UNIT 1 NETWORK CLASSIFICATION AND REFERENCE MODELS

Structure **Page Nos.**

1.0 INTRODUCTION

Earlier computers used to be standalone. Different computers were used for information gathering, processing or distributing. Due to rapid technological progress the areas of information gathering, processing or distributing are rapidly converging and differences between them are quickly disappearing. In this unit we will learn about the different types of networks, their applications, networking models and topologies. We will also examine reference models, its various layers and functions of each layer.

1.1 OBJECTIVES

After going through this unit you should be able to:

- define and classify network;
- distinguish between different types of networks, and
- understand what is OSI model and TCP reference model and functions of each layer.

1.2 WHAT IS A NETWORK?

In the simplest form, data transfer can take place between two devices which are directly connected by some form of communication medium. But it is not practical for two devices to be directly point to point connected. This is due to the following reasons:

(i) The devices are very far apart.

(ii) There is a set of devices, each of whom may require to connect to others at various times.

Solution to this problem is to connect each device to a communication network. Computer Networks means interconnected set of autonomous systems that permit distributed processing of information.

In order to meet the needs of various applications, networks are available with different interconnection layouts and plans, methods of access, protocols and DATA carrying capacities. Networks can be classified on the basis of geographical coverage.

1.2.1 Classification of Networks

- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN).

1.2.2 Local Area Network (LAN)

A local area network is relatively smaller and privately owned network with the maximum span of 10 km. to provide local connectivity within a building or small geographical area. The LANs are distinguished from other kinds of networks by three characteristics:

(i) Size
(ii) Transmission technology, and
(iii) Topology.

Accordingly, there are many LAN standards such as IEEE standards 802 x.

1.2.3 Metropolitan Area Network (MAN*)*

Metropolitan Area Network is defined for less than 50 km. and provides regional connectivity typically within small geographical area. It is designed to extend over an entire city. It may be a single network such as cable television, network, or it may be a means of connecting a number of LANs into a large network, so that resources may be shared LAN to LAN as well as device to device. For example, a company can use a MAN to connect to the LANs in all of its offices throughout a city.

1.2.4 Wide Area Network (WAN)

Wide Area Network provides no limit of distance. In most WANs, the subnet consists of two distinct components. Transmission lines also called circuits or channels or links and switching and routing devices (switches & routers). Transmission-lines are used for moving bits between machines, whereas routers are used to connect two or more transmission lines.

A WAN provides long distance transmission of data, voice, image and video information over large geographical areas that may comprise a country, a continent or even the whole world.

In contrast to LANs (which depend on their own hardware for transmission), WANs may utilise public, leased or private communication devices usually in combination and span own unlimited number of miles.

A WAN that is wholly owned by a single company is often referred to as an enterprise network.

1.3 COMPUTER NETWORK GOALS/ MOTIVATION

The main goal of a computer network is to enable its users to share resources and to access these resources (i.e. hard disks, high quality expensive laser printer, modems, peripheral devices, licensed software, etc.), regardless of their physical locations. Physical locations may be a few feet or even thousands of miles apart, but users exchange data and programs in the same way. In other words, distance is removed as barrier for the above application. The computer network thus creates a global environment for its users and computers. Other goal is to provide communication services (such as E-mail) and in general to provide robust transport network. i.e., (highway) over which network applications can be built.

1.4 APPLICATIONS OF NETWORKS

The following is the list of some application of computer network.

Generic application

- Resource sharing (CPU, peripherals, information and software)
- Personal communication (text + graphics + audio + video + data)
- Network-wide information discovery and retrieval.

Some Specific end applications

- Campus-wide computing and resources sharing
- Collaborative research and development
- Integrated system for design + manufacturing + inventory
- Electronic commerce, publishing and digital libraries
- Multi-media communication (tele-training, etc.)
- Health-care delivery (remote diagnosis, telemedicine)
- Video-on-demand.

We are now moving from personalised computing to network computing. Therefore, its application are increasing everyday.

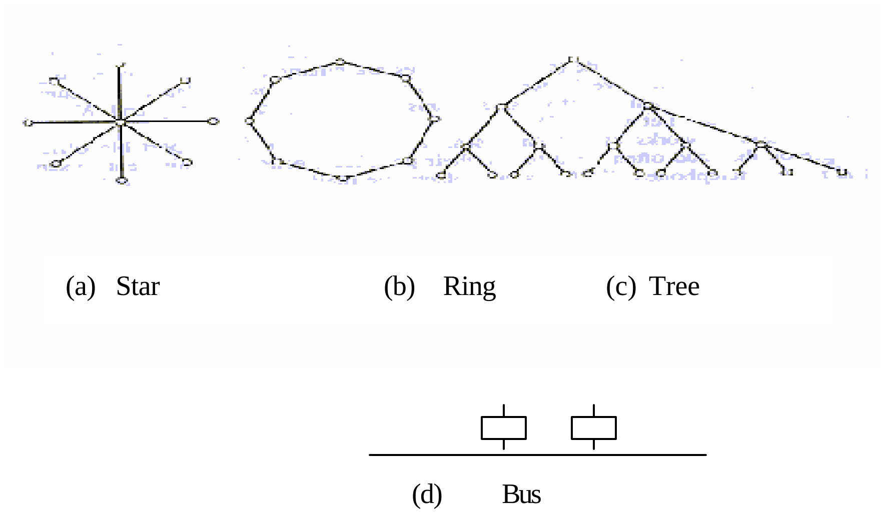
1.5 TYPES OF NETWORK

There are basically two types of network based on whether the network contains switching elements or not. These are point-to-point network and broadcast network.

1.5.1 Point to Point Network or Switched Networks

Point-to point networks consist of many connections between individual pairs of machines. Data is usually transferred in relatively small fragments called packets (units bits or bytes).To go from the source to the destination, a packet on this type of networks may have to first visit one or more intermediate routers. When a packet is sent from one router to another intermediate routers, the entire packet is stored at each intermediate router, stored there till the output line is free and then forwarded. A subnet using this principle is called point to point or packet switched network.

Some of possible topologies for a point to point subnet are:



(a) Star (b) Ring (c) Tree

(d) Bus

Figure 1: Caption

Star

In a star topology, each device has a dedicated point to point link only to a central controller, usually called a hub. These devices are not linked to each other. If one device wants to send data to another, it sends to the hub, which then relays the data to the other connected devices. In a star, each device needs only one link and one I/O Port to connect it to any number of other devices. This factor makes it easy to install and reconfigure. Far less cabling need to be housed and additions, moves and deletions involve only one connection between that device and the hub. However, reliability is low as hub failure disrupts the whole data transfer.

Tree

A tree topology is a variation of a star. As in a star, modes in a tree are linked to a central hub that controls the traffic to the network. However, not every device plugs directly into the central hubs. The majority of devices connect to a secondary hub that in turn is connected to the central hubs.

The advantage and disadvantages of a tree topology are generally the same as those of star. The addition of secondary hubs, however, brings two further advantages. First, it allows more devices to be attached to a single central hubs and can, therefore, increase the distance of a signal can travel between devices. Second it isolates the network and prioritize communication from different computers.

Ring

In a ring topology, each device has a dedicated point to point line configuration only with the two devices on either side of it. A signal is passed along the ring in one direction from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receiver a signal intended for another device, its repeater regenerates the bits and passes them along.

A ring is relatively easy to install and reconfigure. Each device is linked to its immediate neighbours. However, unidirectional traffic can be disadvantaged. In a simple ring, a break in ring can disable the entire network. This weakness can be solved by using a dual ring or use of switches capable of closing off breaks .

Bus

Bus, unlike other topologies is multipoint configurations. When the taps are passive. It can become point-to-point when taps are active switches. One long cable acts as a backbone to link all the devices in the network. Advantage of a bus topology includes use of installation. Disadvantage include difficult reconfiguration and fault isolation.

1.5.2 Broadcast Networks

Broadcast systems generally also allow the possibility of addressing a packet to all destinations by using a special code in the address field. When a packet with this code transmitted, it is received and processed by every machine on the network. This mode of operation is called broadcasting.

Broadcast networks have a single communication channel that is shared by all the machines on the network. Short messages, called packets sent by any machine are received by all the others. An address field within the packet specifies for whom it is intended. Upon receiving a packet, a machine checks the address field. If the packet is intended for itself, it processes the packet; if the packet is intended for some other machine, it is just ignored.

Some broadcast systems also support transmission to a subset of the machines, something known as multicasting. One possible scheme is to reserve one bit to indicate multicasting. The remaining (n-1) address bits can hold a group number. Each machine can "subscribe" to any or all of the groups. When a packet is sent to a certain group, it is delivered to all machines subscribing to that group.

1.6 REFERENCE MODEL

In this section we will discuss two important network architectures: the OSI reference model and the TCP/IP reference model.

1.6.1 OSI (Open Systems Interconnection) Reference Model

The OSI model is based on a proposal developed by the International Standards Organisation as a first step towards international standardisation of the protocols used in the various layers. The model is called the ISO - OSI (International Standard Organisation - Open Systems Interconnection) Reference Model because it deals with connecting open systems — that is, systems that follow the standard are open for communication with other systems, irrespective of manufacturer.

Its main objectives were to:

(i) Allow manufacturers of different systems to interconnect equipment through standard interfaces.
(ii) Allow software and hardware to integrate well and be portable on different systems.

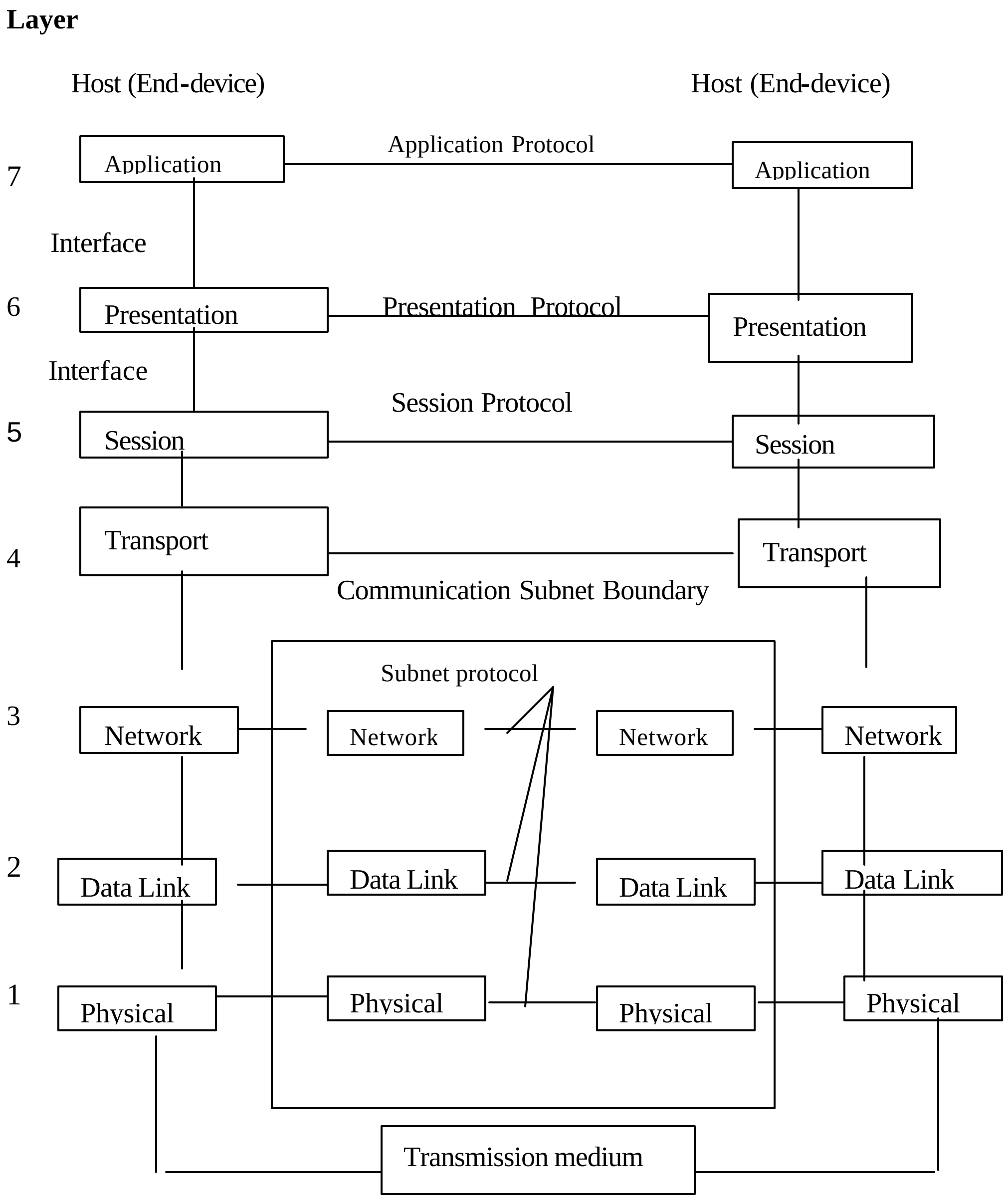
The OSI model has seven layers shown in *Figure 2.* The principles that were applied to arrive at the seven layers are as follows:

1. Each layer should perform a well-defined function.
2. The function of each layer should be chosen with an eye toward defining internationally standardised protocols.
3. The layer boundaries should be chosen to minimize the information flow across the interfaces.

The set of rules for communication between entities in a layer is called protocol for that layer.

The seven layers of ISO OSI reference model are:

(a) Physical Layer
(b) Data Link Layer
(c) Network Layer
(d) Transport Layer
(e) Session Layer
(f) Presentation Layer
(g) Application Layer.



Note: Submit is that part of the network to which end-devices (Hosts are attached)

Figure 2: OSI Reference Model

The Physical Layer

Physical Layer defines electrical and mechanical specifications of cables, connectors and signaling options that physically links two nodes on a network.

The Data Link Layer

The main task of the data link layer is to provide error free transmission. It accomplishes this task by having the sender configure the input data into data frames, transmit the frames sequentially, between network devices and process the acknowledgement frames sent back by the intermediate receiver.

The data link layer creates and recognises frame boundaries. This can be accomplished by attaching special bit patterns to the beginning and end of the frame. Since these bit patterns can accidentally occur in the data, special care must be taken to make sure these patterns are not incorrectly interpreted as frame boundaries.

The Network Layer

Whereas the datalink layer is responsible for delivery on a hop, the network layer ensures that each packet travels from its sources to destination successfully and efficiently. A key design issue is determining how packets are routed from source to destination. Routes can be based on static tables that are “wired into” the network and rarely changed. They can also be determined at the start of each conversation, for example a terminal session. Finally, they can be highly dynamic, being determined anew for each packet, to reflect the current network load.

When a packet has to travel from one network to another to get its destination, many problems can arise. The addressing used by the second network may be different from the first one. The second network one may not accept the packet at all because it is too large. The protocols may differ, and so on. It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.

The Transport Layer

The basic function of the transport layer is to accept data from the session layer, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. Furthermore, all this must be done efficiently, and in a way that isolates the upper layers from the inevitable changes in the hardware technology.

Transport Layer provides location and media independent end-to-end data transfer service to session and upper layers.

The Session Layer

The main tasks of the session layer is to provide:

- Session Establishment
- Session Release – Orderly or abort
- Synchnonization
- Data Exchange
- Expedited Data Exchange.

The session layer allows users on different machines to establish sessions between them. A session allows ordinary data transport, as does the transport layer, but it also provides enhanced services useful in some applications. A session might be used to allow a user to log into a remote timesharing system or to transfer a file between two machines.

One of the services of the session layer is to manage dialogue control. Sessions can allow traffic to go in both directions at the same time, or in only one direction at a time. If traffic can only go one way at a time (analogous to a single railroad track), the session layer can help keep track of whose turn it is.

A related session service is token management. For some protocols, it is essential that both sides do not attempt the same operation at the same time. To manage these activities, the session layer provides tokens that can be exchanged. Only the side holding the token may perform the desired operation.

Another session service is synchronization. Consider the problem that might occur when trying to do a 2 hour file transfer between two machines with a 1 hour mean time between crashes. After each transfer was aborted, the whole transfer would have to start over again and would probably fail again the next time as well. To eliminate this problem, the session layer provides a way to insert markers after the appropriate checkpoints.

The Presentation Layer

Unlike all the lower layers, which are just interested in moving bits reliably from here to there, the presentation layer is concerned with the syntax and semantics of the information transmitted.

A typical example of a presentation service is encoding data in a standard agreed upon way. Most user programs do not exchange random binary bit strings, they exchange things such as people's names, dates, amounts of money and invoices. These items are represented as character strings, integers, floating-point number, and data structures composed of several simpler items. Different computers have different codes for representing character strings (e.g., ASCII and Unicode), integers (e.g., one's complement and two's complement), and so on. In order to make it possible for computers with different representations to communicate, the data structure to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire". The presentation layer manages these abstract data structure and converts from the representation used inside the computer to the network standard representation and back.

Application Layer

Application Layer supports functions that control and supervise OSI application processes such as start/maintain/stop application, allocate/deallocate OSI resources, accounting, check point and recovering. It also supports remote job execution, file transfer protocol, message transfer and virtual terminal.

1.6.2 TCP Reference Model

The TCP/IP network architecture is a set of protocols that allow communication across multiple diverse networks. The architecture evolved out of research that had the original objective of transferring packets across three different packet networks: the **ARPANET** packet-switching network, a packet radio network, and a packet satellite network. The military orientation of the research placed a premium on robustness with regard to failures in the network and on flexibility in operating over diverse networks. This environment led to a set of protocols that are highly effective in enabling communications among the many different types of computer systems and networks. Today, the Internet has become the primary fabric for interconnecting the world's computers. In this section we introduce the TCP/IP network architecture and TCP/IP is the main protocol for carrying information.

Figure 3 shows the **TCP/IP network architecture,** which consists of four layers. The application layer provides services that can be used by other applications. For example, protocols have been developed for remote login, for e-mail, for file transfer, and for network management.

The application layer programs are intended to run directly over the transport layer. Two basic types of services are offered in the transport layer. The first service consists of reliable connection-oriented transfer of a byte stream, which is provided by the **Transmission Control Protocol (TCP)**. The second service consists of best-effort connectionless transfer of individual messages, which is provided by the **User Datagram Protocol (UDP)**. This service provides no mechanisms for error recovery or flow control. UDP is used for applications that require quick but reliable delivery is not guaranteed.

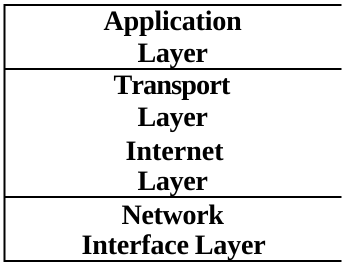


Figure 3: TCP/IP Network Architecture

The TCP/IP model does not require strict layering. In other words, the application layer has the option of bypassing intermediate layers. For example, an application layer may run directly over the Internet layer.

The **Internet layer** handles the transfer of information across multiple networks through the use of gateways or routers, as shown in *Figure 4*. The Internet layer corresponds to the part of the OSI network layer that is concerned with the transfer of packets between machines that are connected to different networks. It must therefore deal with the routing of packets across these networks as well as with the control of congestion. A key aspect of the Internet layer is the definition of *globally unique addresses* for machines that are attached to the Internet. The Internet layer provides a single service, namely, *best-effort connectionless packet transfer*. IP packets are exchanged between routers without a connection setup; the packets are routed independently, and so they may traverse different paths. For this reason, IP packets are also called **datagrams.** The connectionless approach makes the system robust; that is, if failures occur in the network, the packets are routed around the points of failure; there is no need to set up the connections. The gateways that interconnect the intermediate networks may discard packets when congestion occurs. The responsibility for recovery from these losses is passed on to the transport layer.

Finally, the **network interface layer** is concerned with the network-specific aspects of the transfer of packets. As such, it must deal with parts equivalent to OSI network layer and data link layer. Various interfaces are available for connecting end computer systems to specific networks such as X.25, ATM, frame relay, Ethernet, and token ring.

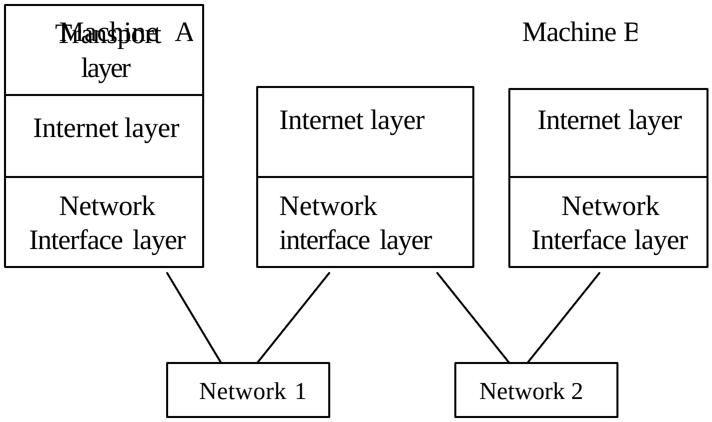


Figure 4: The Internet Layer and Network Interface Layers

The network interface layer is particularly concerned with the protocols that access the intermediate networks. At each gateway the network access protocol encapsulates the IP packet into a packet of the underlying network or link. The IP packet is recovered at the exit gateway of the given network. This gateway must then encapsulate the IP packet into new packet of the type of the next network or link. This approach provides a clear separation of the internet layer from the technology-dependent network interface layer. This approach also allows the internet layer to provide a data transfer service that is transparent in the sense of not depending on the details of the underlying networks. The next section provides a detailed example of how IP operates over the underlying networks.

Figure 5 shows some of the protocols of the TCP/IP protocol suite. The Figure shows two of the many protocols that operate over TCP, namely, HTTP and SMTP. The figure also shows DNS and Real-Time Protocol (RTP), which operate over UDP. The transport layer protocols TCP and UDP, on the other hand, operate over IP. Many network interfaces are defined to support IP. The salient part of *Figure 5* is that all higher-layer protocols access the network interfaces through IP. This feature provides the capability to operate over multiple networks. The basic IP protocol is complemented by additional protocols (ICMP, IGMP, ARP, RARP) that are required to operate an internet.

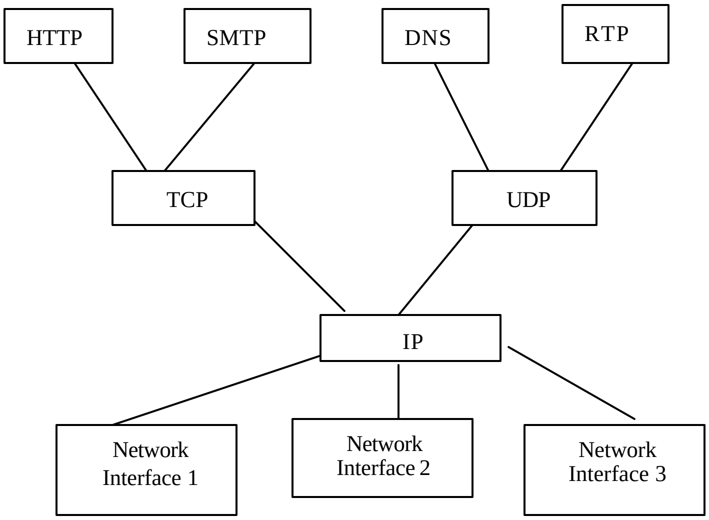


Figure 5: TCP/IP Protocol Graph

The hourglass shape of the TCP/IP protocol graph underscores the features that make TCP/IP so powerful. The operation of the single IP protocol over various networks provides independence from the underlying network technologies. The communication services of TCP and UDP provide a network independent platform on which applications can be developed. By allowing multiple network technologies to coexist, the Internet is able to provide wide connectivity and to achieve economies of scale.

1.6.3 Difference between OSI Reference Model & TCP Reference Model

OSI Reference Model	TCP Reference Model
1. Seven layers	1. 4 layers
2. It distinguishes between service, interface, protocol.	2. Did not clearly distinguish between service, interface and protocol.
3. Firstly description of model and protocol came next	3. Protocol comes first and description of model later.
4. Both have Network	4. Transport and Application layer.
5. Supports connectionless and connection oriented communication in network layer and only connection-oriented communication in transport layer.	5. TCP/1P has only one mode in Network layer (connection less) but supports both modes in Transport layer.
6. Protocol in OSI model are better hidden and can be replaced relatively easily (No Transparency).	6. Protocols in TCP/IP are not hidden and thus cannot be replaced easily. (Transparency)

1.7 IEEE MEDIUM ACCESS CONTROL (MAC) PROTOCOL STANDARDS FOR LAN

The medium access control (MAC) layer is a part of data link layer which interact with the physical layer.

Although there are many standards, we will describe some features of three of them:

- IEEE Standard 802.3 (Ethernet)
- IEEE Standard 804 (Token Bus)
- IEEE Standard 802.5 (Token Ring)

IEEE Standard 802.3 and Ethernet

1. 802.3 is a simple protocol. Stations can be installed on fly without taking network down. A passive cable can be used and modems are not required. Delay at low load is practically zero. A station is allowed to attempt transmission immediately. Each station has to be able to detect the signal of the weakest of other stations even when it itself is transmitting. Packets can collide. Minimum valid frame is 64 bytes.

2. 802.4 bus – It uses highly reliable cable envision equipments which is available from numerous vendors. It uses tokens to allow stations for start of transmission. It is more deterministic than 802.3 although repeated losses of the token at critical moments can introduce more uncertainty than its supporters like to admit. Token Bus also supports priorities.

3. Token Ring – Point to Point Connection means that the engineering is easy and can be fully digital. Ring can be built using suitable in a transmission medium including optical fibers. The standard twisted pair is cheap and simple to install line in the Token Bus in token ring priorities are possible.

☞ Check Your Progress

1) What are various types of networks?

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

2) What is the difference between broadcasting and Multicasting?

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

1.8 SUMMARY

A communication system that supports many users is called a network. In a network many computers are connected to each other by various topologies like star, ring, complete, interconnected or irregular. Depending on the area of coverage a network can be classified as LAN, MAN or WAN. A network is required for better utilisation of expensive resources, sharing information, collaboration among different groups, multimedia communication and video conferencing.

The two different types of networking models OSI and TCP/IP are existing. The difference between these models was discussed in detail.

1.9 SOLUTIONS/ANSWERS

1. There are basically two types of networks:

   (i) Point to point network or switched networks
   (ii) Broadcast Networks.

2. Broadcasting refers to addressing a packet to all destinations in a network whereas multicasting refers to addressing a packet to a subset of the entire network.