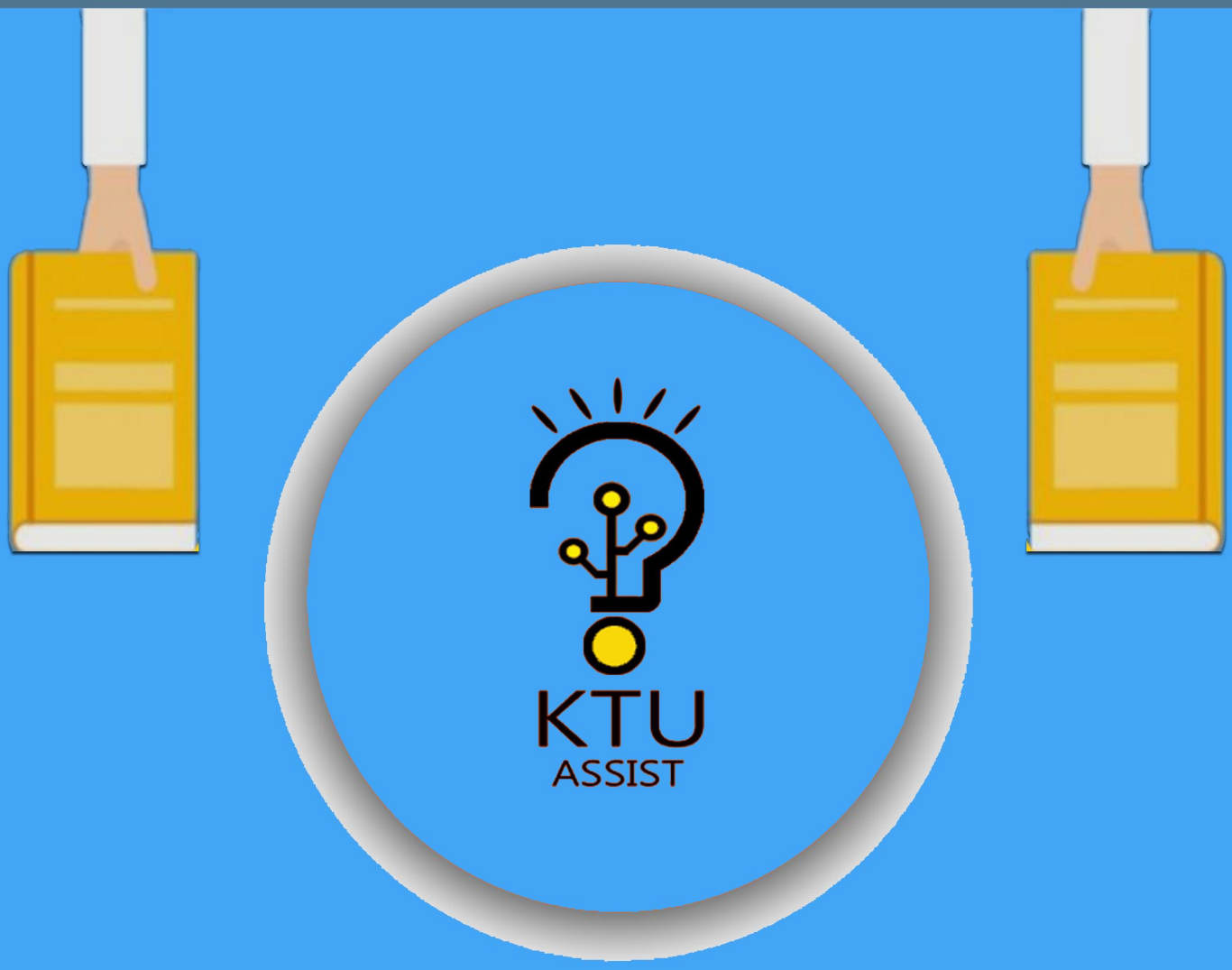
APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

STUDY MATERIALS



(CS306)

COMPUTER NETWORKS

Module	Contents	Hours	Sem. Exam Marks
I	Introduction – Uses – Network Hardware – LAN –MAN – WAN, Internetworks – Network Software – Protocol hierarchies – Design issues for the layers – Interface & Service – Service Primitives. Reference models – OSI – TCP/IP.	7	15
II	Data Link layer Design Issues – Flow Control and ARQ techniques. Data link Protocols – HDLC. DLL in Internet. MAC Sub layer – IEEE 802 FOR LANs & MANs, IEEE 802.3, 802.4, 802.5. Bridges - Switches – High Speed LANs - Gigabit Ethernet. Wireless LANs - 802.11 a/b/g/n, 802.15.PPP	8	15
	FIRST INTERNAL EXAM		
III	Network layer – Routing – Shortest path routing, Flooding, Distance Vector Routing, Link State Routing, RIP, OSPF, Routing for mobile hosts.	7	15
IV	Congestion control algorithms – QoS. Internetworking – Network layer in internet. IPv4 - IP Addressing – Classless and Classfull Addressing. Sub-netting.	7	15
	SECOND INTERNAL EXAM		
V	Internet Control Protocols – ICMP, ARP, RARP, BOOTP. Internet Multicasting – IGMP, Exterior Routing Protocols – BGP. IPv6 – Addressing – Issues, ICMPv6.	7	20
VI	Transport Layer – TCP & UDP. Application layer –FTP, DNS, Electronic mail, MIME, SNMP. Introduction to World Wide Web.	7	20
	END SEMESTER EXAM		

Module 1

Computer Network and Reference Models

COMPUTER NETWORK

Ques 1) What is computer network? What are the main components of computer network?

Or

Give the introduction of computer network.

Ans: Computer Network

A computer network can be defined as the group of interconnected computers which are very useful when users want to share the resources such as printer, database, electronic mail, bulletin boards etc.

Every single station is known as **node**. These nodes may be any peripherals devices, computer terminals and different kinds of communication devices.

Network allows the computers to exchange the data and information via data connection and these data travel in the form of **packets** through various nodes in the network. Computer network can be considered as information highways for data.

Components of Networks

There are various important components in a network. Following are some basic components of a network:

1) **Servers:** These are also called host computers. These are very powerful computers and connect with various resources (shared by the users of a network) and can also store applications and data.

2) **Client:** In a network an individual computer is known as client and can access the servers and shared resources.

3) **Modem:** A modem (modulator-demodulator) is a device used to convert the incoming analog signal into the digital signal and *vice versa*. Basically they are of two types:
   i) **Internal Modem:** These are built inside the computer and cheaper in the cost.
   ii) **External Modem:** These are external devices and cost higher than internal modem.

4) **Routers:** It is a dedicated hardware that forwards data packets between computer networks. Routers may be wireless or wired. To protect from unauthorised access of a wireless router, user needs to set a password to access the router.

5) **Channels:** It is a path over which information travels between client and servers in the network. Channels are also known as network circuit. Channels are the transmission media which are selected on the basis of their speeds and capabilities.

Ques 2) What is topology? Discuss the various topologies.

Or

Discuss the bus, star, ring, mesh and tree topologies with suitable diagram.

Ans: Network Topologies

Network topology is the pattern used to arrange (physically or logically) the nodes or stations of a network.

It also defines the path which is used by pair of stations for communication in a network.

Types of Topology

1) **Physical Topology:** It is the actual geometric configuration of nodes interconnected via cables in a network.
2) **Logical Topology:** Logical topology means how information is passed between two nodes in a network. This topology is bound to the network protocols and defines how data is moved throughout the network.

Basic Network Topologies

Basically there are five types of network topologies:

1) **Bus Topology:** It is the simplest physical network. In this topology all the computers including servers are connected by a single cable with the help of interface connectors.

   The cable is known as **bus** and acts as backbone of the network which joins every computer and peripheral in the network (**figure 1.1**):

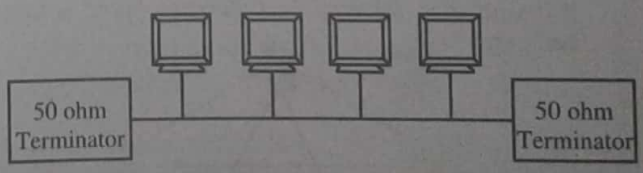


Figure 1.1: Bus Topology

2) **Ring Topology:** In a ring topology all the computers (nodes) are connected in a closed loop. This topology works on the token based system and token travels in the loop. If token is free, then the node can capture the token and attach the data and destination address to the token, and then leaves the token.

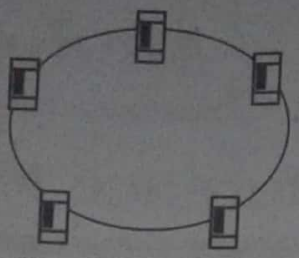


Figure 1.2: Ring Topology

When token reaches at the destination node the data is removed by the destination node and token is free to carry the next data. If another node wants to send the data, it can capture the free token. In this topology each node or computer works as a **repeater**.

The main drawback of ring topology is that if one node fails, then the complete network will go down. The **figure 1.2** shows a ring topology.

3) **Star Topology:** This is a most popular topology to create a network. In this topology nodes are attached with a centrally located device known as **hub** with **UTP** (Unshielded Twisted-Pair) wire. In this topology data are transferred from one node to another node via hub.

In star topology each computer (node) has a distinct connection to the hub, so it is easy to maintain and troubleshoot it. **Figure 1.3** shows the example of star topology.

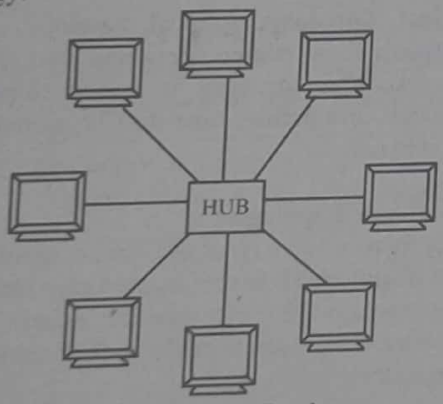


Figure 1.3: Star Topology

4) **Mesh Topology:** In a mesh topology (**figure 1.4**) all the computers are associated with each other via various redundant connections. So there are many paths for data delivery from one computer to another computer.

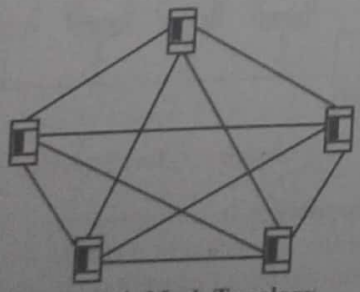


Figure 1.4: Mesh Topology

Mesh topology provides two types of connection management:

i) **Full Mesh Topology:** In this topology, each computer or device is connected to all other computers or devices in a network.

ii) **Partial Mesh Topology:** In this topology, not all but only certain computers or devices are connected to those computers or devices with which they communicate frequently. While, other remaining computers (nodes) are connected to all computers (nodes).

5) **Tree Topology:** In a tree topology (**figure 1.5**) all the computers are connected with each other in hierarchical fashion.

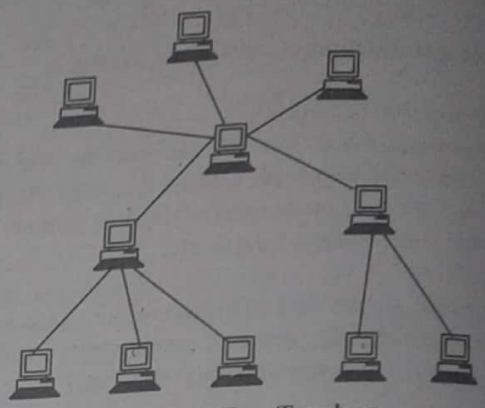


Figure 1.5: Tree Topology

The top most node of the network is known as **root node**. Except the root node, all other nodes have exactly single parent node, while all the nodes in the tree are descendants of the root node.

So, only one path exists for data transmission from one node to other node in the tree topology.

Ques 3) What are the advantages and disadvantages of networks?

Ans: Advantages of Networks

1) **Resource Sharing:** A computer network provides the facility of resource sharing. Resource sharing deals with the sharing of resources (such as printer etc.) among various nodes or client of a computer network.

2) **High Reliability:** It is a property of computer network where network provides substitute source of supply. **For example,** a client can duplicate the files on two or more than two nodes in a network, so if one node fails or is unavailable then client can retrieve the file from another computer.

3) **Saving Money:** Mainframe computers are ten times faster than small computers but they are thousand time costlier than small computers, so to save the cost there are various system designers who created various models in which we can arranged the system to achieve the performance. System designer build systems where one user have one personal computer and data are saved on one or more than one shared file server machines. This model is known as **client-server model** where users are known as **client**.

4) **Scalability:** By adding processors, a computer network increases the system performance when there is more workload. In a mainframe system when this situation occurs, another larger system is replaced by the working system. This takes huge expense and disruption to the user. In a client-server model when needed, new servers and client can be added.

5) **Communication Medium:** Very powerful communication medium can be provided by a computer network between separated clients giving the virtual absence of geographical boundaries.

6) **Increased Productivity:** On computer network two or more process can be handled at the same time. **For example,** one client can handle account receivable and another process can handle the profit and loss statements.

Disadvantages of Networks

1) **Crashes:** The major problem in a server-based network is that when server crashes then no one (client) can access the network resources. Clients lost all benefits available in that network. So for the security reason backups are always taken because crash may result in the loss of days and even in month of time and data.

2) **Data Security:** If proper precautions and security will not be taken then it is possible that an unauthorized employ can access classified information. So, proper implementation of security is necessary.

3) **Privacy:** Privacy is a big issue in network. **For example,** one can (like your boss) read your private mails by changing some privilege setting in the network.

Ques 4) What are the uses of network?

Or

What are the main applications of network?

Ans: Uses of Networks/Applications of Network

Network has added new efficiencies in the work place. They also help business to achieve competitive advantage. Some common applications are as below:

1) **Business Applications:** Many companies have a substantial number of computers. **For example,** a company may have separate computers to monitor production, keep track of inventories, and do the payroll. Initially, each of these computers may have worked in isolation from the others, but at some point, management may have decided to connect them to be able to extract and correlate information about the entire company.

   The aim of networking is to make all programs, equipment, and especially data available to anyone on the network without regard to the physical location of the resource and the user. The next aim is to have a group of office workers share a common printer. None of the individuals really needs a private printer, and a high-volume networked printer is often cheaper, faster, and easier to maintain than a large collection of individual printers.

2) **Home Applications:** The main usage of networks in home is **Internet**. Some of the more popular uses of the Internet for home users are as follows:

   i) **Access to Remote Information:** This can be surfing the World Wide Web for information or just for fun. Many newspapers have gone on-line and can be personalized. The next step beyond newspapers (plus magazines and scientific journals) is the on-line digital library.

      Many professional organizations, such as the ACM (www.acm.org) and the IEEE Computer Society (www.computer.org), already have many journals and conference proceedings on-line.

   ii) **Person-to-Person Communication:** The second broad category of network use is person-to-person communication. E-mail is already used on a daily basis by millions of people all over the world and its use is growing rapidly.

      It already routinely contains audio and video as well as text and pictures. A multi-person chat room is one in which a group of people can type messages for all to see.

   iii) **Interactive Entertainment:** One of the main feature is video on demand. A decade or so hence, it may be possible to select any movie or television program ever made, in any country, and have it displayed on your screen instantly.

   iv) **Electronic Commerce:** The fourth category is electronic commerce. Home shopping is already popular and enables users to inspect the on-line catalogs of thousands of companies. Some of these catalogs will soon provide the ability to get an instant video on any product by just clicking on the product's name.

      Another area in which e-commerce is already happening is access to financial institutions. Many people already pay their bills, manage their bank accounts, and handle their investments electronically.

3) **Mobile Users:** Mobile computers, such as notebook computers and personal digital assistants (PDAs) want to be connected to their office or home even when away from home or en route. Since having a wired connection is impossible in cars and airplanes, there is a lot of interest in wireless networks.

   People on the road often want to use their portable electronic equipment to send and receive telephone calls, faxes, and electronic mail, surf the Web, access remote files, and log on to remote machines and they want to do this from anywhere on land, sea, or air.

   Wireless networks are of great value to fleets of trucks, taxis, delivery vehicles, and repairpersons for keeping in contact with home. Wireless networks are also important to the military.

NETWORK HARDWARE

Ques 5) What are the different types of networks? List them.

Or

What is LAN? What are the advantages and disadvantages of LAN?

Ans: Types of Network

Network can be classified into three major categories:

1) Local Area Network (LAN)
2) Metropolitan Area Network(WAN)
3) Wide Area Network (WAN)

Local Area Network (LAN)

Local Area Network (LAN) is a group of computers that provides reliable high speed communication channels for associated information processing devices in a small geographical area such as campus, offfice building, etc.

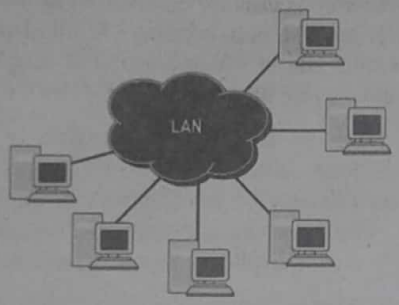


Figure 1..6 LAN Architecture

In a LAN, computers and peripherals are interconnected through a common medium in order that users can access the host computers, application files, etc.

If there are two LANs then one can access both the LANs using a dedicated device known as **gateway** or using a computer which is authorised and connected with both the networks.

LANs are basically used in college, university, industry & business organisations, science & engineering, etc. With the development of LAN users may achieve a paperless office.

IEEE (Institute of Electrical and Electronics Engineers) developed specification for LANs. LANs provide a bandwidth of 1 Mbps to 100 Mbps or even more. Organisations can also extend the area of LAN by using some network devices such as bridges, routers, etc.

Advantages of LAN

1) **File and Program Sharing:** LAN is more beneficial when user wants to share the files and programs. **For example,** if a user wants to use a program which is no longer needed to the user, then user uninstalls the program. After uninstallation, if user again needs the same program, then he/she can install it again. This is a lengthy process. So, to solve this problem LAN facilitates a service in which files or programs can be kept on a central computer or a common location and accessed by other computers or users (also simultaneously) over the network.
2) **Sharing of Expensive Devices:** Sharing of expensive devices (such as laser printers, etc.) is another advantage of LAN because these devices are costly and always need maintenance. So, organisations cannot attach these devices to all the individual computers. Hence, sharing of these devices is must, which can be achieved using LAN technology. **For example,** if a user wants to take a print, he can just give the print command from his computer to the commonly attached printer which might be placed at any different place within the office.
3) **Communication:** LAN can also be used for communication amongst employees. It can work like an office intercom. **For example,** if one wants to share a message with another user, a group of users or all the users within the office, then by using LAN he/she can flash a message on the screen of other computers. This process decreases the need of face-to-face communication among employees and also saves the employees' time.
4) **Easy Backup:** Compared to distributed system, it is easy to take the backup on a central computer.
5) **Resource Management:** Software and resources are managed centrally.

Disadvantages of LAN

1) **Reliability:** If a service interruption (even for a short duration) occurs in LAN, then it will affect the working of many users.
2) **Capacity:** If too many numbers of devices are attached to a single LAN, it could get saturated with increasing time.
3) **Power Backup:** A power backup is necessarily required for continuous working.
4) **Security:** Every node (computer) of the LAN is entry point for outsiders (undesirables).
5) **Covers Limited Area:** It covers only limited geographical area.

Ques 6) What is MAN? What are the advantages and disadvantages of MAN?

Or

What are the main features of MAN?

Ans: Metropolitan Area Network (MAN)

A MAN (Metropolitan Area Network) is larger than LAN and can cover a city and its surrounding areas.

Generally, MANs can be create by interconnecting two LANs. Geographical area cover by MAN is larger than LAN but smaller than WAN (Wide Area Network).

These networks deliver fast and efficient communication by using a high-speed carrier e.g., fiber optic cables.

According to Kenneth C. Laudan and Jane P. Laudan, "A Metropolitan Area Network (MAN) is a large computer network that spans a metropolitan area or campus. Its geographic scope falls between a WAN and LAN. MANs provide internet connectivity for LANs in a metropolitan region, and connect them to wider area networks like the internet". Area of MAN lies between the LAN and MAN and can cover approximately 50km of diameter or sometimes entire city.

MAN is owned by either a group of people or by ngle network provider. This service provider gives the network service to many users.

Features of MAN

1) A MAN may cover 5 to 50 km or more (diameter) in a geographical area. So, it falls between LAN and WAN. It uses may vary from a group of buildings to an entire city.
2) Like a WAN, MAN is not commonly owned and maintained by a single organisation. Either a group of users or a single network provider owns the communication links and equipment of MAN.
3) Like a large LAN, MAN also works as a high-speed network, which allows the sharing of local resources.

Advantages of MAN

1) It provides and manages services to large number of clients.
2) Error rates are moderate.

Disadvantages of MAN

1) It needs huge space to set-up.
2) Its speed of accessing data is less.
3) Equipment used in MAN is expensive.

Ques 7) What is WAN? What are the advantages and disadvantages of WAN?

Ans: Wide Area Network (WAN)

WAN connect devices of a larger geographical area (area which is not served by the LAN and MAN) and uses common carriers like satellite systems, telephone line, etc., to facilitate the transmission.

It works at the physical layer, the data link layer, and the network layer of OSI (Open System Interconnection) model. **Figure 1.7** shows a WAN:

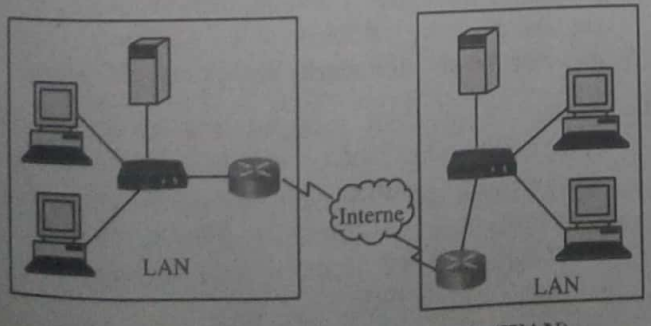


Figure 1.7: Wide Area Network (WAN)

The most useful example of WAN is internet.

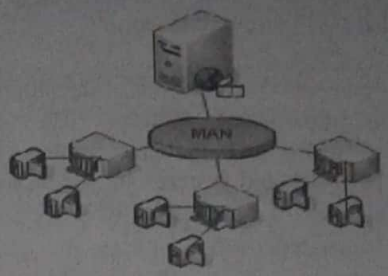


Figure 1.8: Metropolitan Area Network

Advantages of WAN

1) It can be increased without any bound.
2) It is used to share data and resources globally.

Disadvantages of WAN

1) Requirements of large space at the various locations.
2) Data access rate is slower as compared to others (such as LAN and MAN).
3) Equipment used is very expensive.
4) Error rates are high.

Ques 8) What is difference between LAN, MAN and WAN?

Ans: Difference between LAN, MAN and WAN

The difference between LAN, MAN and WAN are shown in **table 1.1:**

Table 1.1: Difference between LAN, MAN and WAN

Basis	LAN	MAN	WAN
Coverage	Diameter of not more than a few kilometres.	Diameter covers a town or a city.	Covers entire countries.
Data Rate	A total data rate of atleast 10 to 100Mbps.	A total data rate is variable.	Data rate more than 1Mbps (Megabits per second).
Ownership	Complete ownership by a single organisation.	Complete ownership is collectively held by few (3-4) organisations.	Owned by multiple organisation.
Error Rate in Data Transmission	Very low error rates.	Low error rate.	Comparatively higher error rates.
Topology used	Symmetrical topology.	Distributed Queue Dual Bus.	Irregular topologies.
Standard	It uses IEEE 802 standard.	It also uses IEEE 802 standard.	It uses ITU standard.

Ques 9) What is internetwork? What are the advantages and disadvantages of internetwork?

Ans: Internetworks

An internetwork is a communication sub-system in which several networks are linked together to provide common

data communication facilities that overlay the technologies and protocols of the individual component networks and the methods used for their interconnection.

Internetworks are needed for the development of extensible, open distributed systems. The openness characteristic of distributed systems implies that the networks used in distributed systems should be extensible to very large number of computers, whereas individual networks have restricted address spaces and some have performance limitations that are incompatible with their large-scale use.

In internetworks, a variety of local and wide area network technologies can be integrated to provide the networking capacity needed by each group of users. Thus, internetworks bring many of the benefits of open systems to the provision of communication in distributed systems.

Advantages of Internetworks

1) **Improved Data Flow:** E-mails can be delivered in matter of minutes anywhere in the world.
2) **Increased Reach:** The Internetworks has brought the world closer.
3) **Improved Availability:** The servers around the world are constantly up and running making information available round the clock.
4) **Access to Knowledge:** The Internetworks can be easily considered as a vast encyclopedia containing the latest information on almost all the subjects under the sound beyond.

Disadvantages of Internetworks

1) **Theft of Personal Details:** While using the Internetworks, there is high probability that personal details like name, address and credit card number may be accessed by cheater and used for fraudulent purposes.
2) **Virus Threat:** Virus is a program that interrupts the usual operation of personal computer system. PCs linked to the Internetworks have high probability of virus attacks and as a result of this hard disk can crash, giving user a lot of trouble.

Ques 10) What are the different network devices?

Or

Explain the following devices:

1) Network Interface Card (NIC):
2) Hub
3) Repeaters
4) Router
5) Modems

Ans: Network Devices

Computers, servers, printers and other devices can exchange data among them using network communication devices. This communication may be between two nearby computers, a computer to a printer or computers across wide-area networks. It is these devices which guarantee that data sent is routed and received by the specific device in the network.

The following are the different network devices:

1) **Network Interface Card (NIC):** Any computer on network requires an add-on card called Network Interface Card (NIC) or Ethernet Adapter or Network Interface Adapter. Its role is movement of serial signals on the network cables or media into parallel data stream.
2) **Hub:** Hubs act as central attachment point for network cables and hence are network connectivity devices which are positioned centrally. These are available for all guided media barring Ethernet cable. Star topology refers to the topology of a network which uses hub.

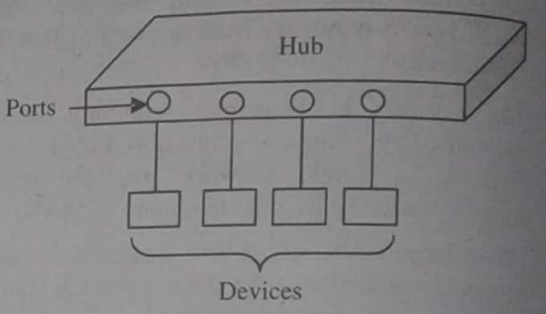


Figure 1.9: A Hub

Hubs can connect multiple communication devices as it has multiple ports. Adding or removing a device is fairly simple in hubs. Any cable break can also be easily detected.

3) **Repeaters:** Repeaters are used to connect the two or more than two similar LAN networks. Over wire it also extends the reach. While two or more networks are connected using same protocol it repeats the signals.

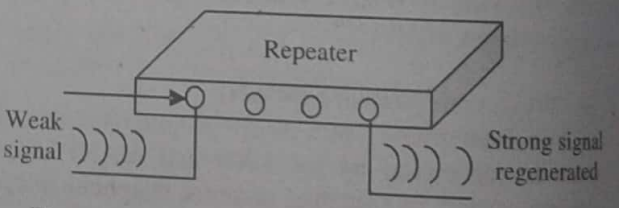


Figure 1.10: Repeater Regenerates a Weak Signal

Incoming signals (electrical, wireless or optical) are regenerated by the repeaters. When data transmission (with physical media such as Ethernet or Wi-Fi) is performed then after a limited distance, quality of the signals degrades. Repeaters are the device which preserve the signal integrity and extend the distance.

4) **Router:** Routers are used to route the data packets along networks and connected minimum two networks. **For example,** consider the following group of networks:
   i) LANs or WAN
   ii) LAN and its ISPs

Routers are used where gateways are placed. Routers read the address information from the packet to identify the destination of the packet. In the next step, they compare the information from their routing table (or routing policy) and send the information (packets) in another network. On the Web (Internet) routers are used to transfer the traffic direction. Home and small office routers are the simplest form of routers. These routers pass webpages, emails, videos, etc. kind of data from the home computer to the Internet.

5) **Modems:** Modems are used for connecting the computer to the internet using telephone line by dialing ISP and also connecting to DSL. It uses modulation and de-modulation techniques to convert analog signal to digital and *vice-versa* to ensure that signals travel on telephone lines.

NETWORK SOFTWARE

Ques 11) What is protocol? What are the different elements of protocols?

Ans: Protocols

A network protocol is a set of rules and standards which must be followed by network devices for proper communication among them. Most commonly used network protocols are Transmission Control Protocol, Internet Protocol, File Transfer Protocol etc.

Network protocols consist of rules related to mechanisms for device identification, connection between devices, format and packaging of transmitted data etc. These protocols may also include rules regarding message acknowledgement, data encryption and data compression to support secure, reliable and high performance network communication. There are various such protocols which are designed to fulfil specific requirements and are suitable for specific type of network.

The Internet Protocol is one of the most widely used network protocols. It supports various types of inter-network transmission utilising higher level protocols like HTTP, TCP, UDP, FTP etc. These high level protocols interact with applications like web browser, FTP client, messaging applications etc. Internet Protocol also supports some lower level inter-network protocols like ARP and ICMP. These lower level protocols interact with switches, network adapters, modems etc.

Elements of a Protocol

The key elements of a protocol are as follows:

1) **Syntax:** Syntax concerns the format or structure of the data blocks. It refers the order in which they are presented. **For example,** a simple protocol may expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of receiver, and the rest of the stream to be the message itself.
2) **Semantics:** It refers to the meaning of each section of data bits. How are a specified pattern to be interpreted; and what action is to be taken based on that interpretation? **For example,** does an address identify the route to be taken or the final destination of the message?
3) **Timing:** Timing refers to two characteristics:
   i) When data should be sent.
   ii) How fast they can be sent.

   For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and data will be largely lost.

Ques 12) Describe protocol hierarchy.

Ans: Protocol Hierarchy

To reduce the design complexity of computer communications hardware and software, the needed functionality is organized as a series of layers, each built on its predecessor.

Network software is arranged in a hierarchy of layers. Each layer presents an interface to the layers above it that extends the properties of the underlying communication system. A layer is represented by a module in every computer connected to the network.

Several tools have been developed to help protocol designers understand subparts of the communication problem and plan an entire protocol suite. One of the most important tools is called **layering model**. Layering model provide a simple explanation of the relationships among the complex hardware and protocol components of a network. In all networks, the purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the provided services are actually implemented.

Layer n in one machine carries on a conversation with layer n on another machine, the rules and conventions used in this conversation are collectively known as layer n "protocol". Protocol is an agreement between the communication parties on how communication is to proceed. A five layer network is illustrated in **figure 1.11**:

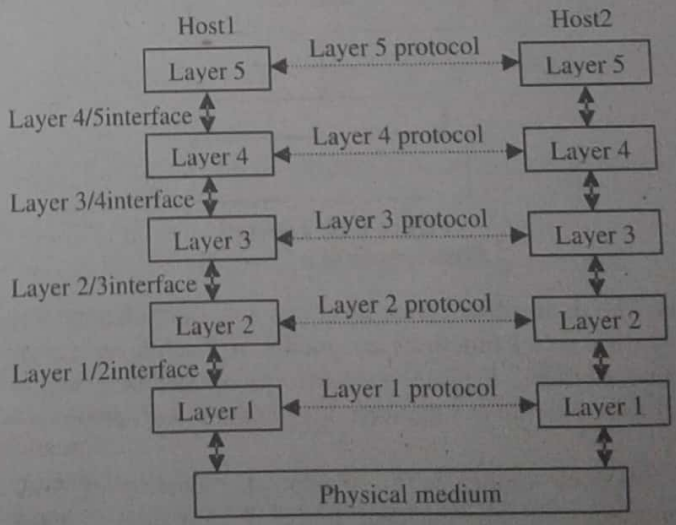


Figure 1.11: Layers Protocols and Interfaces

The entities comprising the corresponding layers on different machines are called "peers". In other word it is the **peers** that communicate using the protocol. In reality, no data are transferred directly from layer n on one machine to layer n on another machine. Instead, each layer passes data and control information to the layer below it, until the lowest layer is reached. Below layer 1 is the "physical medium" through which the actual communication occurs.

In **figure 1.11** virtual communication is shown by dotted lines (refers to layer protocol) and physical communication by solid line (refer to layer interface).

Between each pair of adjacent layers there is an "interface", the interface defines which operations and services that the lower layer offers to upper layer through it. A list of protocols used by certain system one protocol per layer is called a "protocol stack".

Ques 13) Explain the layered architecture of computer network. Also discuss the design issues for the layers.

Ans: Layered Architecture of Computer Network
Decomposition of the organization into offices and each office into hierarchical functional levels and the interaction procedures define the overall organization architecture.

A computer network is also partitioned into end systems interconnected using a sub network and the communication process is decomposed into hierarchical functional layers (**figure 1.12**).

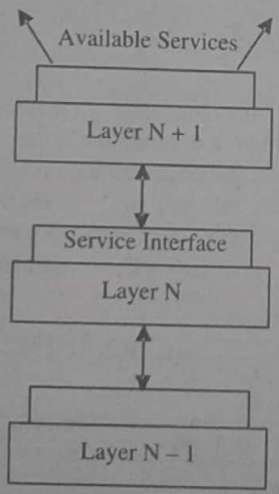


Figure 1.12: Layered Architecture of a Computer

Just like in an office, each layer has a distinct identity and a specific set of functions assigned to it. Each layer has an active element, a piece of hardware or software, which carries out the layer functions. It is called **layer entity**.

A reference model is a conceptual blueprint of how communication should take place. It addresses all the processes required for effective communication and divides these processes into logical groupings called **layers**. When a communication system is designed in this manner, it is known as **layered architecture**.

Design Issues of the Layers
Design issues can be discussed under the following topics:

1) **Addressing:** Each layer needs a mechanism for the source and the destination machine. There should be two addresses:
   i) Destination Address
   ii) Source Address.
2) **Mode of Communication:** The designing of the layer should have to keep the mode of transmission in mind. The protocol used for congestion control or media access should be considered under the mode of transmission.
3) **Error Control:** Two types of error control:
   i) Error detecting code.
   ii) Error correcting code.
4) **Sequencing:** Order of the Packets/Frames must be ensured by implement sequence number in their frames. Sequence number is needed for error control and detection.
5) **Flow Control:** How to keep fast sender from swapping a slow receive with data Agreement upon transmission rate.
6) **Packet Size:** A standard packet size is to be specified to make transmission compatible. Each strategy or mode (standard) have their own standard e.g., frame size and this is strictly followed.
7) **Multiplexing:** Multiplexing is used in the physical layer. Multiplexing is needed when a single media or wire is used by more than one user.
8) **Laws:** The communication/transmission can be of two types (on the basis of law and authority):
   i) Leased Line-Dynamic routing strategy.
   ii) Dedicated Line-Static routing strategy.
9) **Routing Strategy:** Routing of the packet form source to destinations to be specified by the frame itself as there are two type of routing:
   i) **Static Routing:** In this strategy routes are predefined. A virtual circuit is established before sending frames and the frame contains **Virtual Circuit Number (VCN)** in its frame.
   ii) **Dynamic Routing (Datagram):** Which route to choose and which not are based on some algorithm. In this strategy each packet can take its own course to reach the destination.

Ques 14) What are the advantages of layering?

Ans: Advantages of Layering
1) It divides the network communication process into smaller and simpler components, thus aiding component development, design, and troubleshooting.
2) It allows multiple-vendor development through standardization of network components.

3) It encourages industry standardization by defining what functions occur at each layer of the model.
4) It allows various types of network hardware and software to communicate.
5) It prevents changes in one layer from affecting other layers, so it does not hamper development.

Ques 15) Write short note on interfaces and services.
Or
What are the different types of services?

Ans: Interfaces and Services
The process provides a common technique for the layer to communicate with each other. The standard terminology used for layered networks to request services is provided.

In **figure 1.13** the layers (N + 1), N and (N – 1) are involved in the communication process for layer communication, with each other.

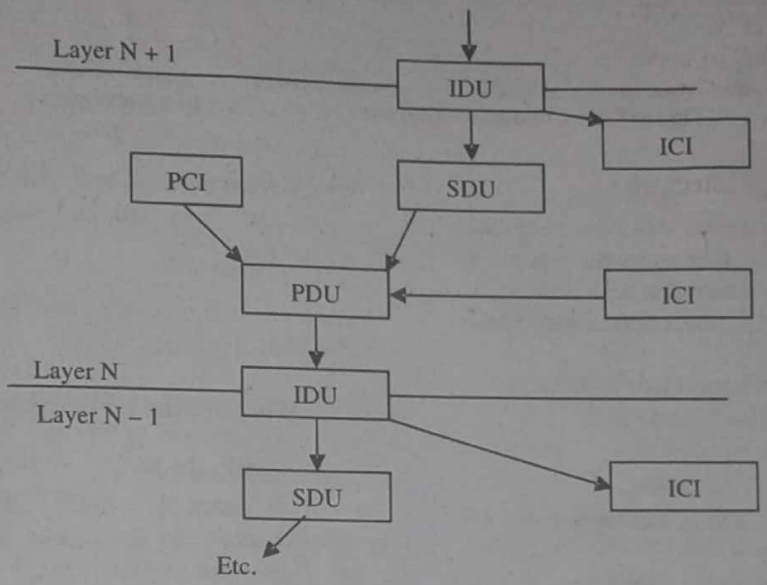


Figure 1.13: Communication between Layers

Following components are involved and their function is as follows:
1) **SDU:** Transfer user data by layer (N + 1) to layer N and (N – 1).
2) **PCI:** To perform service function, it is used to exchange information by peer entities at different sites on the network.
3) **PDU:** Combination of the SDU and PCI.
4) **ICI:** It passes temporary parameter between N and N – 1 to invoke service function.
5) **IDU:** The total unit of information transferred across the layer boundaries.

When the IDU from layer N + 1 passes to layer N, it becomes the SDU to that layer. PCI is added to SDU at layer N. ICI performs its function and is discarded.

Another ICI is added to PDU at layer N and it becomes IDU to layer N – 1. Thus a full protocol unit is passed through each layer.

Each layer adds header to data. This header is used by the peer layer entity at another node of the network to invoke function. This process repeats itself through each layer.

As each unit traverses through the layer, it has a header added to it, i.e., user data and header (SDU and PCI). This full protocol data unit is passed onto the communication path, where it arrives at the receiving site.

In short, each layer added its header to user's data and passes to its next layer. This layer process on that data and adds its own header and provides to next layer for processing. Through transmission channel data passes to receiving site.

Figure 1.14 shows the communication between two sites in a network.

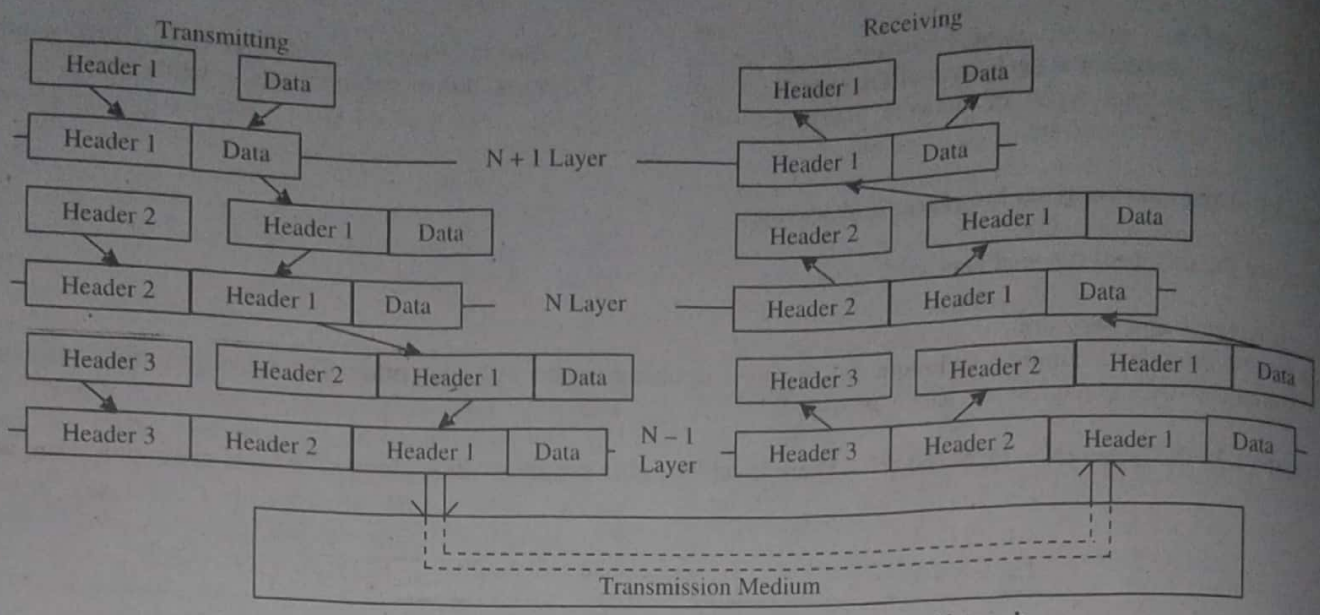


Figure 1.14: Communication between two Sites in a Network

Types of Services

The two primary types of services which are made available by a particular network layer and which actually are also useful classifications for many non-technical types of service industries are known as connection-oriented and connectionless communication:

1) **Connection-Oriented Services:** Given valid input parameters, the service:
   i) Establishes the connection,
   ii) Allows me to utilize the connection,
   iii) Tears down the connection when I am done using it.

   The primary difference between this method and that of a connectionless service is that in a connection-oriented system, all of my communications are taking place on the same transmission channel. On the other hand, with a connectionless service, all transmissions are independently routed, and perhaps re-assembled in some order at the other end – the service in between has no inherent responsibility for ensuring ordinality – it need only assure that each transmission gets delivered from its source to its destination.

2) **Connectionless Services:** A good analogy for a connectionless service is the process of sending letters through the postal system. Each transmission (the "letter") contains the full destination address and is processed independent of related messages. As described above, the service has only to ensure that each reaches its host within certain time parameters. Unlike a connection-oriented service, the system has free reign on what happens enroute between the sender and receiver:
   i) A message can be delayed to ensure another arrives first.
   ii) Widely different channels of communication can be used for transmitting messages.
   iii) A message can be handed-off to a trusted third party in the distribution network.
   iv) A message can be intercepted by a third party, copied or logged, and passed on to the intended receiver.

   These operations are basically impossible for a connection-oriented service.

Ques 16) What are the service primitives?

Ans: Service Primitive

A service is formally specified by a set of primitives (operations) available to a user process to access the service. These primitives tell the service to perform some action or report on an action taken by a peer entity. If the protocol stack is located in the operating system, as it often is, the primitives are normally system calls. These calls cause a trap to kernel mode, which then turns control of the machine over the operating system to send the necessary packets.

The set of primitives available depends on the nature of the service being provided. The primitives for connection-oriented service are different from those of connectionless service. Five service primitive are shown in **table below**:

Table 1.2: Five Service Primitives for Implementing a Simple Connection Oriented Service

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

NETWORK REFERENCE MODELS

Ques 17) What do you understand by Network Reference Model? List out the types of network reference model.

Ans: Network Reference Model

A communication subsystem is a complex piece of hardware and software. Early attempts at implementing the software for such subsystems were often based on a single, complex, unstructured program (normally written in assembly language) with many interacting components. The resulting software was difficult to test and often very difficult to modify.

To overcome this problem, the ISO has adopted a layered approach for the **reference model**. The complete communication subsystem is broken down into a number of layers each of which performs a well-defined function.

Conceptually, these layers can be considered as performing one of two generic functions; network-dependent functions and application-oriented functions. This in turn gives rise to three distinct **operational environments**:

1) **Network Environment:** The network environment, which is concerned with the protocols and standards relating to the different types of underlying data communication networks.

2) **OSI Environment:** The OSI environment, which embraces the network environment and adds additional application-oriented protocols and standards to allow end systems (computers) to communicate with one another in an open way.

3) **Real Systems Environment:** The real systems environment, which builds on the OSI environment and is concerned with a manufacturer's own proprietary software and services which have been developed to perform a particular distributed information processing task.

This is shown in diagrammatic form in **figure 1.15**

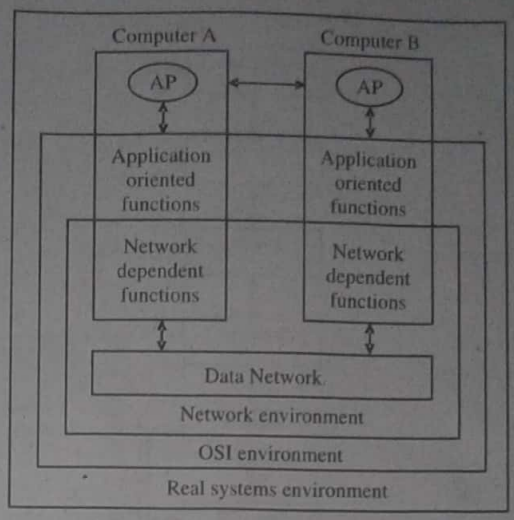


Figure 1.15: Operational Environments

Both the network-dependent and application-oriented (network-independent) components of the OSI model are implemented as a number of layers. The boundaries between each layer and the functions performed by each layer have been selected on the basis of experience gained during earlier standardization activity.

Each layer performs a well-defined function in the context of the overall communication subsystem. It operates according to a defined protocol by exchanging messages, both user data and additional control information, with a corresponding peer layer in a remote system. Each layer has a well-defined interface between itself and the layer immediately above and below.

Consequently, the implementation of a particular protocol layer is independent of all other layers.

Types of Reference Models

The two important network models are as follows:

1) OSI Reference Model
2) TCP/IP Reference Model

Ques 18) What is OSI model? What are the different layers of OSI model?

Or

What are the functions of different layers of OSI reference model?

Ans: OSI Reference Model

A networking reference model defined by the ISO (International Organization for Standardization) divides computer-to-computer communications into **seven connected layers**.

Such layers are known as a **protocol stack**. Each successively higher layer builds on the functions of the layers below.

Open Systems Interconnection (OSI) is a reference model that determines the way in which messages should be transmitted between any two points in a network.

In OSI model, two end points in a network are divided into layers. The data flow through each layer at one end down through the layers and, at the other end, when the message arrives, data flow up through the layers in the receiving end point and ultimately to the end user or program.

The OSI reference model is shown in **figure 1.16.**

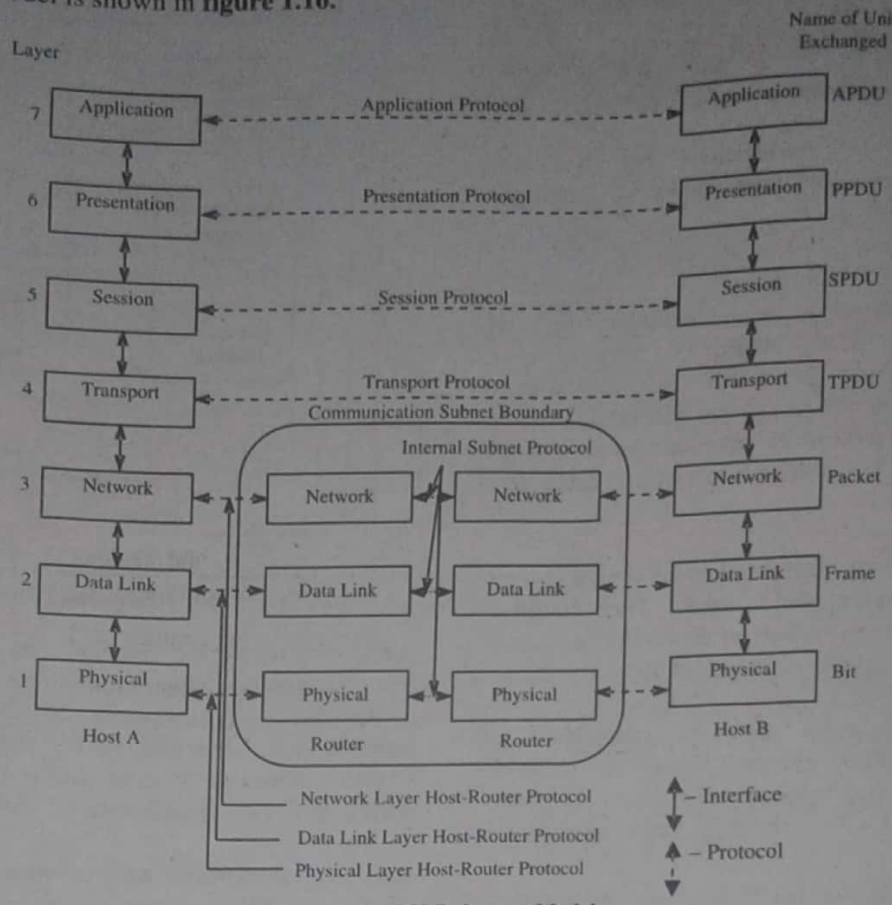


Figure 1.16: OSI Reference Model

Where

APDU-Application Protocol Data Unit
PPDU-Presentation Protocol Data Unit
SPDU-Session Protocol Data Unit
TPDU-Transport Protocol Data Unit

The different layers of the OSI reference are as below:

1) **Application Layer:** The application layer serves as a window for users and application processes to access network services. It handles issues such as network transparency, resource allocation etc. This layer is not an application in itself, although some applications may perform application layer functions. This layer provides network services to the end-users. **Examples** of network applications are Mail, FTP, Telnet, DNS, NIS, NFS.

Functions of Application Layer

i) **Authentication:** Authenticates the sender or receiver of the message or both.

ii) **File Access, Transfer and Management:** Allows the user at a remote site to access files on another host.

iii) **Directory Services:** Provides access to global information and database sources.

2) **Presentation Layer:** The presentation layer serves as the data translator for a network. It is usually a part of an operating system and converts incoming and outgoing data from one presentation format to another. This layer is also known as **syntax layer**.

Functions of Presentation Layer

i) **Data Compression:** Provides efficiency while transmitting data. It refers to a process of encoding data using less number of bits.

ii) **Encryptions:** Ensures security by using different algorithms for coding, passwords and log-in-codes.

3) **Session Layer:** The session layer establishes a communication session between processes running on different communication entities in a network and can support a message-mode data transfer. It deals with session and connection coordination.

Functions of Session Layer

i) **Session Management:** Divides the sessions into sub-sessions by inserting checkpoints.

ii) **Synchronization:** Selects the order in which the dialog units must pass to the transport layer. It also gets confirmation from the receiver machine.

iii) **Dialog Control:** Controls which user will send data and at what time.

iv) **Closing the Session:** Ensures that the data transfer is completed before the session closes.

4) **Transport Layer:** The transport layer ensures that messages are delivered in the order in which they are sent and that there is no loss or duplication. It ensures complete data transfer. Transport layer subdivides user-buffer into network-buffer sized datagrams and enforces desired transmission control. Two transport protocols, **Transmission Control Protocol (TCP)** and **User Datagram Protocol (UDP)**, sits at the transport layer.

Functions of Transport Layer

i) **Service-Point Addressing:** Transport layer includes service-point address (also referred to as port address) in the header. Using these port addresses, transport layer delivers the packets to the correct process.

ii) **End-to-End Message Delivery:** Ensures that the entire message is transmitted to the destination.

iii) **Segmentation and Reassembly:** Divides each message into segments and assigns a sequence number to these segments. This helps to reassemble the message if some error occurs during message transmission.

iv) **Connection Control:** Decides whether all the packets will be sent using a single path or not.

5) **Network Layer:** It determines the physical path that data takes on the basis of network conditions, priority of service, and other factors. The network layer is responsible routing and forwarding data packets.

Functions of Network Layer

i) **Source-to-Destination Delivery:** Transfers packets from the source to its destination.

ii) **Logical Addressing:** Adds the source and destination addresses in the header.

iii) **Routing:** Selects the optimal path out of the multiple paths so that a packet can follow.

iv) **Address Transformation:** Interprets the logical address.

v) **Multiplexing:** Utilizes one physical line for transferring data between several devices at a time.

6) **Data-Link Layer:** The data-link layer is responsible for error free transfer of data frames. This layer provides synchronization for the physical level. Data Link layer defines the format of data on the network.

Data Link Layer: Sub-Layers

The IEEE Ethernet Data Link Layer works with two sub-layers:

i) **Logical Link Control (LLC) 802.2:** The LLC 802.2 is responsible for diverting the packets to the Network layer of the host that is receiving. It identifies the address of the Network layer protocol from the header. It is also responsible for providing flow control and arranging the control bits in a series.

ii) **Media Access Control (MAC) 802.3:** MAC is a link between the LLC and the network's physical layer. It is responsible for transferring the packets over the networks.

Functions of Data-Link Layer

i) **Framing:** The main problem is to decide where successive packets start and end. Therefore, the DLL encapsulates the packet into a frame by adding its own header and trailer.

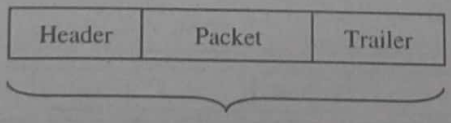


Figure 1.17: From Packet to

ii) **Arbitration:** Arbitration simply means determining how to negotiate access to a single data channel when multiple hosts are attempting to use it at the same time.

iii) **Physical Addressing:** Physical addressing is different from network addressing. Network addresses differentiate between nodes or devices in a network, allowing traffic to be routed or switched through the network. Primary form of physical addressing is the media access control (MAC) address.

iv) **Error Detection:** Error detection is the process of detecting whether errors occurred during the transmission of the bits across the wire. The Data Link layer uses a calculated value called the CRC (Cyclic Redundancy Check) that's placed into the Data Link trailer that's added to the message frame before it's sent to the Physical layer.

v) **Encapsulation:** DLL identifies encapsulated data. Encapsulation is a method of designing modular communication protocols in which logically separate functions in the network are **abstracted** from their underlying structures by inclusion or information hiding within higher level objects.

7) **Physical Layer:** Physical layer defines the cable or physical medium itself, e.g., thinnet, thicknet, Unshielded Twisted Pairs (UTP). All media are functionally equivalent. The main difference is in convenience and cost of installation and maintenance. Converters from one media to another operate at this level. The physical layer is responsible for packaging and transmitting data on the physical media. This layer conveys the bit stream through the network at the electrical and mechanical level.

Functions of Physical Layer

i) **Line Configuration:** Defines the way in which two or more devices can be connected physically.

ii) **Data Transmission:** Defines the transmission mode between the two devices on the network.

iii) **Topology:** Determines the way in which the network devices are arranged.

iv) **Signals:** Determines the type of signal that is used for transmitting information.

Ques 19) What is TCI/IP reference model? What are the different layers of TCI/IP reference model?

Ans: TCP/IP Reference Model

As the number of networks that were connected to the ARPAnet increased, communication among the computers became a problem. Common standards were required for communication because the hardware and the software that were used were vendor-specific. A common protocol was necessary for communication between the computers. This led to the creation of TCP and IP. With the increase in the number of requirements, several protocols were created to address all the requirements. This also led to the creation of a new reference model, called the **TCP/IP reference model**. The TCP/IP consists of four layers – Application, Transport, Internet, and Network Interface, as shown in **figure 1.18**.

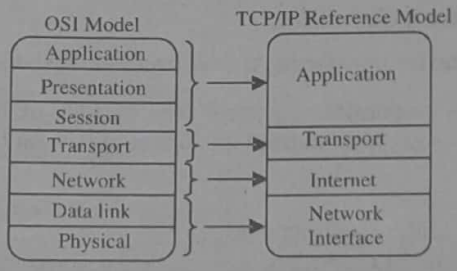


Figure 1.18 TCP/IP Reference Model is a Standard Reference Model for Communication in the Internet

All protocols that belong to the TCP/IP protocol suite are located in the top three layers of the model. The TCP/IP reference model is based on a suite of protocols in which each protocol solves a particular network communications problem. The TCP/IP model can be used in a heterogeneous environment that has equipment from many different vendors. As shown in **figure 1.19** layer of TCP/IP Model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) reference model proposed by the International Standards Organization (ISO).

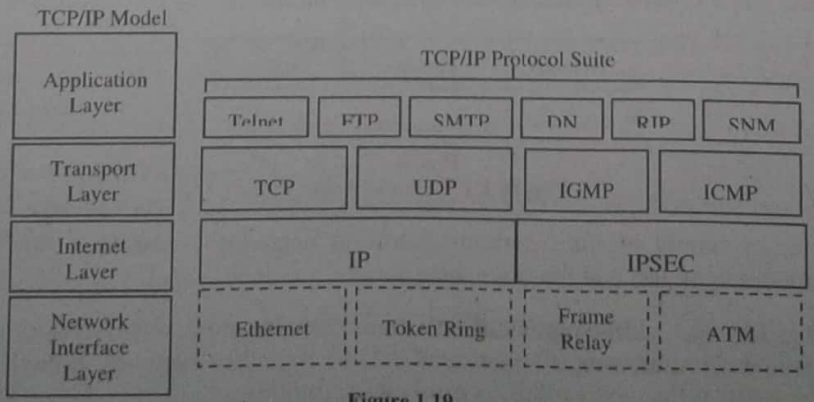


Figure 1.19

The different layers of TCP/IP models are given below:

1) **Network Access Layer:** The network access layer is responsible for exchanging data between a host and the network and for delivering data between two devices on the same network. Node physical addresses are used to accomplish delivery on the local network.

   Functions performed at this level include encapsulation of IP datagram (i.e. the packet format defined by Internet Protocol.) into the frames transmitted by the network, and the mapping of IP addresses into the physical addresses used by the network.

   TCP/IP network access layer can encompass the function of all three lower layers of the OSI reference model (Network Layer, Data Link Layer, and Physical Layer.)

2) **Internet Layer:** The internet layer is responsible for sending source packets from any network on the internetwork and has them arrive at their destination regardless of the path they took.

   Internet Protocol (IP) is used in this layer and it provides the packet delivery service on which the TCP/IP is based. IP protocol implements a system of logical host addresses called IP addresses. The IP addresses are used by the internet and higher layers to identify devices and to perform internetwork routing.

3) **Transport Layer:** The transport layer is responsible for the reliability, flow control, and error correction of data being sent across the network. Its main protocol is called the transmission control protocol (TCP). TCP provides reliable data delivery service with end-to-end error detection and correction.

   User Datagram Protocol (UDP) is another protocol used which provides slow-overhead, connectionless datagram delivery service. UDP is unreliable but enhances network throughput when error correction is not required at the host-to-host-layer. Both protocols deliver data between the Application Layer and the Internet Layer.

4) **Application Layer:** The application layer is responsible for handling high-level protocols, issues of representation, encoding and dialog control. This layer is broadly equivalent to the application, presentation and session layers of the OSI model. It gives an application access to the communication environment.

   Examples of protocols found at this layer are Telnet, FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol), HTTP (Hyper Text Transfer Protocol) and SMTP (Simple Mail Transfer Protocol).

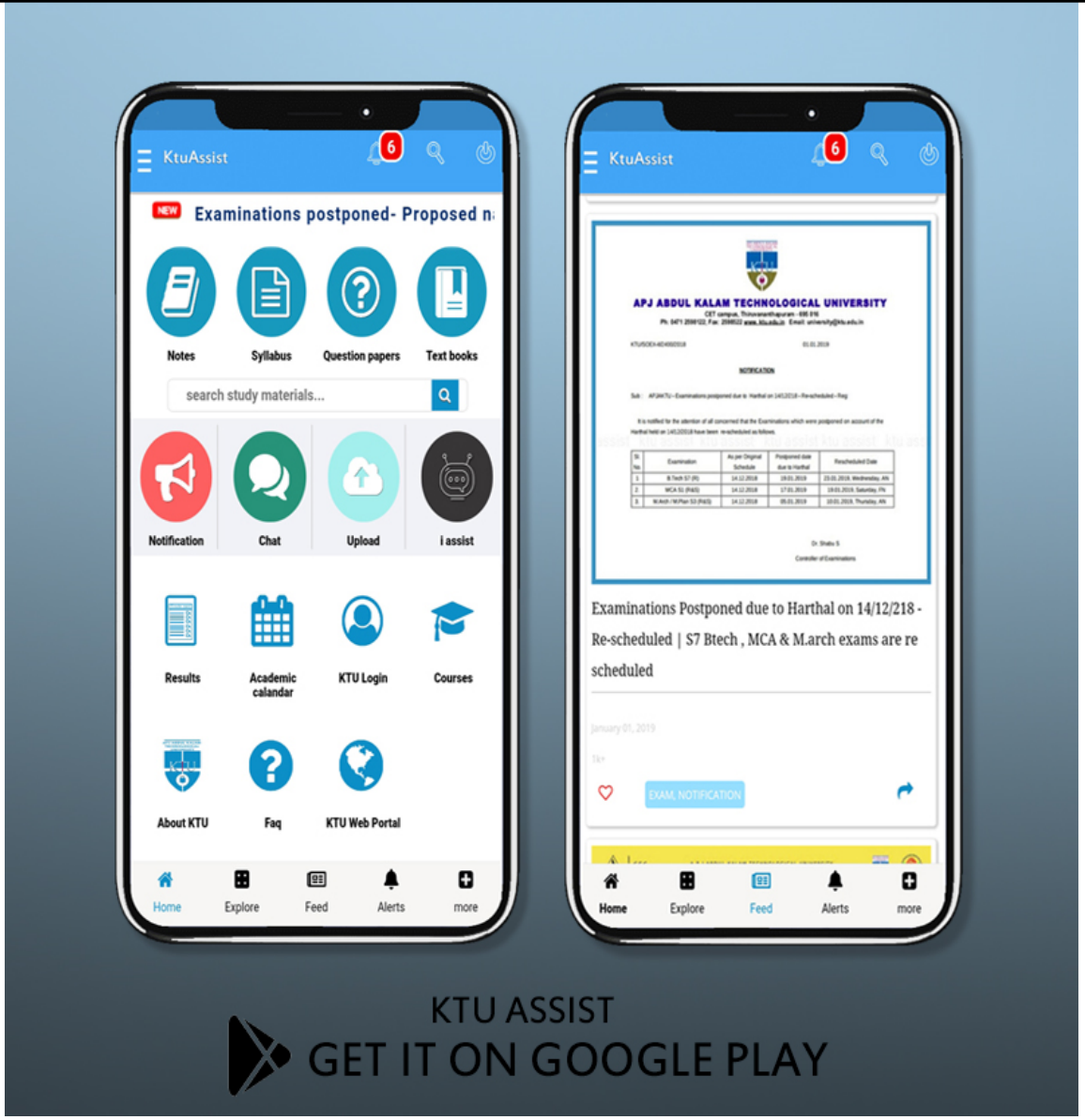
Ques 20) What is difference between OSI and TCP/IP reference model?

Ans: Comparison between OSI and TCP/IP Reference Models

The difference between OSI and TCP/IP is shown in **table 1.3**:

Table 1.3: OSI *vs.* TCP/IP

Basis	OSI	TCP/IP
No. of Layers	7 Layers	4 Layers
Implementation	Model was first defined before implementation takes place.	Model defined after, protocol was implemented.
Model Concepts	OSI model based on three concepts, i.e., service, interface and protocol.	TCP/IP model did not originally clearly distinguish between service, interface and protocol.
Delivery of Packets	OSI model gives guarantee of reliable delivery of packet.	Transport layer does not always guarantee the reliable delivery of packet.
Internet Working	OSI does not support internet working.	TCP/IP support internet working.
Layering	Strict layering	Loose layering
Connection Type	Support connectionless and connection-oriented communication in the network layer.	Support only connection-oriented communication in the transport layer.



END

facebook.com/ktuassist

instagram.com/ktu_assist