5. It provides flexibility to modify and develop network services.
6. Addition of new services and management of network infrastructure becomes easy.

Disadvantages of protocol layering :

1. We lose the touch with reality.
2. Sometimes the protocol layering can result in poor performance of protocol.

2.2.2 Principles of Protocol Layering :

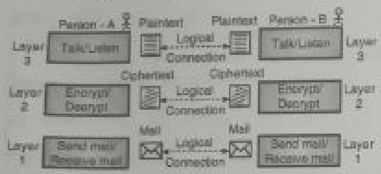
There are two different principles of protocol layering. We will discuss them one by one.

1. **First principle :**
   - According to the first principle, in order to have a successful bidirectional communication, each layer should be able to perform two opposite tasks one in each direction.
   - For example layer-1 performs send and receive mail functions or layer-2 performs the encryption and decryption and so on.
2. **Second principle :**
   - According to the second principle, in protocol layering the two objects under each layer at both the ends should be the same.
   - For example in Fig. 2.2.1(b), the object under the second layer at A as well as B is cipher text.

2.2.3 Logical Connections :

- We can think of the logical connection between each layer as shown in Fig. 2.2.2. This is after following the two principles of protocol layering.

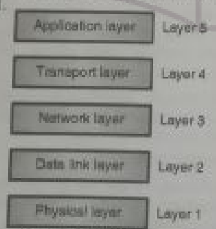
- Fig. 2.2.2 shows that there is a logical (imaginary) connection from a layer at A to the corresponding layer at B.
- The logical connection between each layer implies that there is a layer to layer communication.
- Due to logical connections, persons A and B can think that it is possible to send the object created from layer to the corresponding layer at the other end.



(G-2064) **Fig. 2.2.2 : Concept of logical connections between the peer layers**

2.3 TCP/IP Protocol Suite :

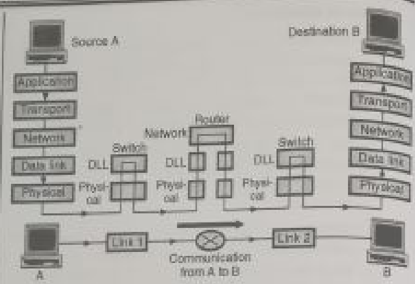
- After discussing about the concept of protocol layering and about the logical communication taking place between layers, now it is time to introduce the **TCP/IP protocol suite.**
- TCP/IP is the short form of two important protocols namely Transmission Control Protocol/Internet Protocol.
- A **protocol suite** is defined as the set of protocols organized in different layers. The TCP/IP protocol suite is used in Internet today.
- TCP/IP is a hierarchical protocol suite means that each upper layer protocol receives support and services from either one or more lower level protocols.
- In the original TCP/IP protocol suite, there were four software layers built upon the hardware. But today's TCP/IP protocol suite uses a five layer model as shown in Fig. 2.3.1.



(G-2065) **Fig. 2.3.1 : Layers in TCP/IP protocol suite**

2.3.1 Layered Architecture :

- In order to understand how the communication takes place between various layers of TCP/IP protocol suite, we have considered a small internetwork consisting of three LANs (links) with all LANs connected to each other via a router as shown in Fig. 2.3.2.



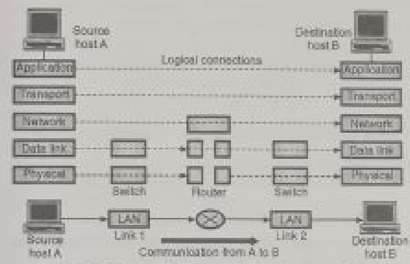
(G-2176) **Fig. 2.3.2 : Communication through an Internet**

- In Fig. 2.3.2, there are two computers A and B communicating with each other and three more devices namely : the link layer switch in link-1, the router and the link layer switch in link-2.
- Computer A is called as the **source host** and computer B is called as the **destination host.**
- Each device in the Internet has a specific role to play, depending on which each device uses a set of layers as shown in Fig. 2.3.2.
- All the five layers are involved in communication for the source and destination hosts A and B respectively.
- At the source host, a message is created at the application layer and then it is sent in down the layers in order to physically send it to the destination host.
- At the destination host this message is received at the physical layer and then it is delivered to the application layer via the other layers between the physical and application layers.
- At the router, as shown in Fig. 2.3.2 only three layers of TCP/IP protocol suite are needed to be involved. Thus a router does not need the transport or application layers when it is being used only for routing.
- The router is connected to multiple links. At each link we use a switch which involves only two layers of the TCP/IP protocol suite as shown in Fig. 2.3.2.
- However note that the link layer and physical layer protocols used by each link can be completely different.
- Thus the router may have to receive a packet from link-1 based on one pair of protocol and may have to deliver a packet to link-2 based on a totally different pair of protocols.
- Now consider a switch in Fig. 2.3.2 which shows that it has two different connections. But both of them belong to the same link. Therefore two different protocol pairs will not be involved. A switch has to deal with only one pair of DLL and physical layer protocols.

2.3.2 Layers in the TCP/IP Protocol Suite :

- Now we are going to discuss the functions and duties of various layers in the TCP/IP protocol suite.

- In this section, we will think about the logical connections between various layers, so as to clearly understand the duties of each layer.
- The logical connections in a simple internetwork have been shown in Fig. 2.3.3.



(G-2177) **Fig. 2.3.3 : Logical connections between the layers of TCP/IP suite**

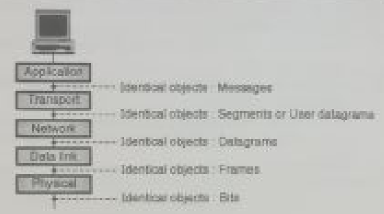
- Each layer has some specific duties and we can use the logical connections to think about them easily.
- From Fig. 2.3.3 it is clear that the network, transport and application layers have an **end-to-end** duty. But the data link and physical layers have the **hop to hop** duty. (Hop is a host or router).
- In this way the upper three layers have a **domain of duty** of the entire Internet while the lower two have a domain of duty of only link.

Data unit created by every layer :

- We can think about the logical connections in a different way i.e. in terms of the **data unit** created by each layer.
- The names of data units (packets) created by different layers are as follows :

Layer	Data unit	Layer	Data unit
Application	Message	Datalink	Frame
Transport	Segment	Physical	Bits
Network	Datagram		

- The data unit (packet) created by the top three layers, should not be changed by a router or a link layer switch.
- However the data unit created at the lower two levels can be changed only by the router. The link layer switches cannot modify it.
- The second principle that we discussed for the protocol layering has been shown in Fig. 2.3.4. Note that the objects shown below each layer related to each device are identical.



(G-2178) **Fig. 2.3.4 : Identical objects in the TCP/IP suite**

2.4 Detailed Description of Each Layer :

In this section we are going to discuss the duties of various layers in TCP/IP.

2.4.1 Detailed Introduction to Physical Layer :

- Physical layer is the lowest layer in the TCP/IP protocol suite. The communication at the physical layer level is still **logical** because of the presence of a hidden layer (transmission media) under the physical layer.
- The **primary responsibility** of the physical layer is to carry the individual bits present in a frame across the link.
- The transmission media (wired or wireless) is used for connecting two devices to each other. Here it is important to understand that the transmission media does not actually carry the bits.
- Instead it carries the electrical or optical signals which represents the bits which are to be carried from one device to the other.
- That means the bits received in a frame from the data link layer are transformed into an electrical or optical signal and sent over the transmission media.
- Still we consider **bit** as the data unit for communication between physical layers of two communicating devices.
- For the transformation of bits to signal, several physical layer protocols are available.

Following are the functions of the physical layer :

1. To define the type of encoding i.e. how 0's and 1's are changed to signals.
2. To define the transmission rate i.e. the number of bits transmitted per second.
3. To deal with the synchronization of the transmitter and receiver.
4. To deal with network connection types, including multipoint and point-to-point connections.
5. To deal with physical topologies i.e. bus, star, ring, or mesh.

6. To deal with the media bandwidth i.e. baseband and broadband transmission.
7. Multiplexing which deals with combining several data channels into one.
8. To define the characteristics between the device and the transmission medium.
9. To define the transmission mode between two devices i.e. whether it should be simplex, half duplex or full duplex.

> **Note :** Passive hubs, simple active hubs, terminators, couplers, cable and cabling, connectors, repeaters, multiplexers, transmitters, receivers, transceivers are associated with the physical layer.

2.4.2 Detailed Introduction to Data Link Layer :

- An internetwork consists of many LANs and WANs, connected to each other by routers.
- While travelling from source to destination a datagram has to travel through many overlapping sets of links.
- It is the responsibility of router to choose the best possible link for a datagram to travel.
- When a router does so, it is the responsibility of the data link layer to take the datagram across the link.
- The said link can be anything such as a wired LAN, a wireless LAN, or a link layer switch etc. Every type of link will use different types of protocols. The data link layer should be able to handle all the different types of protocols and move the packet through the link.
- The data link layer receives a datagram from the network layer and encapsulates it into a packet called as **frame.**
- There are no specific data link layer protocols defined by the TCP/IP suite. Instead it supports all the standard protocols that can carry the datagram successfully over the link.
- The services provided by each data link layer protocol are different.

Following are the functions of data link layer :

1. Framing :

The bits received from the network layer are divided into another type of data units called frames at the data link layer.

2. Flow control :

It provides a flow control mechanism to avoid a fast transmitter from over-running a slow receiver by buffering the extra bits.

3. Physical addressing :

It adds a header to the frame which consists of the physical address of the sender and / or receiver of that frame.

4. Error control :

A trailer is added at the end of the frame in order to achieve error control. It also uses a mechanism to prevent duplication of frames.

5. Access control :

- The data link layer protocol perform an important function of determining which device has control over the link at any given time, when two or more devices are connected to the same link.
- The Institution of Electrical and Electronics Engineers (IEEE) felt the need to define the data link layer in more details, so they split it into two sub-layers :
  1. Logical Link Control (LLC).
  2. Media Access Control (MAC).

2.4.3 Detailed Introduction to Network Layer :

- The primary responsibility of the network layer is to create a connection between the source and destination computers. The communication at the network layer level is called as host to host communication.
- The several routers present between the source and destination hosts choose the best route for each travelling packet.
- Therefore the two responsibilities of the network layer are : host to host communication and routing of the packet through the possible routers.
- The main protocol in the network layer of the Internet is IP (Internet Protocol). The format of the packet (datagram) at network layer is decided by IP.
- The routing of datagrams from their source to destination is also the responsibility of IP. It achieves this by making each router forward the datagrams to the next router in its path towards the destination.
- IP is a **connectionless** protocol. It does not provide services like **flow control, error control** or even the **congestion control.**
- Therefore it is dependent on the transport layer in case if an application needs these services.
- The routing protocols included in the network layer are of unicast (one-to-one) and multicast (one-to-many) nature.
- These routing protocols have a responsibility of creating the forwarding tables for the routers to help them in the process of routing.
- There are some auxiliary protocols at the network layer, that are designed to assist IP in its delivery and routing tasks. The examples of such protocols are ICMP, IGMP, DHCP, ARP etc.
- The functioning of these protocols is as follows :

Sr. No.	Protocol	Function
1.	ICMP	To help IP report problems when routing a packet
2.	IGMP	Helps IP in multitasking
3.	DHCP	To help IP to get the network layer address for a host.
4.	ARP	Helps IP to find the link layer address of a host or router.

Functions of the network layer :

1. It translates logical network address into physical machine addresses i.e. the numbers used as destination IDs in the physical network cards.
2. It determines the quality of service by deciding the priority of message and the route a message will take if there are several ways a message can get to its destination.
3. It breaks the larger packets into smaller packets if the packet is larger than the largest data frame the data link will accept.
4. It is concerned with the circuit, message or packet switching.
5. It provides connection oriented services, including network layer flow control, network layer error control and packet sequence control.
6. Routers and gateways operate in the network layer.

2.4.4 Detailed Introduction to Transport Layer :

- The primary responsibility of the transport layer is also to provide an end to end connection.
- At the source host, the application layer sends a message to the transport layer which **encapsulates** it into a transport layer packet (which is also called as a **segment** or **user datagram**) and sends it through the logical connection (which is imaginary) to the transport layer of the destination host.
- In short the transport layer takes message from the application layer of source host and via the transport layer at the destination host delivers the message to the application layer at the destination.
- For the Internet applications, there are number of transport layer protocols designed to give specific service to various application programs.
- The main protocol in the transport layer is TCP (Transmission Control Protocol) which is a connection oriented protocol.
- The main task of TCP is to establish a logical connection between the transport layers of the source and destination hosts before actually transferring the data.
- Being connection oriented, the TCP is a reliable protocol which provides the following services to an application layer program :
  1. Flow control 2. Error control and
  3. Congestion control
- The other commonly used transport layer protocol is UDP (User Datagram Protocol). This is a connectionless protocol. Therefore it does not need to create any logical connection before transmitting the user datagrams.
- The UDP treats each datagram as a totally in dependent packet with absolutely no relation with the previous or next datagrams.
- UDP is a very simple protocol as compared to TCP. It does not provide flow control, error control or congestion control.
- UDP is an attractive protocol for certain application program specially for those who want to send small messages or those who do not afford retransmission of a packet if the packet is corrupted or lost.
- For new emerging applications in the field of multimedia, a new transport layer protocol has been designed which is called as SCTP (Stream Control Transmission Protocol).

Functions of transport layer :

The transport layer performs the following functions :

1. It divides each message into packets at the source and re-assembles then at the destination.
2. The transport layer header H4 includes a service point address to deliver a specific process from source to a specific process at the destination.
3. The transport layer is capable of either connectionless or connection-oriented transfer of data.
4. It performs end to end flow control. Flow control is an important function of the transport layer.
5. It makes sure that the entire message arrives at the receiving transport layer without error.

2.4.5 Detailed Introduction to Application Layer :

- The logical connection between the application layers of source and destination hosts is **end-to-end** type.
- The communication between the application layers of source and destination hosts takes place through all the layers.
- The application layer communication is between **two processes.** A process is nothing but a program running at the application layer.
- Thus the primary responsibility of the application layer is the **process to process communication.**
- There are many predefined protocols at the application layer in the Internet. Some of these protocols are HTTP, WWW, SMTP, FTP, TELNET, SNMP etc. These protocols and their functions are shown in Table 2.4.1.

Table 2.4.1

Sr. No.	Protocol	Function
1.	HTTP	As tool to access World Wide Web i.e. WWW.
2.	SMTP	It is the main protocol used in e-mail service.
3.	FTP	To transfer files from one host to the other.
4.	TELNET	To access a website remotely.
5.	SNMP	To manage the Internet.

Sr. No.	Protocol	Function
6.	DNS	To find the network layer address of a computer.
7.	IGMP	To collect the membership in a group.

The application layer performs the following functions :

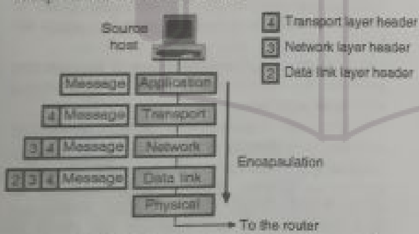
1. The application layer allows the creation of a virtual terminal which is the software version of a physical terminal. The user can log on to the remote host due to this arrangement.
2. The application layer provides File Transfer Access and Management (FTAM) which allows a user to access, retrieve, manage or control files in a remote computer.
3. It creates a basis for forwarding and storage of e-mails.

2.5 Encapsulation and Decapsulation :

- The encapsulation / decapsulation is one of the most important concepts in the protocol layering in Internet.
- This concept applied to a small Internet has been illustrated in Fig. 2.5.1.
- In this figure, the layers of data link switches have not been shown because encapsulation or decapsulation does not take place in the data link layer switches.
- In Fig. 2.5.1, the encapsulation takes place at the source host, decapsulation takes place at the destination host while both encapsulation and decapsulation takes place at the router.

2.5.1 Encapsulation at the Source Host :

Refer Fig. 2.5.1(a) to understand the process of encapsulation at the source host.



(G-2866) **Fig. 2.5.1(a) : Encapsulation at the source host**

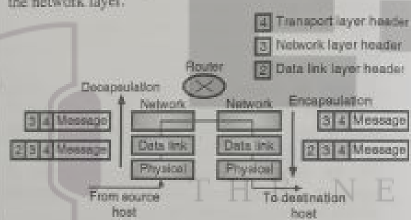
1. The data to be exchanged at the application layer is called as **message.** Normally a message does not contain any header or trailer. This message is passed on to the transport layer.
2. The transport layer takes this message which is also called as the **payload** and adds a transport layer header to it to produce the **segment** of **user datagram.** It is then passed on to the network layer. The transport layer header consists of the identifiers of the application programs at the source and destination and some additional information needed for the flow control, error control and congestion control.
3. The packet from transport layer is accepted by the network layer as its payload and adds its own header to it to produce a **datagram** as shown in Fig. 2.5.1(a). The network layer header contains the source and destination host's addresses and some additional information needed for checking errors in the header. This network layer packet (datagram) is then passed on to the data link layer.
4. The packet from the network layer is taken by the data link layer as its payload and adds its own header to it to produce a **frame** (packet at the data link layer). The link layer header contains the link layer addresses of the host or the next hop i.e. the router. This **frame** is then passed on to the physical layer for transmission.

2.5.2 Decapsulation and Encapsulation at the Router :

Refer Fig. 2.5.1(b) which illustrates the processes of decapsulation and then encapsulation occurring at a router connected to two or more links.

1. **Decapsulation :**

The router receives a set of bits at its input port. When these bits are delivered to the data link layer at the router, it decapsulates the datagram from the frame as passes it on to the network layer.

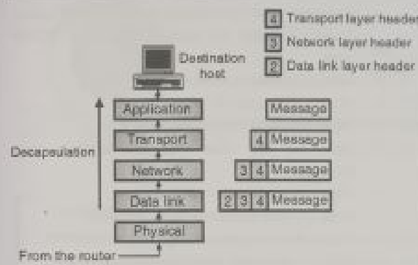


(G-2867) **Fig. 2.5.1(b) : Decapsulation / Encapsulation at the router**

2. The router checks the header for source and destination addresses. Then it refers to its forwarding tables and finds out the next hop to which this datagram is to be forwarded. Note here that the network layer at the router should not change the contents of the datagram unless fragmentation of the datagram is needed. Fragmentation is done if the datagram is too large in size. After all this, the datagram is passed to the data link layer.
3. At the data link layer, the datagram received from the network layer is encapsulated again into a frame and the frame is passed on to the physical layer which transmits it to the destination host.

2.5.3 Decapsulation at the Destination Host :

- At the destination host, only the decapsulation process is carried out at each layer, as shown in Fig. 2.5.1(c).



(G-2868) **Fig. 2.5.1(c) : Decapsulation at the destination host**

- At each layer, the payload is removed from the packet and the payload is delivered to the higher layer, by removing the headers at each stage.
- Finally after removing all the headers, the message is delivered to the application layer.
- It is important to note that the **error checking** is involved in the process of decapsulation at the destination host.

2.6 Addressing :

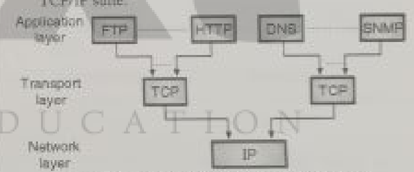
- Addressing is another important concept related to the protocol layering in the Internet.
- There is a logical connection between the pair of layers as discussed earlier. For any communication to take place between a source and a destination, two addresses namely source address and destination address are needed.
- Thus we will need four pairs of such addresses corresponding to the data link, network, transport and application layers.
- There is no need of addresses at the physical layer because communication at the physical layer takes place in bits which can not have an address.
- Fig. 2.6.1 shows the addressing at each layer.

(G-2869) **Fig. 2.6.1 : Addressing in TCP/IP protocol suite**

- Fig. 2.6.1 also shows the relationship between various layers, the addresses used in each layer and the name of the packet at each layer.
- We generally use the **names** to define the **site address** which provides the required services. For example **techmaxbook.com,** at the application layer. It is also possible to use the email address such as **jayantkatre@gmail.com.**
- The addresses at the transport layer are called as **port numbers.** These define the programs at the application layer of source and destination.
- There are several application layer programs running at a time. Port numbers are the local addresses which are used to distinguish between these programs.
- The addresses at the network layer are global in nature because the whole Internet is the scope of these addresses.
- The connection of a device to the Internet is uniquely defined by a network layer address.
- The addresses at the data link layer are called as the **MAC addresses.** These are the locally defined addresses. Each host or router in a network such as LAN or WAN always has a MAC address.

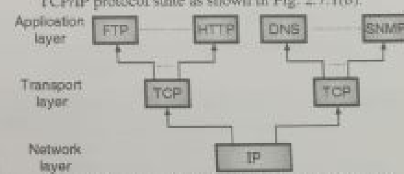
2.7 Multiplexing and Demultiplexing :

- In TCP/IP protocol, many protocols are being used at the same layer. Therefore multiplexing is needed at the source and demultiplexing is needed at the destination.
- In the process of **multiplexing** as shown in Fig. 2.7.1(a), a protocol at one layer in TCP/IP can encapsulate a packet (one at a time) from several protocols corresponding to the next higher layer in TCP/IP suite.



(G-2870) **Fig. 2.7.1(a) : Multiplexing in TCP/IP**

- In the process of demultiplexing, a protocol will decapsulate and deliver a packet one at a time to several protocols belonging to the next higher layer in TCP/IP protocol suite as shown in Fig. 2.7.1(b).



(G-2871) **Fig. 2.7.1(b) : Demultiplexing in TCP/IP**

- As shown in Fig. 2.7.1(a), at the transport layer two protocols TCP and UDP are capable of multiplexing the messages coming from various protocols at the application layer.

- Next the segments from TCP or user datagrams from UDP are accepted and multiplexed by IP at the network layer.
- IP can also multiplies the packets from some other protocols such as ICMP or IGMP etc.
- The frames at the data link layer level can carry the payload coming from the network layer protocols such as IP or ARP etc.

Review Questions

Q. 1 State the names of two network models.
Q. 2 Define the word protocol.
Q. 3 What is protocol layering ?
Q. 4 Explain the concept of logical connections.
Q. 5 Draw the layers of TCP/IP suite.
Q. 6 Explain the layered architecture of TCP/IP suite.
Q. 7 Explain in detail the physical layer in TCP/IP suite.
Q. 8 Explain in detail the data link layer in TCP/IP suite.
Q. 9 Explain in detail the network layer in TCP/IP suite.
Q. 10 Explain in detail the transport layer in TCP/IP suite.
Q. 11 Explain in detail the application layer in TCP/IP suite.
Q. 12 Name any three network layer protocols.
Q. 13 Write a short note on : IP.
Q. 14 State various functions of network layer.
Q. 15 State the two most important transport layer protocols.
Q. 16 State various duties of transport layer.
Q. 17 State any four application layer protocols.
Q. 18 Explain the concept of encapsulation in TCP/IP.
Q. 19 Explain the concept of decapsulation in TCP/IP.
Q. 20 Write a note on following in TCP/IP suite :
1. Addressing.
2. Multiplexing and demultiplexing.

❑❑❑

CHAPTER 3

Unit I

Data and Signals

Syllabus :

Data and signals, Analog and digital data, Analog and digital signals, Sine wave phase, Wavelength, Time and frequency domains, Composite signals, Bandwidth, Digital signal, Bit rate, Bit length, Transmission of digital signals, Transmission impairments, Attenuation, Distortion, Noise, Data rate limits, Performance, Bandwidth, Throughput, Latency (Delay).

3.1 Analog and Digital Signals :

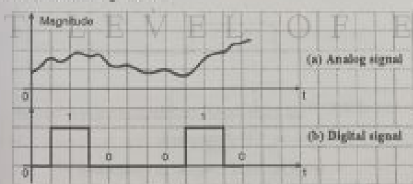
- Signals can be of two types :
1. Analog signals. 2. Digital signals.

1. Analog signal :

It is the signal in which the signal magnitude varies in a smooth fashion without any break with respect to time, as shown in Fig. 3.1.1(a).

2. Digital signal :

It is the signal in which the signal magnitudes has a constant level for some period of time, then it changes suddenly to another constant level as shown in Fig. 3.1.1(b). The examples of digital signal are binary signal, hexadecimal signal etc.



(L-24) **Fig. 3.1.1 : Types of signals**

3.1.1 Analog and Digital Data :

- Data are the entities which convey meaning, or information such as temperature, pressure etc. Signals are electric or electromagnetic representation of data. Thus signal is the representation of data.
- Data can be of two types :
1. Analog data 2. Digital data.

1. Analog data :

Analog data is the type of data that varies continuously (smoothly) with respect to time. Voice and video are the best examples of analog data. The other examples are temperature, pressure etc.

2. Digital data :

Digital data is the type of data that can take on discrete values i.e. it is discrete in nature. The examples of digital data are text and integers.

3.1.2 Sources of Digital Signal :

- The digital signals can be obtained directly from the computers. All the data used by the computers is digital.
- We can also use an A to D converter (Analog to digital converter) so as to convert analog signals into digital signals.

3.1.3 Advantages of Digital Signals :

1. Digital signals can be processed and transmitted more efficiently and reliably than analog signals.
2. It is possible to store the digital data.
3. Play back or further processing of the digital data is possible.
4. The effect of "noise" (unwanted voltage fluctuations) is less. So digital data does not get corrupt.
5. It is possible to separate signal and noise and use repeaters between the transmitter and receiver.
6. Use of microprocessor and digital systems is possible.

3.1.4 Comparison of Digital and Analog Signals :

Sr. No.	Parameter	Analog signals	Digital signals
1.	Number of values	Infinite	Finite (2, 8, 16 etc.)
2.	Nature	Continuous	Discrete
3.	Sources	Signal generators, transducers etc.	Computers, A to D converters
4.	Examples	Sinewave, triangular wave	Binary signal