*Overview of Network Models based on Protocol Layering*

*Author*  : *Sukanya K. Kamdi KDKCOE 7276820414* [*sukanyakamdi007@gmail.com*](mailto:sukanyakamdi007@gmail.com)

*Author : Nikhil Gourkhede KDKCOE 8446671776* [*nikhilone994@gmail.com*](mailto:nikhilone994@gmail.com)

*Author : Nilesh Parate KDKCOE 9175742422 nileshparate751993@gmail.com*

*Abstract –* Two models have been devised to define Computer Networks Operations: the TCP/IP Protocol suite and the OSI model. Both the models are based on the concept of protocol layering. This paper discusses two principles upon which protocol layering is based. The first principle dictates that the layer needs to have two opposite tasks. The second principle dictates that the corresponding layer should be identical. The layers of network models and their tasks are discussed.

*Index Terms –* International Organization for Standardization (ISO), Local area networks (LANs), Wide area networks (WANs), Transmission control protocol/Internet control protocol (TCP/IP), Open systems interconnection (OSI).

# Introduction

In data communication and networking, a protocol defines the rules that both sender and receiver and all intermediate devices need to follow to be able to communicate effectively. When communication is simple we may need only one simple protocol; when communication is complex, we may need to divide the task between layers, in which case we need a protocol at each layer , or **protocol layering**.

The two reference network models TCP/IP and OSI model have layered architecture. They have five and seven layers respectively. Each layers are assigned with particular task. Protocol layering enables us to divide a complex task into several smaller and simpler tasks. A layer can be defined as a black box with inputs and outputs, without concern about inputs are changed to outputs. One of the advantages of protocol layering is that it allows us to separate the services from the implementation. A layer needs to be able to receive a set of services from the lower layer and to give services to the upper layer. Another advantage of protocol layering is that communication does not always use only two end systems; there are intermediate systems that need only some layers, but not all layers. If we did not use protocol layering, we would have to make each intermediate system as complex as end systems, which makes the whole system more expensive.

# Scenarios

In first scenario, communication is so simple that it can occur in only one layer. Even in this simple scenario, we can see that a set of rules needs to be followed.

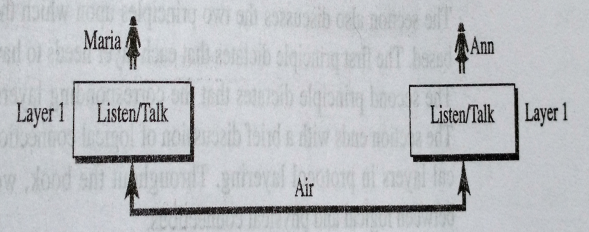


Fig. 1 A single-layer protocol.

First, Maria and Ann know that they should greet each other when they meet. Second, they know that they should confine their vocabulary to the level of their friendship. Third, each party knows that she should refrain from speaking when the other party is speaking. Fourth, each party knows that the conversation should be a dialog, not a monolog: both should get the opportunity to talk about the issue. Fifth, they should exchange some nice words when they leave.

Second scenario, the two friend lives in different cities but still want to continue their communication and exchange ideas because they have come up with an innovative project to start a new business when they both retire. They decide to continue their conversation using regular mail through the post office. However, they do not want that their ideas to be revealed by other people if the letter are intercepted. They agree on an encryption/ decryption technique. The sender of the letter encrypts it to make unreadable by an intruder; the receiver of the letter decrypts it to get the original letter.

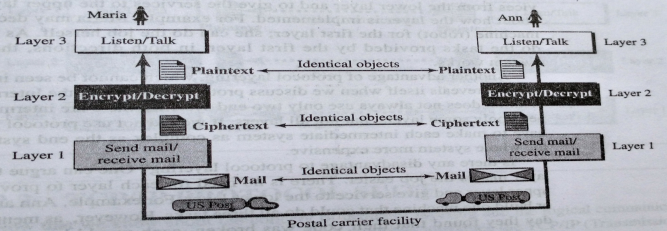


Fig. 2 A three-layer protocol.

Let us assume that Maria sends the first letter to Ann. Maria talks to the machine at the third layer as though the machine is Ann and is listening to her. The layer machine listens to what Maria says and creates the plaintext, which is passed to second layer machine. The second layer machine takes the plaintext, encrypts it, and creates a cipher text, which is passed to first layer machine, presumably a robot, takes a cipher text, puts it in envelope, adds the sender and receiver addresses, and mails it. On the other hand the reverse process is done in order to obtain the original message.

# Principles of protocol layering

The first principle dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction. For example, the third layer task is to listen (in one direction) and talk (in other direction).

The second principle is that the two object under each layer at both sites should be identical. For example, the object under layer three at both sites should be a plaintext letter.

# logical connections

After following the above two principles, we can think about logical connection between each layer as shown in fig.3. this means that we have layer-to-layer communication. Maria and Ann can think that there is a logical (imaginary) connection at each layer through which they can send the object created from that layer.

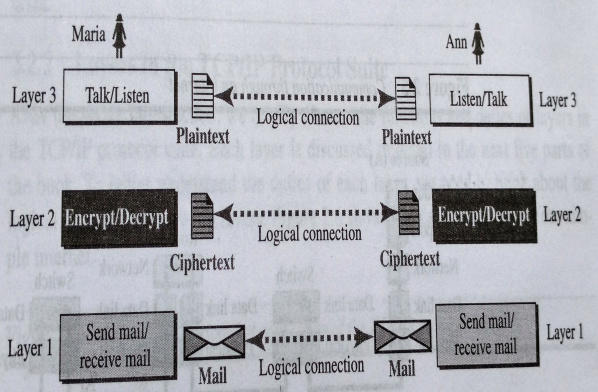


Fig.3 Logical connection

# tcp/ip protocol suite

TCP/IP is a protocol suite used in the Internet today. It is a hierarchical protocol made up of interactive modules, each of which provides specific functionality. The original TCP/IP protocol suite was defined as four software layers built upon the hardware. Today, however, TCP/IP is thought of as a five layer model.

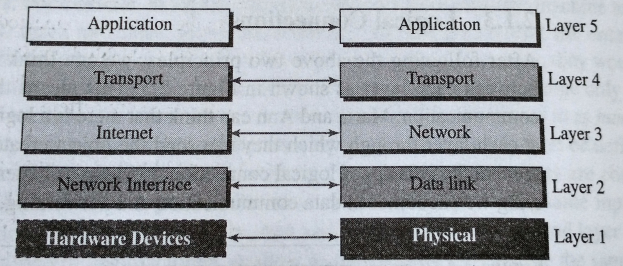


Fig.4 layers in the TCP/IP protocol suite.

1. *Physical Layer*

The physical layer is responsible for carrying individual bits in a frame across the link. Although the physical layer is the lowest layer in the TCP/IP protocol suite, the communication between two devices at the physical layer is still logical communication because there is another, hidden layer, the transmission media, under the physical layer(cable or air).the transmission media does not carry bits; it carries electrical or optical signals. So the bits received a frame from data link layer are transformed and sent through the transmission media. But it is thought that the logical unit between two physical layers in two devices is a bit. There are several protocols that transform a bit to a signal.

1. *Data-Link Layer*

An internet is made up of several links (LANs and WANs). The routers are responsible for choosing the best links. The data link layer is responsible for taking the datagram and moving it across the link.TCP/IP does not define any specific protocol for the data link layer. It supports all the standard and proprietary protocols. Any protocol that can take the datagram and carry it through the link suffice for the network layer. The data link layer takes a datagram and encapsulates it in a packet called a frame. some link layer protocols provide complete error detection and correction, some provides only error correction.

1. *Network Layer*

The network layer is responsible for creating a connection between the source computer and the destination computer that is host to host communication and routing the packets through possible router. The network layer in the Internet includes the main protocol, IP that defines the format of the packet, called a datagram at the network layer. IP is responsible for routing a packet from source to destination, which is achieved by each router forwarding the datagram to next router in its path. IP is a connectionless protocol that provides no flow control, no error control, and no congestion control services. The network layer also include unicast (one to one) and multicast (one to many) routing protocols. A routing protocol does not take part in routing(it is responsible for IP), but it creates forwarding tables for router to help them in the routing process. The network layer also has some auxiliary protocols that helps IP in its delivery and routing tasks. The Internet Control Message Protocol(ICMP) helps IP to report some problems when routing a packet. The Internet Group Management Protocol (IGMP) is another protocol that helps IP in multitasking. The Dynamic Host Configuration Protocol(DHCP) helps IP to get the network layer address for a host.

1. *Transport Layer*

The logical connection at the transport layer is also end to end. The transport layer at the source host gets the message from the application layer encapsulates it in a transport layer packet (called a segment or user datagram) and sends it, through the logical connection, to the transport layer at the destination host. In other words, the transport layer is responsible for giving services to application layer. The main protocol, TCP is a connection oriented protocol that first establishes a logical connection between transport layer at two host before transferring data. It creates a logical pipe between two TCPs for transferring stream of bytes. TCP provides flow control (matching the sending data rate of the source host with the receiving data rate of the destination host to prevent overwhelming the destination ), error control and congestion control to reduce the loss of segments due to congestion in the network. The other common protocol, User Datagram Protocol (UDP) is a connectionless protocol that transmits user datagram without first creating a logical connection.

1. *Application Layer*

The two application layers exchange messages between each other as though there were a bridge between the two layers. Communication at the application layer is between two processes( two programs running at this layer). To communicate, a process sends a request to the other process and receives a response. Process to process communication is the duty of the application layer. The application layer in the Internet includes many predefined protocols, but a user can also create a pair of processes to be run at the two hosts. The Hyper Text Transfer protocol(HTTP) is a vehicle for accessing the World Wide Web(WWW). The Simple Mail Transfer Protocol (SMTP) is the main protocol used in electronic mail (e-mail) service. The File Transfer Protocol (FTP) is used for transferring files from one host to another.

# communication through an internet.

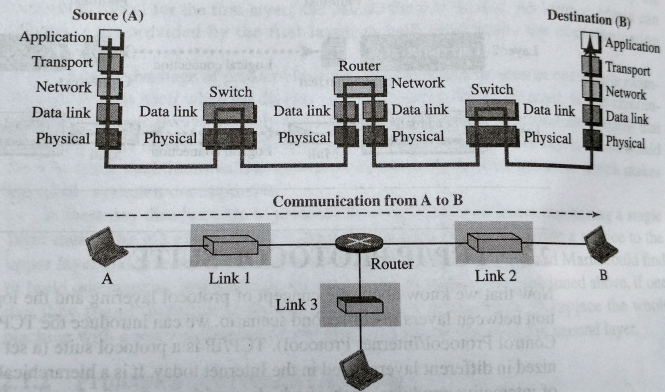


Fig.5 Communication through an internet.

Let us assume that computer A communicates with computer B. As shown in fig. 5 There are five communicating device in this communication: source host (computer A),the link layer switch in link 1,the router, the link layer switch in link 2, and the destination host (computer B). Each device is involved with a set of layers depending on the role of the device on the internet. The two hosts are involved in all five layers; the source host needs to create a message in the application layer and send it down the layers so that it is physically sent to the destination host. The destination host needs to receive the communication at the physical layer and then deliver it through the other layers to the application layer. The router is involved in only three layers; there is mo transport or application layer in a router as long as the router is used only for routing. Although router is always involved in one network layer, it is involved in n-combinations of link and physical layers in which ‘n’ is the number of links the router is connected to. The reason is that each link may use its own data link or physical protocol. Each link may be use in different link layer and physical layer protocols; the router needs to receive a packet from link 1 based on 1 pair of protocols and deliver it to link two based on another pair of protocols. A link layer switch in a link, however, is involved only in two layers, data link and physical. Although each switch in the above figure has two different connections, the connections are in same link which uses only one set of protocols. This means that, unlike a router, a link layer switch is involved only in one data link and one physical layer.

Using Logical connections it makes it easier to understand about the duty of each layer. Logical connections between layers of the TCP/IP protocol suite is as shown in fig.6. In the top three layers, the data unit (packets) should not be changed by any router or link layer switch. In the bottom two layers the packet created by the host is changed only by the routers, not by the link layer switches.

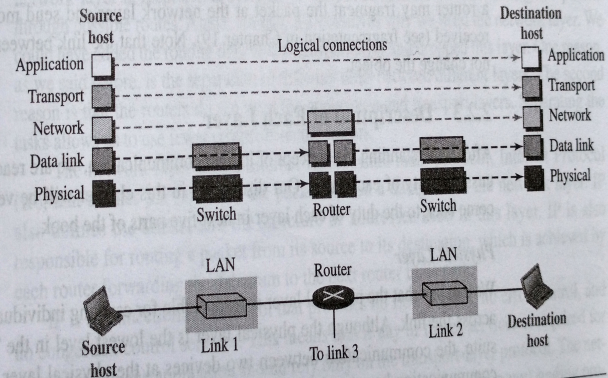


Fig. 6 Logical connections between layers of the TCP/IP protocol suite.

Although the logical connection at the network layer is between the two hosts, the identical objects should exist between two hosts in this case because a router may fragment the packet at the network layer and send more packet than received.

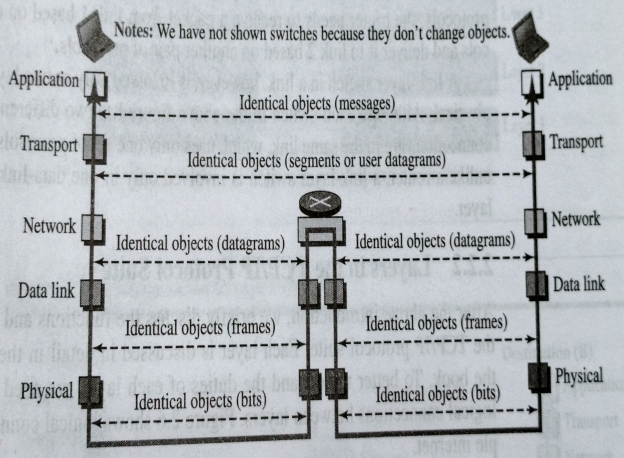


Fig.7 Identical objects in the TCP/IP protocol suite.

# Encapsulation and decapsulation

Encapsulation is done at source host and router where as decapsulation is done at destination host and router. In encapsulation the message is processed in each layer and each layer adds its own header. Where as the reverse process takes place in decapsulation. All headers are removed in order to obtain the original message. The fig.8 shows encapsulation and decapsulation.



Fig. 8 Encapsulation and Decapsulation

# addressing

Any communication that involves two parties needs two addresses : source address and destination address. Here it requires five pair of addresses, one pair per layer, normally only four because the physical layer does not need address; the unit of data exchange at the physical layer is a bit which definitely can not have an address. The fig.9 shows relationship between the layer, the address used in that layer, and the packet name at that layer.

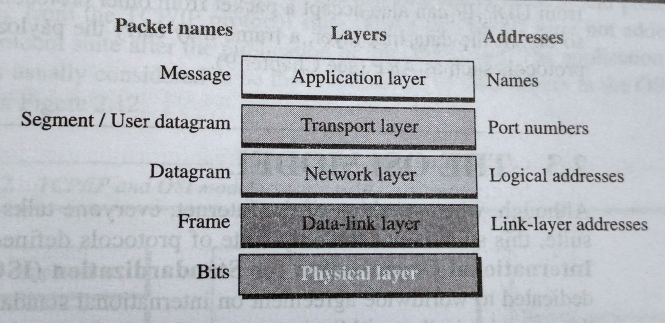


Fig. 9 Addressing in the TCP/IP protocol suite.

# the osi model

The International Organization for Standardization (ISO) standard that cover all aspects of network communications is the Open Systems Interconnection (OSI) model. Its was first introduce in the late 1970’s. An open system is the set of protocols that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes in the logic of the underlying hardware and software. The OSI model was intended to be the basis for the creation of the protocols in the OSI stacks. It consists of seven separate but related layers as shown in fig. 10. In OSI model two extra layer i.e session and presentation, are present which are missing from the TCP/IP protocol suite.

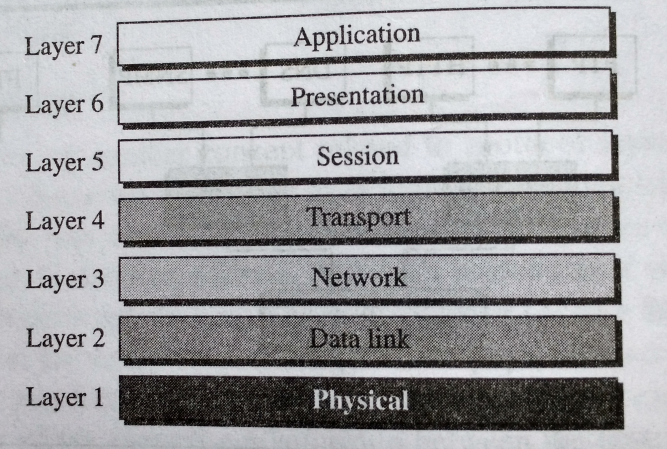


Fig. 10 The OSI Model

TCP/IP model as in fig.11 has more than one transport layer protocol. Some of the functionalities of the session layer are available in some of the transport layer protocol. The application layer is not only one piece of software. Many applications can be develop at this layer. If some of the functionalities mentioned in the session and presentation layers are needed for particular application, they can be included in the development of that piece of software.

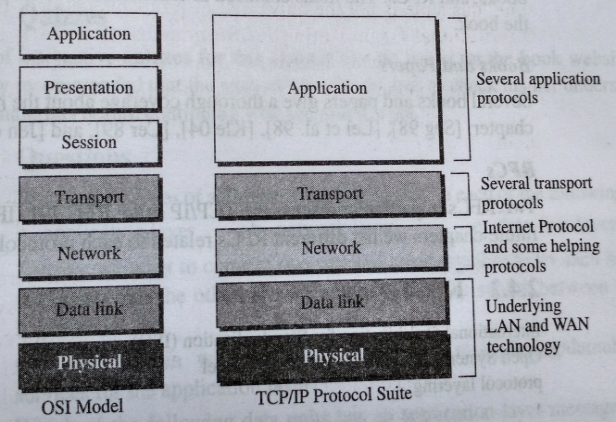


Fig. 11 TCP/IP and OSI Model

# conclusion

The OSI model appeared after the TCP/IP protocol suite. As it was predicted that the TCP/IP protocol suite would be fully replaced by the OSI model. This did not happen for several reasons, some of them are :

1.OSI was completed when TCP/IP was fully in placed a lot of time and money had been spent on the suite; changing it would cost a lot.

2. Some layers in the OSI model were never fully defined.

3. When OSI model was implemented by an organization in a different application, it did not show a high enough level of performance to entice the internet authority to switch from TCP/IP protocol suite to the OSI model.

# Acknowledgment

We would like to thank our Head of Department (Electronics) Dr.P.D.Khandait and Assistant Prof. Mrs.J.S.Gawai for their support and guidance for completing this paper. We are grateful to Assistant Prof. V.V.Chakole for his constant motivation. Also we extend our gratitude to all Authors whose Books and papers are reviewed for completion of this paper.

# 

# References

[1] Behrouz A. Forouzan: Data Communications and Networking, fifth edition ,McGraw Hill Education Private limited. Pg (3 to 31).

[2] Albitz, P. and Liu, C. DNS and BIND, 3rd ed. Sebastopol, CA: O’Reilly,1998.

[3] Buford,J.F.,Yu., and Lua, E.K.P2P Networking and Applications. San Francisco, CA: Morgan Kaufmann,2009.

[4] Forouzan, B. Local Area Networks. New York , McGraw Hill,2003.

[5] Forouzan, B. Cryptography and Network Security. New York , McGraw Hill,2003.

[6] Mao,W.Modern Cryptography. Upper Saddle River, NJ : Prentice Hall,2004.

[7] Hubert Zimmemann, ”OSI Reference model- An ISO model Architecturefor OSI”, in IEEE transaction on communications,Vol.Com-28,No.4.