UNIT I

INTRODUCTION

UNIT I INTRODUCTION 10 hrs.

Introduction: Communication model, Network H/W, Network S/W, OSI reference Model, TCP/IP protocol suite, Network services and Interfaces, Network Topologies, Networks example, Network Standardization, World Wide Web, Multimedia applications.

1. Historical Background

The history of electronic computers is not very old. It came into existence in the early 1950s and during the first two decades of its existence it remained as a centralized system housed in a single large room. In those days the computers were large in size and were operated by trained personnel. To the users it was a remote and mysterious object having no direct communication with the users. Jobs were submitted in the form of punched cards or paper tape and outputs were collected in the form of computer printouts. The submitted jobs were executed by the computer one after the other, which is referred to as batch mode of data processing. In this scenario, there was long delay between the submission of jobs and receipt of the results.

In the 1960s, computer systems were still centralizing, but users provided with direct access through interactive terminals connected by point-to-point low-speed data links with the computer. In this situation, a large number of users, some of them located in remote locations could simultaneously access the centralized computer in time-division multiplexed mode. The users could now get immediate interactive feedback from the computer and correct errors immediately. Following the introduction of on-line terminals and time-sharing operating systems, remote terminals were used to use the central computer. With the advancement of VLSI technology, and particularly, after the invention of microprocessors in the early 1970s, the computers became smaller in size and less expensive, but with significant increase in processing power. New breed of low-cost computers known as mini and personal computers were introduced. Instead of having a single central computer, an organization could now afford to own a number of computers located in different departments and sections. Side-by-side, riding on the same VLSI technology the communication technology also advanced leading to the worldwide deployment of telephone network, developed primarily for voice communication. An organization having computers located geographically dispersed locations wanted to have data communications for diverse applications.

Communication was required among the machines of the same kind for collaboration, for the use of common software or data or for sharing of some costly resources. This led to the development of computer networks by successful integration and cross-fertilization of communications and geographically dispersed computing facilities. One significant development was the APPANET (Advanced Research Projects Agency Network).

Starting with four-node experimental network in 1969, it has subsequently grown into a network several thousand computers spanning half of the globe, from Hawaii to Sweden. Most of the present-day concepts such as packet switching evolved from the ARPANET project. The low bandwidth (3KHz on a voice grade line) telephone network was the only generally available communication system available for this type of network. Version 2 CSE IIT, Kharagpur The bandwidth was clearly a problem, and in the late 1970s and early 80s another new communication technique known as Local Area Networks (LANs) evolved, which helped computers to communicate at high speed over a small geographical area. In the later years use of optical fiber and satellite communication allowed high-speed data communications over long distances.

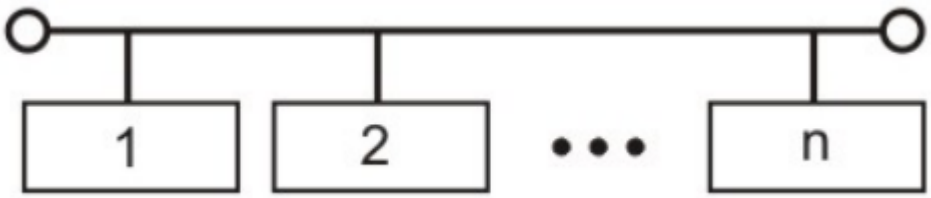


Figure 1.1 Example of a broadcast network based on shared bus

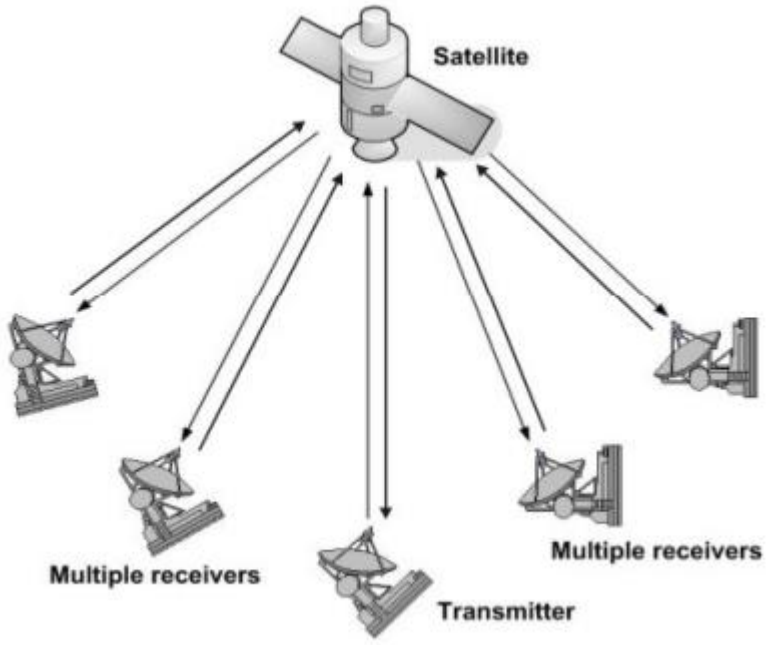


Figure 1.2 Example of a broadcast network based on satellite communication

This system generally also allows possibility of addressing the packet to all destinations (all nodes on the network). When such a packet is transmitted and received by all the machines on the network. This mode of operation is known as Broadcast Mode. Some Broadcast systems also support transmission to a sub-set of machines, something known as Multicasting.

1.1 DATA COMMUNICATION:

Communication means sharing of information. Data is the information presented in whatever form is agreed upon by the parties. Data Communication refers to the exchange of data between two devices via some form of transmission medium such as wire cable.

The effectiveness of data communication depends on three fundamental characteristics.

- **Delivery**: The system must deliver the data correctly to the intended destination.
- **Accuracy:** The system must deliver the data accurately.
- **Timeliness**: The system must deliver data in a timely manner.

1.1.1 Components

The system consists of five components:

1. Message
2. Sender
3. Receiver
4. Medium
5. Protocol

Message:
The message is the information to be communicated. It can consist of text, numbers, pictures, sound or video or any combination of these.

Sender:
The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera and so on.

Receiver:
The receiver is the device that receives the data messages. It can be a workstation, telephone handset, video camera and so on.

Medium:
The transmission medium is the physical path by which a message travels from the sender to receiver. It could be a twisted pair wire, co-axial cable fibre optic cable or radio waves.

Protocol:
A protocol is a set of rules that governs data communications. It represents an agreement between the communication devices. Without a protocol two devices may be connected but not communicating

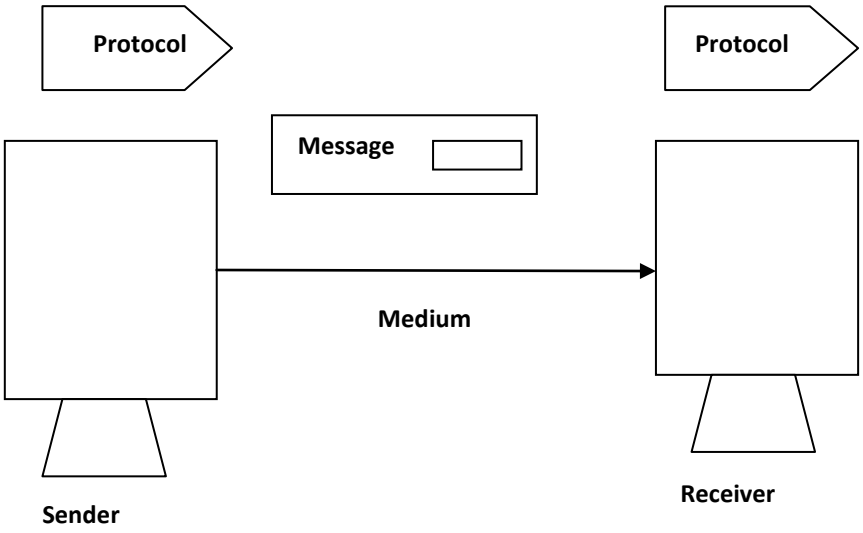
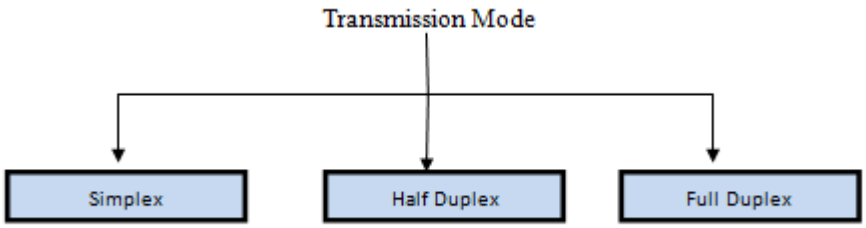


Figure 1.3 Five Components of Data communication

1.2 TRANSMISSION MODE(DIRECTION OF DATA FLOW)

Transmission mode means transferring of data between two devices. It is also called communication mode. These modes direct the direction of flow of information. There are three types of transmission mode. They are

- Simplex Mode
- Half duplex Mode
- Full duplex Mode



1.2.1 Simplex Mode

In half duplex system we can send data in both directions but it is done one at a time that is when the sender is sending the data then at that time we can't send the sender our message. The data is sent in one direction.

Example of half duplex is a walkie- talkie in which message is sent one at a time and messages are sent in both the directions.

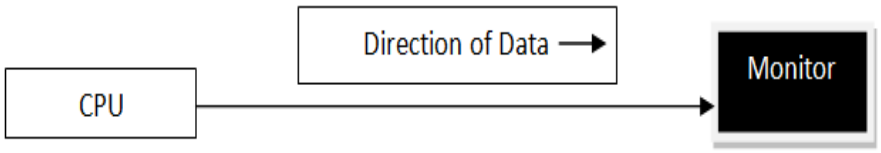


Figure 1.4 Simplex mode of transmission

1.2.2 Half Duplex

In half duplex system we can send data in both directions but it is done one at a time that is when the sender is sending the data then at that time we can't send the sender our message. The data is sent in one direction.

Example of half duplex is a walkie- talkie in which message is sent one at a time and messages are sent in both the directions.

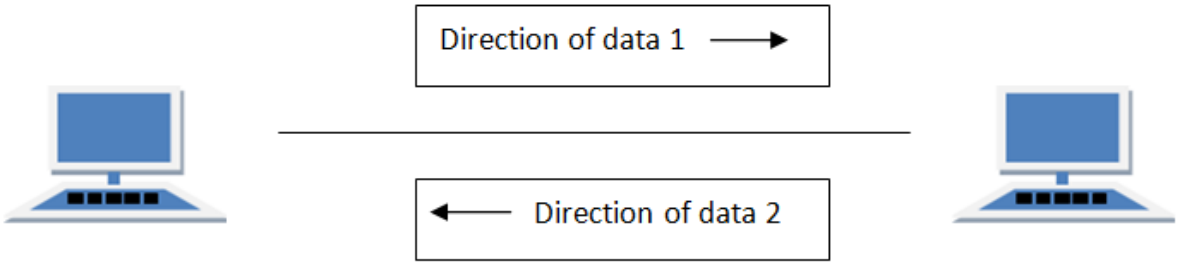


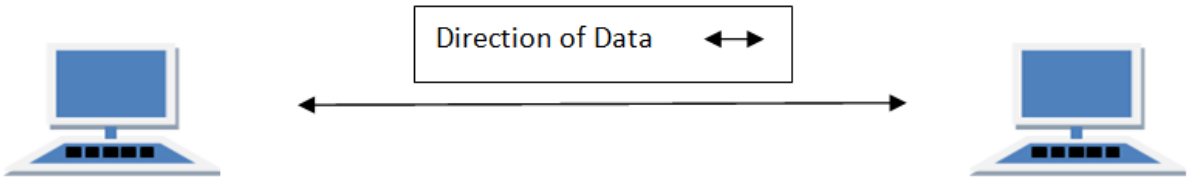
Figure 1.5 Duplex mode of transmission

1.2.3 Full Duplex

In full duplex system we can send data in both directions as it is bidirectional. Data can be sent in both directions simultaneously. We can send as well as we receive the data.

Example of Full Duplex is a Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.

In full duplex system there can be two lines one for sending the data and the other for receiving data.



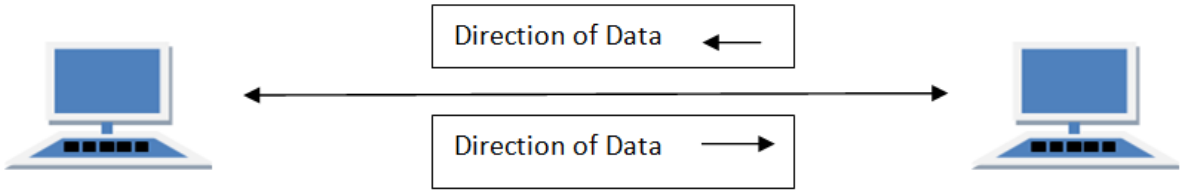


Figure 1.6 Full Duplex mode of transmission

1.3 NETWORK

A network is a group of two or more computer systems linked together. There are many types of computer networks, including the following: local-area networks (LANs): The computers are geographically close together (that is, in the same building)

1.3.1 Distributed Processing:

Most networks use distributed processing, in which a task is divided among multiple computers. Instead of a single large machine being responsible for all aspects of process, separate computers handle a subset.

1.3.2 Advantages of distributed Processing

1. Security/Encapsulation
2. Distributed databases
3. Faster problem solving
4. Security through redundancy
5. Collaborative processing

1.4 TYPES OF NETWORK CONNECTIONS

1.4.1 Point-to-point Connection

A point-to-point connection is a direct link between two devices such as a computer and a printer. It uses dedicated link between the devices. The entire capacity of the link is used for the transmission between those two devices. Most of today's point-to-point connections are associated with modems and PSTN (Public Switched Telephone Network) communications. In point to point networks, there exist many connections between individual pairs of machines.

To move from sources to destination, a packet (short message) may follow different routes. In networking, the Point-to-Point Protocol (PPP) is a data link protocol commonly used in establishing a direct connection between two networking nodes.

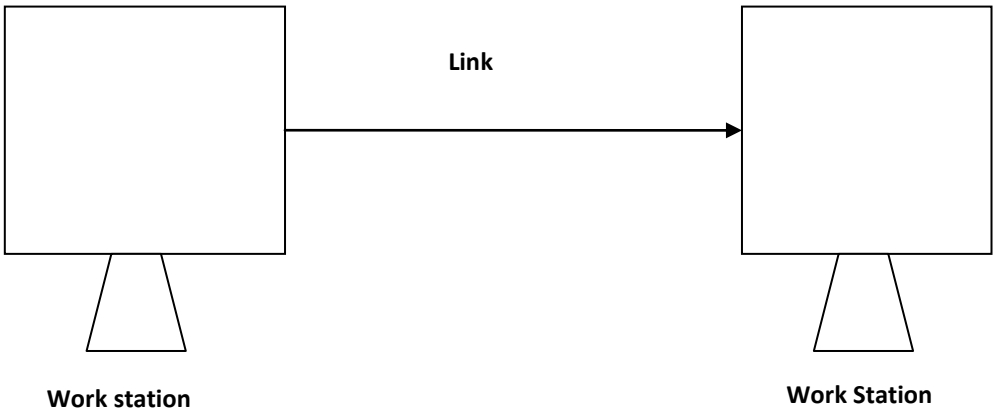


Figure 1.7 Point-to-Point Connections

1.4.2 Multipoint Connection

A multipoint connection is a link between three or more devices. It is also known as Multi-drop configuration. The networks having multipoint configuration are called **Broadcast Networks**. In broadcast network, a message or a packet sent by any machine is received by all other machines in a network. The packet contains address field that specifies the receiver. Upon receiving a packet, every machine checks the address field of the packet. If the transmitted packet is for that particular machine, it processes it; otherwise it just ignores the packet. Broadcast network provides the provision for broadcasting & multicasting. Broadcasting is the process in which a single packet is received and processed by all the machines in the network. It is made possible by using a special code in the address field of the packet. When a packet is sent to a subset of the machines i.e. only to few machines in the network it is known as multicasting.

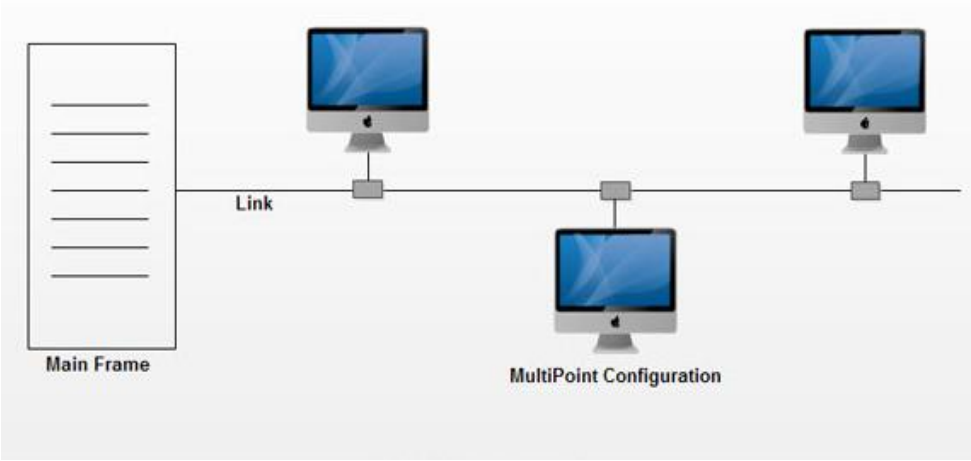


Figure 1.8 Multi point Connections

1.5 NETWORK TOPOLOGY

Topology refers to the way in which the network of computers is connected. Each topology is suited to specific tasks and has its own advantages and disadvantages. The choice of topology is dependent upon type and number of equipment being used, planned applications and rate of data transfer required, response time, and cost. Topology can also be defined as the geometrically interconnection pattern by which the stations (nodes/computers) are connected using suitable transmission media (which can be point to-point and broadcast). Various commonly used topologies are discussed in the following sections.

1.5.1 Mesh Topology

In this topology each node or station is connected to every other station as shown in Fig.1.9 The key characteristics of this topology are as follows:

Key Characteristics:

- Fully connected
- Robust – Highly reliable
- Not flexible
- Poor expandability

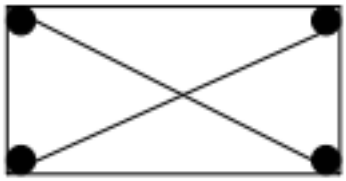


Figure 1.9 Mesh Topology

Two nodes are connected by dedicated point-point links between them. So the total number of links to connect n nodes = n(n-1)/2; which is proportional to n2 . Media used for the connection (links) can be twisted pair, co-axial cable or optical fiber. With this topology there is no need to provide any additional information, which is from where the packet is coming, along with the packet because two nodes have a point-point dedicated link between them. And each node knows which link is connected to which node on the other end. Mesh Topology is not flexible and has a poor expandability as to add a new node n links have to be laid because that new node has to be connected to each of the existing nodes via dedicated link as shown in Fig. 1.10. For the same reason the cost of cabling will be very high for a larger area. And due to these reasons this topology is rarely used in practice.

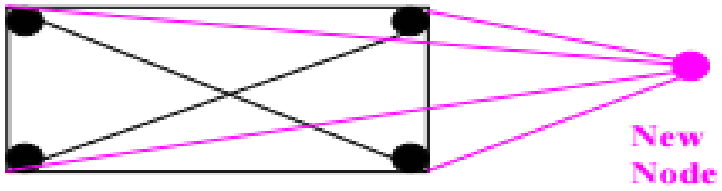


Figure 1.10 Adding a new node in mesh topology

1.5.2 Bus Topology

In Bus Topology, all stations attach through appropriate hardware interfacing known as a tap, directly to a linear transmission medium, or bus as shown in Fig. 1.11.. Full-duplex operation between the station and the tap allows data to be transmitted onto the bus and received from the bus. A transmission from any station propagates the length of the medium

in both directions and can be received by all other stations. At each end of the bus there is a terminator, which absorbs any signal, preventing reflection of signal from the endpoints. If the terminator is not present, the endpoint acts like a mirror and reflects the signal back causing interference and other problems.

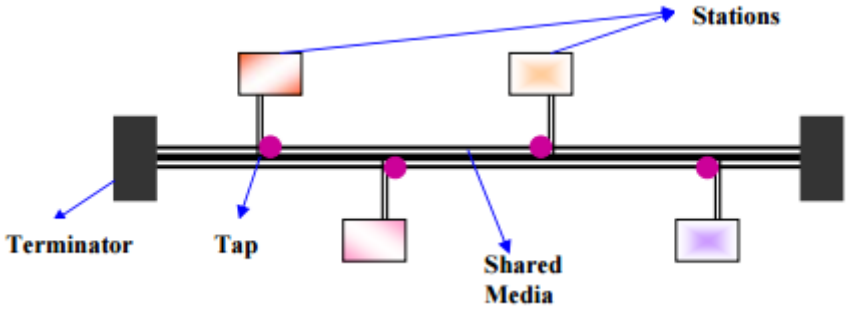


Figure 1.11 bus topology

Key Characteristics of this topology are:

- Flexible
- Expandable
- Moderate
- Reliability
- Moderate performance

A shared link is used between different stations. Hence it is very cost effective. One can easily add any new node or delete any node without affecting other nodes; this makes this topology easily expandable. Because of the shared medium, it is necessary to provide some extra information about the desired destination, i.e. to explicitly specify the destination in the packet, as compared to mesh topology. This is because the same medium is shared among many nodes. As each station has a unique address in the network, a station copies a packet only when the destination address of the packet matches with the self-address. This is how data communications take place among the stations on the bus.

As there are dedicated links in the mess topology, there is a possibility of transferring data in parallel. But in bus topology, only one station is allowed to send data at a time and all other stations listen to it, as it works in a broadcast mode. Hence, only one station can transfer the data at any given time. Suitable medium access control technique should be used so as to provide some way to decide “who” will go next to send data? Usually a distributed medium access control technique, as discussed in the next lesson, is used for this purpose.

As the distance through which signal traverses increases, the attenuation increases. If the sender sends data (signal) with a small strength signal, the farthest station will not be able to receive the signal properly. While on the other hand if the transmitter sends the signal with a larger strength (more power) then the farthest station will get the signal properly but the station near to it may face over-drive. Hence, delay and signal unbalancing will force a maximum length of shared medium, which can be used in bus topology.

1.5.3 STAR Topology

In the star topology, each station is directly connected to a common central node as shown in Fig. 1.12. Typically, each station attaches to a central node, referred to as the star coupler, via two point-to-point links, one for transmission and one for reception.

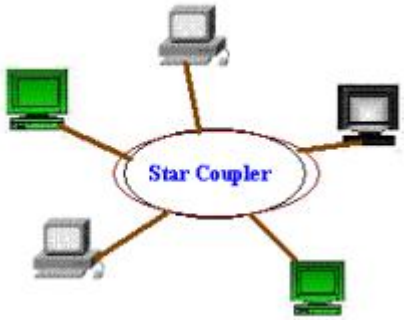


Figure 1.12 Star Topology

In general, there are two alternatives for the operation of the central node.

- One approach is for the central node to operate in a broadcast fashion. A transmission of a frame from one station to the node is retransmitted on all of the outgoing links. In this case, although the arrangement is physically a star, it is logically a bus; a transmission from any station is received by all other stations, and only one station at a time may successfully transmit. In this case the central node acts as a repeater.
- Another approach is for the central node to act as a frame-switching device. An incoming frame is buffered in the node and then retransmitted on an outgoing link to the destination station. In this approach, the central node acts as a switch and performs the switching or routing function. This mode of operation can be compared with the working of a telephone exchange, where the caller party is connected to a single called party and each pair of subscriber who needs to talk have a different connection. Very High speeds of data transfer can be achieved by using star topology, particularly when the star coupler is used in the switch mode. This topology is the easiest to maintain, among the other topologies. As the number of links is proportional to n, this topology is very flexible and is the most preferred topology.

1.5.4 Ring topology

In the ring topology, the network consists of a set of repeaters joined by point-to-point links in a closed loop as shown in Fig. 1.13. The repeater is a comparatively simple device, capable of receiving data on one link and transmitting them, bit by bit, on the other link as fast as they are received, with no buffering at the repeater. The links are unidirectional; that is data are transmitted in one direction only and all are oriented in the same way. Thus, data circulate around the ring in one direction (clockwise or counterclockwise).

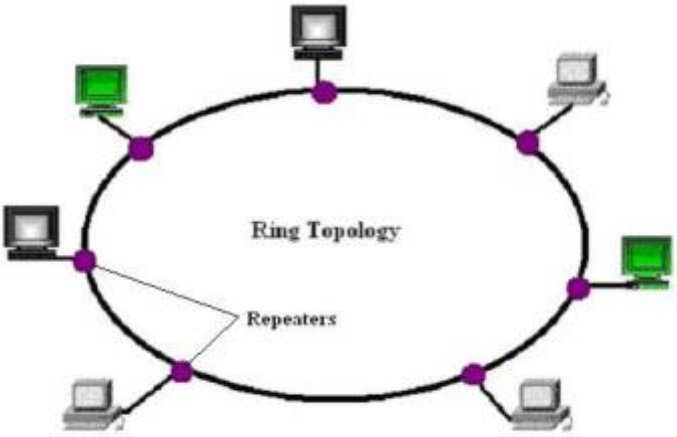


Figure 1.13 Ring Topology

Each station attaches to the network at a repeater and can transmit data onto the network through that repeater. As with the bus and tree, data are transmitted in frames. As a frame circulates past all the other stations, the destination station recognizes its address and copies the frame into a local buffer as it goes by. The frame continues to circulate until it returns to the source station, where it is removed. Because multiple stations share the ring, medium access control is needed to determine at what time each station may insert frames. How the source knows whether it has to transmit a new packet and whether the previous packet has been received properly by the destination or not. For this, the destination change a particular bit (bits) in the packet and when the receiver sees that packet with the changed bit, it comes to know that the receiver has received the packet. This topology is not very reliable, because when a link fails the entire ring connection is broken. But reliability can be improved by using wiring concentrator, which helps in bypassing a faulty node and somewhat is similar to star topology.

Repeater works in the following three modes:

Listen mode:

In this mode, the station listens to the communication going over the shared medium as shown in Fig.1.14.

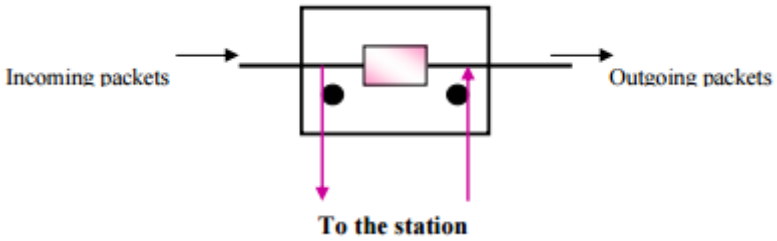


Figure 1.14 Repeater in Listen Mode

Transmit mode: In this mode the station transmit the data over the network as shown in Fig. 1.15.

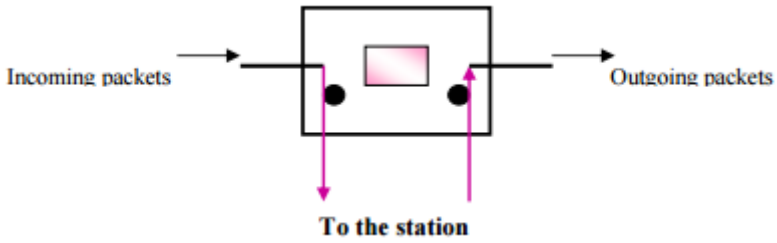


Figure 1.15 Repeater in transmit Mode

By-Pass mode:

When the node is faulty then it can be bypassed using the repeater in bypass mode, i.e. the station doesn't care about what data is transmitted through the network, as shown in Fig. 1.16. In this mode there is no delay introduced because of this repeater.

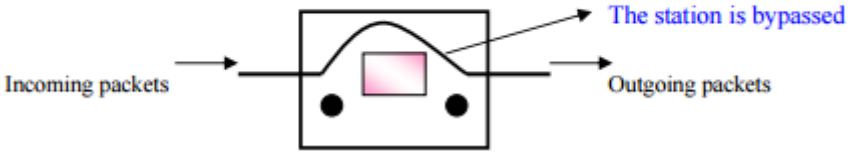


Figure 1.16 Repeater in By-pass Mode

Tree Topology

This topology can be considered as an extension to bus topology. It is commonly used in cascading equipments. For example, you have a repeater box with 8-port, as far as you have eight stations, this can be used in a normal fashion. But if you need to add more stations then you can connect two or more repeaters in a hierarchical format (tree format) and can add more stations. In the Fig. 1.17, R1 refers to repeater one and so on and each repeater is considered to have 8-ports.

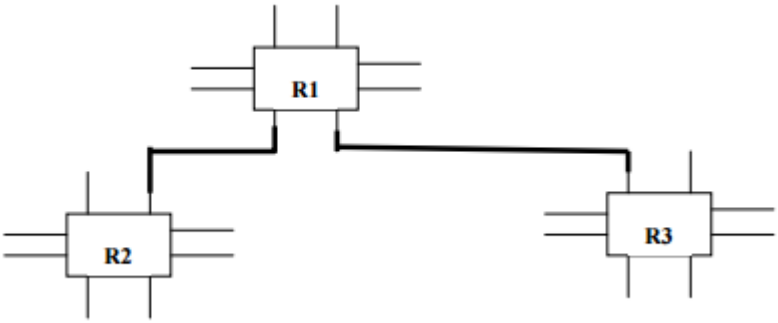


Figure 1.17 Tree Topology

Unconstrained Topology

All the topologies discussed so far are symmetric and constrained by well-defined interconnection pattern. However, sometimes no definite pattern is followed and nodes are interconnected in an arbitrary manner using point-to-point links as shown in Fig 5.1.10. Unconstrained topology allows a lot of configuration flexibility but suffers from the complex routing problem. Complex routing involves unwanted overhead and delay.

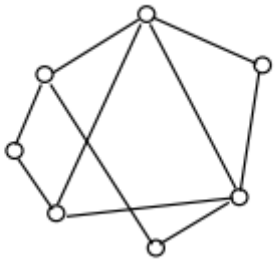


Figure 1.18 Unconstrained topology

1.6 NETWORK HARDWARE

The computer networks are classified based on:

- Transmission technology
- Scale

1.6.1 Transmission technology:

It is broadly classified as **broadcast** links and **point to point** links.

(1) Point to point links:

- Connect Individual pairs of machine.
- Short messages called as packets are sent from the source to the destination travelling through the intermediate nodes.
- Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called unicasting.

(2) Broadcast links

- Communication channel is shared by all the machines in the network.
- Packets sent by any machine are received by all the others.
- An address field within each packet specifies the intended recipient.
- Upon receiving a packet, a machine checks the address field. If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.
- An example of broadcast link is wireless networks.
- Broadcast systems usually 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 is transmitted, it is received and processed by every machine on the network. This mode of operation is called broadcasting.
- Some broadcast systems also support transmission to a subset of the machines, which known as multicasting.

1.6.2 Scale

- Distance is important as a classification metric because different technologies are used at different scales.
- In Fig. 1-19 we classify multiple processor systems by their rough physical size.

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Figure 1.19 Classification of interconnected processors by scale

The network hardware is scaled as follows:

1.6.3 Personal Area Network(PAN)

PANs (Personal Area Networks) let devices communicate over the range of a person. A common example is a wireless network that connects a computer with its peripherals. Almost every computer has an attached monitor, keyboard, mouse, and printer. Without using wireless, this connection must be done with cables.

A short range wireless network can be designed using a Bluetooth service. Bluetooth networks use the master-slave paradigm of Fig1.20. The system unit (the PC) is normally the master, talking to the mouse, keyboard, etc., as slaves. The master tells the slaves what addresses to use, when they can broadcast, how long they can transmit, what frequencies they can use, and so on.

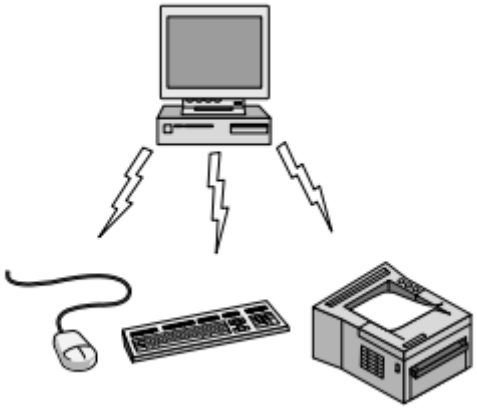


Figure1.20 Bluetooth PAN configuration

A completely different kind of PAN is formed when an embedded medical device such as a pacemaker, insulin pump, or hearing aid talks to a user-operated remote control. As a general rule (although there are many exceptions), smaller, geographically localized networks tend to use broadcasting, whereas larger networks normally use are point-to point communication. PANs can also be built with other technologies that communicate over short ranges, such as RFID on smartcards and library books.

1.6.4 Local Area Network (LAN)

LAN is usually privately owned and links the devices in a single office, building or campus of up to few kilometers in size. These are used to share resources (may be hardware or software resources) and to exchange information. LANs are distinguished from other kinds of networks by three categories: their size, transmission technology and topology. LANs are restricted in size, which means that their worst-case transmission time is bounded and known in advance. Hence this is more reliable as compared to MAN and WAN. Knowing this bound makes it possible to use certain kinds of design that would not otherwise be possible. It also simplifies network management. LAN typically used transmission technology consisting of single cable to which all machines are connected. Traditional LANs run at speeds of 10 to 100 Mbps (but now much higher speeds can be achieved). The most common LAN topologies are bus, ring and star. A typical LAN is shown in Fig. 1.21.

The topology of many wired LANs is built from point-to-point links. IEEE 802.3, popularly called Ethernet, is, by far, the most common type of wired LAN. Each computer speaks the Ethernet protocol and connects to a box called a switch with a point-to-point link. Hence the name. A switch has multiple ports, each of which can connect to one computer. The job of the switch is to relay packets between computers that are attached to it, using the address in each packet to determine which computer to send it to.

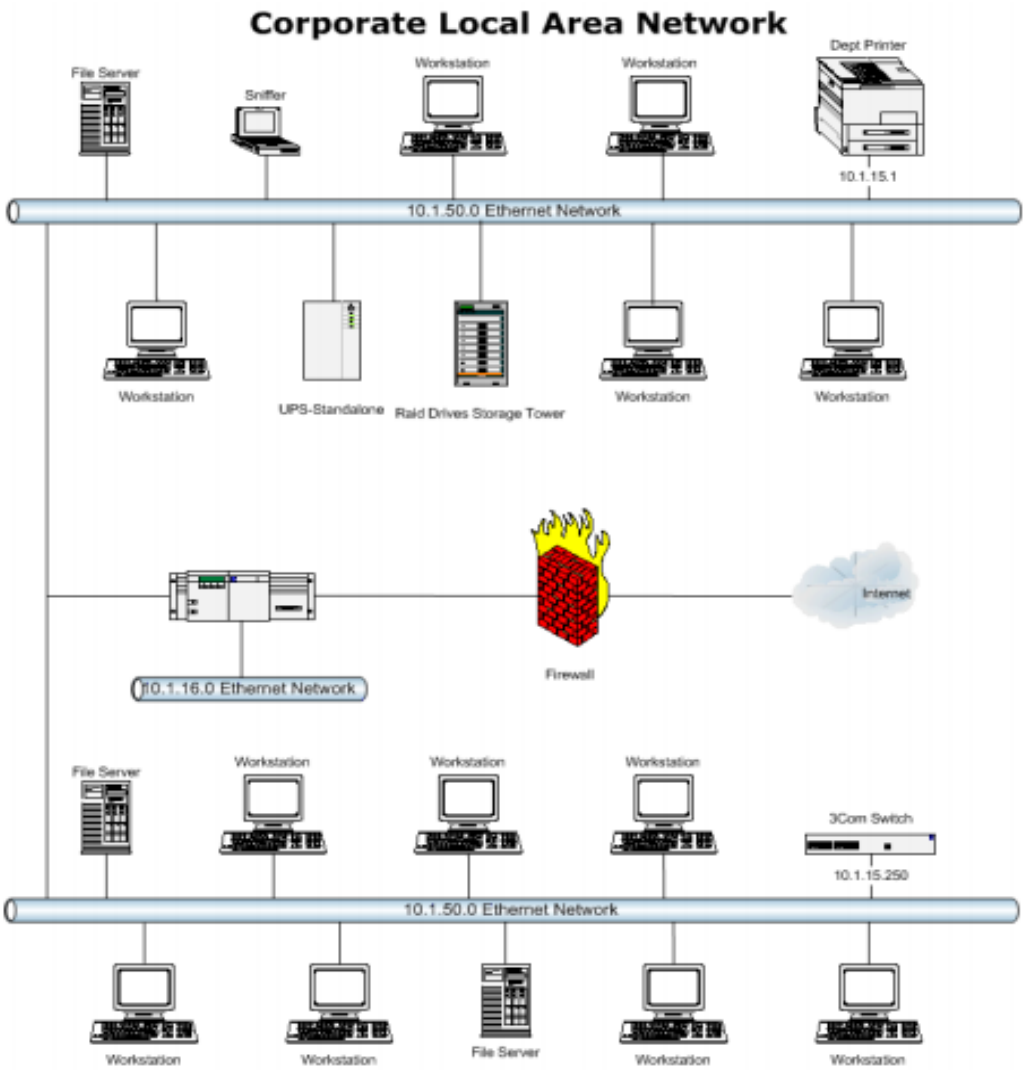


Figure 1.21 Local Area Network

1.6.5 Metropolitan Area Networks (MAN)

MAN is designed to extend over the entire city. It may be a single network as a cable TV network or it may be means of connecting a number of LANs into a larger network so that resources may be shared as shown in Fig. 1.22. For example, a company can use a MAN to connect the LANs in all its offices in a city. MAN is wholly owned and operated by a private company or may be a service provided by a public company.

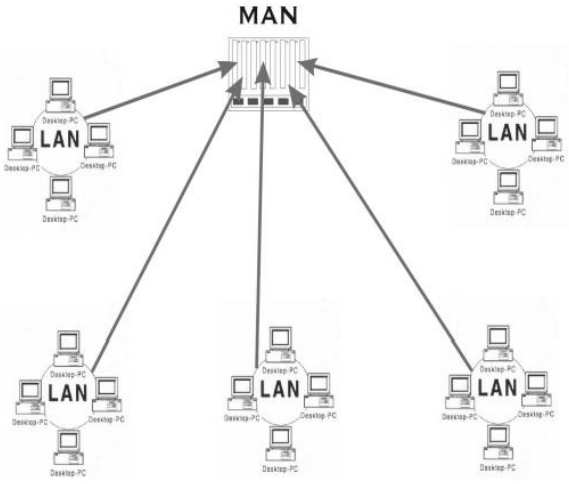


Figure 1.22 Metropolitan Area Network

The main reason for distinguishing MANs as a special category is that a standard has been adopted for them. It is DQDB (Distributed Queue Dual Bus) or IEEE 802.6.

1.6.6 Wide Area Network (WAN)

WAN provides long-distance transmission of data, voice, image and information over large geographical areas that may comprise a country, continent or even the whole world. In contrast to LANs, WANs may utilize public, leased or private communication devices, usually in combinations, and can therefore span an unlimited number of miles as shown in Fig. 1.23. A WAN that is wholly owned and used by a single company is often referred to as enterprise network.

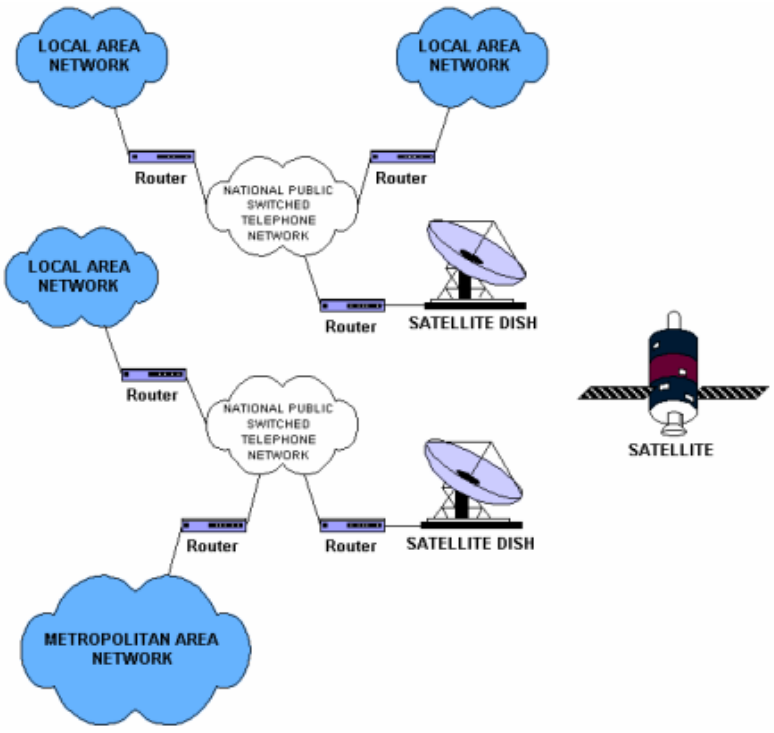


Figure 1.23 Wide Area Network

1.6.7 The Internet

Internet is a collection of networks or network of networks. Various networks such as LAN and WAN connected through suitable hardware and software to work in a seamless manner. Schematic diagram of the Internet is shown in Fig.1.24. It allows various applications such as e-mail, file transfer, remote log-in, World Wide Web, Multimedia, etc run across the internet. The basic difference between WAN and Internet is that WAN is owned by a single organization while internet is not so. But with the time the line between WAN and Internet is shrinking, and these terms are sometimes used interchangeably.

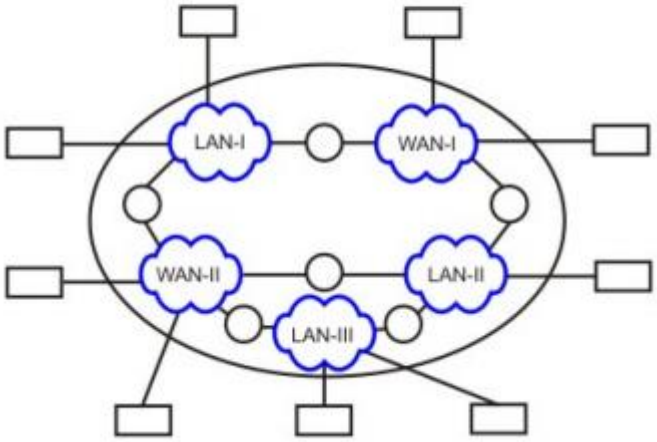


Figure 1.24 Internet – network of networks

1.6.8 Applications

In a short period of time computer networks have become an indispensable part of business, industry, entertainment as well as a common-man's life. These applications have changed tremendously from time and the motivation for building these networks are all essentially economic and technological. Initially, computer network was developed for defense purpose, to have a secure communication network that can even withstand a nuclear attack. After a decade or so, companies, in various fields, started using computer networks for keeping track of inventories, monitor productivity, communication between their different branch offices located at different locations. For example, Railways started using computer networks by connecting their nationwide reservation counters to provide the facility of reservation and enquiry from anywhere across the country. And now after almost two decades, computer networks have entered a new dimension; they are now an integral part of the society and people. In 1990s, computer network started delivering services to private individuals at home. These services and motivation for using them are quite different. Some of the services are access to remote information, person-person communication, and interactive entertainment. So, some of the applications of computer networks that we can see around us today are as follows:

Marketing and sales: Computer networks are used extensively in both marketing and sales organizations. Marketing professionals use them to collect, exchange, and analyze data related to customer needs and product development cycles. Sales application includes teleshopping, which uses order-entry computers or telephones connected to order processing network, and online-reservation services for hotels, airlines and so on.

Financial services: Today's financial services are totally depended on computer networks. Application includes credit history searches, foreign exchange and investment services, and electronic fund transfer, which allow user to transfer money without going into a bank (an automated teller machine is an example of electronic fund transfer, automatic pay-check is another).

Manufacturing: Computer networks are used in many aspects of manufacturing including manufacturing process itself. Two of them that use network to provide essential services are computer-aided design (CAD) and computer-assisted manufacturing (CAM), both of which allow multiple users to work on a project simultaneously.

Directory services: Directory services allow list of files to be stored in central location to speed worldwide search operations.

Information services: A Network information service includes bulletin boards and data banks. A World Wide Web site offering technical specification for a new product is an information service.

Electronic data interchange (EDI): EDI allows business information, including documents such as purchase orders and invoices, to be transferred without using paper.

Electronic mail: probably it's the most widely used computer network application. **Teleconferencing:** Teleconferencing allows conference to occur without the participants being in the same place. Applications include simple text conferencing (where participants communicate through their normal keyboards and monitor) and video conferencing where participants can even see as well as talk to other fellow participants. Different types of equipments are used for video conferencing depending on what quality of the motion you want to capture (whether you want just to see the face of other fellow participants or do you want to see the exact facial expression).

Voice over IP: Computer networks are also used to provide voice communication. This kind of voice communication is pretty cheap as compared to the normal telephonic conversation.

Video on demand: Future services provided by the cable television networks may include video on request where a person can request for a particular movie or any clip at anytime he wish to see.

1.7 NETWORK SOFTWARE

- **Protocols :**A set of rules that governs data communication; the key element of a protocol are
- **Syntax:** data formats & signal levels.
- **Semantics:** Control Information and error handling
- **Timing :**Speed matching and sequencing
- **Standards**: To ensure the products from different manufacturers can work together as expected.

1.7.1 Protocol Hierarchies

In order to understand how the actual communication is achieved between two remote hosts connected to the same network; a general network diagram is shown in Fig. 1.25 divided into a series of layers. As it seen later on the course the actual number as well as their function of each layer differs from network to network. Each layer passes data and control information to the layer below it. As soon as the data are collected form the next layer, some functions are performed there and the data are upgraded and passed to the next layer. This continues until the lowest layer is reached. Actual communication occurs when the information passes layer 1 and reaches the Physical medium. The entities comprising the corresponding layers on different machines are called peers. The peers may be software processes, hardware devices, or even human beings. In other words, it is the peers that communicate by using the protocol to talk to each other.

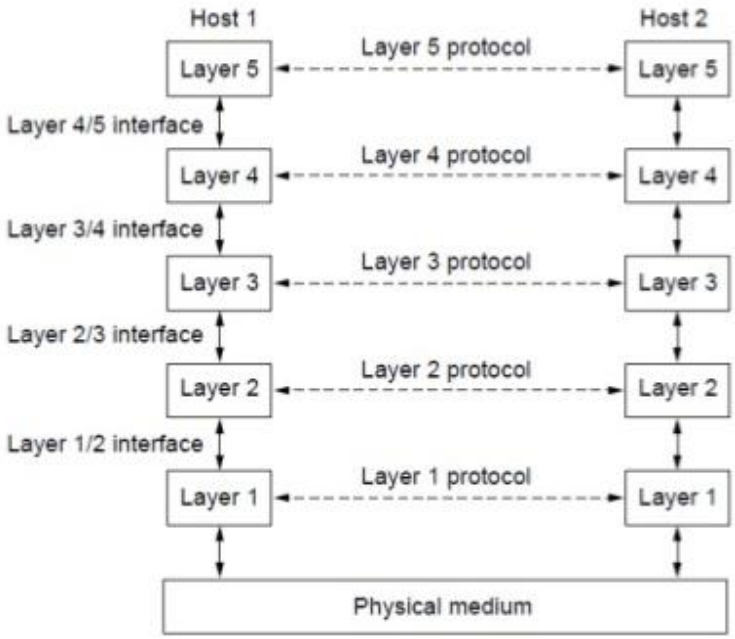


Figure 1.25 Layers, Protocols and Interfaces

Theoretically layer n on one machine maintains a conversation with the same layer in the other machine. The way this conversation is achieved is by the protocol of each layer. Protocol is collection of rules and conventions as agreement between the communication parties on how communication is to proceed. The later is known as virtual communication and is indicated with the dotted lines on the diagram above.

As far as the Fig. 1.25 is concerned another important issue to be discussed is the interface between each layer. It defines the services and operation the lower layer offers to the one above It. When a network is built decisions are made to decide how many layers to be included and what each layer should do. So each layer performs a different function and as a result the amount of information past from layer to layer is minimized.

1.7.2 Design Issues for the Layers

The design issues for the layers are classified into three respectively as reliability, evolution of network, resource allocation and security.

(1) Reliability: Is the design issue of making a network that operates correctly even though it is made up of a collection of components that are themselves unreliable.

Error Detection and Correction: Detecting the errors in received information. Resending and correcting the data using powerful codes through which the incorrect bits are corrected.

Routing: To route the packets in the correct path among the multi paths

(2) Evolution of Network: Over time, networks grow larger and new designs emerge that need to be connected to the existing network.

Protocol layering: key structuring mechanism used to support change by dividing the overall problem

Addressing: Every layer needs a mechanism to identify the sender and receiver.

Scalability: When networks get large, new problems arise. Cities can have traffic jams, a shortage of telephone numbers, and it is easy to get lost. Not many people have these problems in their own neighborhood, but citywide they may be a big issue. Designs that continue to work well when the network gets large are said to be scalable.

(3) Resource Allocation: Networks provide a service to hosts from their underlying resources, such as the capacity of transmission lines. To do this well, they need mechanisms that divide their resources so that one host does not interfere with another too much.

Statistical multiplexing: Many designs share network bandwidth dynamically, according to the short term needs of hosts. Thus sharing based on the statistics of demand is called statistical multiplexing.

Flow Control: An allocation problem that occurs at every level is how to keep a fast sender from swamping a slow receiver with data. Feedback from the receiver to the sender is often used.

Congestion: Sometimes the problem is that the network is oversubscribed because too many computers want to send too much traffic, and the network cannot deliver it all. This overloading of the network is called congestion.

Quality of service: It is interesting to observe that the network has more resources to offer than simply bandwidth. For uses such as carrying live video, the timeliness of delivery matters a great deal. Most networks must provide service to applications that want this real-time delivery at the same time that they provide service to applications that want high throughput.

(4) Security: secure the network by defending it against different kinds of threats. One of the threats we have mentioned previously is that of eavesdropping on communications.

Authentication: Mechanisms for authentication prevent someone from impersonating someone else.

Integrity: prevent surreptitious changes to messages, such as altering.

1.7.3 Connection-oriented and Connectionless Services

Connection-Oriented service:

The user first establishes a connection then uses the connection and then releases the connection. The sender transmits bits of information and the receiver takes them out in the same order as they were originally sent.

Connectionless Service

Each packet of information carries the full destination address and is routed independently from the others from the source to destination. Packets may take different routes to the destination and it is possible for two packets sent to the same destination the first one to send can be delayed and the second one arrives first. So care must be taken in order for the all the bits arrive correctly and in the same order they were sent.

1.8 NETWORK EXAMPLES

1.8.1 Internet

The Internet is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link billions of devices worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web(WWW), electronic mail, telephony, and peer-to-peer networks for file sharing.

Although the Internet protocol suite has been widely used by academia and the military industrial complex since the early 1980s, events of the late 1980s and 1990s

such as more powerful and affordable computers, the advent of fibre optics, the popularization of HTTP and the Web browser, and a push towards opening the technology to commerce eventually incorporated its services and technologies into virtually every aspect of contemporary life.

ARPANET

The Advanced Research Projects Agency Network (ARPANET) was an early packet switching network and the first network to implement the protocol suite TCP/IP. Both technologies became the technical foundation of the Internet. ARPANET was initially funded by the Advanced Research Projects Agency (ARPA) of the United States Department of Defence.

Packet switching—today the dominant basis for data communications worldwide—was a new concept at the time of the conception of the ARPANET. Prior to the advent of packet switching, both voice and data communications had been based on the idea of circuit switching, as in the traditional telephone circuit, wherein each telephone call is allocated a dedicated, end to end, electronic connection between the two communicating stations. Such stations might be telephones or computers.

The (temporarily) dedicated line is typically composed of many intermediary lines which are assembled into a chain that stretches all the way from the originating station to the destination station. With packet switching, a data system could use a single communication link to communicate with more than one machine by collecting data into datagram and transmitting these as packets onto the attached network link, as soon as the link becomes idle. Thus, not only can the link be shared, much as a single post box can be used to post letters to different destinations, but each packet can be routed independently of other packets.

NSFNET

The National Science Foundation Network (NSFNET) was a program of coordinated, evolving projects sponsored by the National Science Foundation(NSF) beginning in 1985 to promote advanced research and education networking in the United States.NSFNET was also the name given to several nationwide backbone networks that were constructed to support NSF's networking initiatives from 1985 to 1995. Initially created to link researchers to the nation's NSF-funded supercomputing centres, through further public funding and private industry partnerships it developed into a major part of the Internet backbone.

Architecture of Internet

Two ways to describe the Internet Architecture

- Network hardware and Software
- Networking Infrastructure that provides services to distributed applications

Host/End systems

Computing Devices such as PCs, PDAs, TVs, Server and Mobile Computers and automobiles connected to the internet is called as hosts/end systems.

Communication Links

End systems are connected together by communication link. Communication links are made up of different type of media including twisted pair cables, co-axial cable, fiber optics and radio spectrum.

Bandwidth

Different links can transmit data at different data rates. The link transmission rate is often called as bandwidth of the link which is measured in bits per second.

Routers

End systems are not directly connected to each other via single communication link. They are indirectly connected through switching devices called as routers. The routers receive the chunk information from one of the incoming communication link and forwards to the outgoing communication link.

Packets

The chunk of information is called packets

Route/Path

The path that the packet takes from the sending system through series of communication links and routers, to the end system is known as route/path.

Packet Switching

The internet uses a technique known as packet switching that allows multiple communicating end systems to share a path, or parts of the path at the same time.

Internet Service Providers (ISPs)

End systems access the internet through the ISPs. The different ISPs provide a variety of different types of network access to the end systems including 56Kbps dialup modem access, cable modem or DSL, high speed LAN access and wireless access.

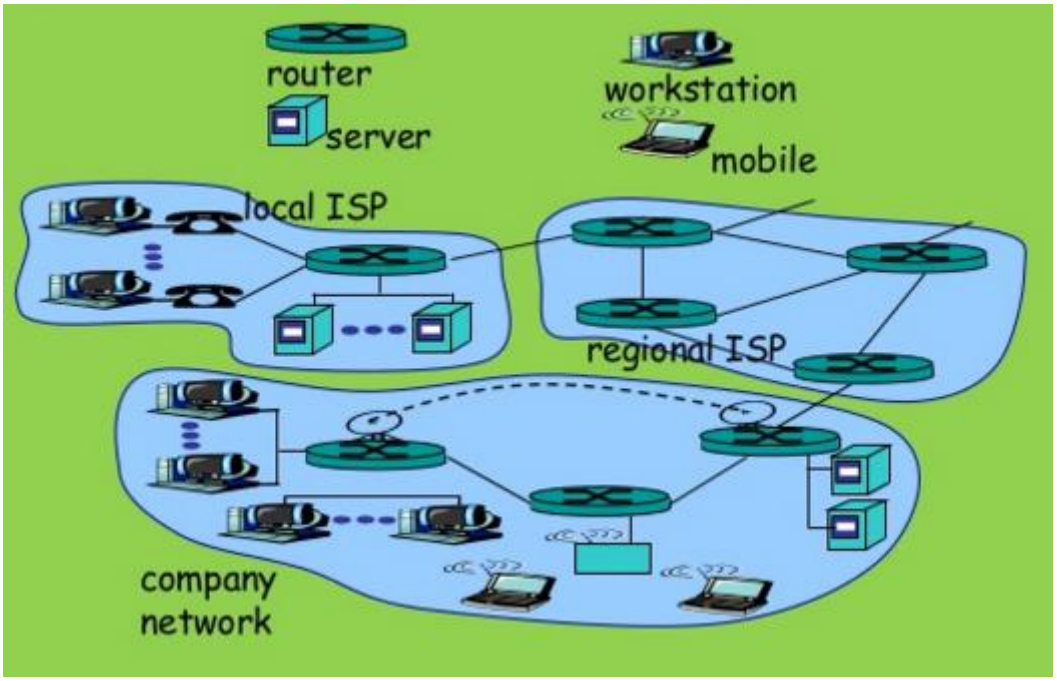


Figure 1.26 A piecewise architecture of Internet

Protocols

End systems, routers and other pieces of the Internet run protocols that control the sending and receiving of information within the Internet.TCP and IP are the two of the important Internet protocols. The Internets' principle protocol is collectively called as TCP/IP suite protocol.

Intranets

There are many private networks, such as many co-corporate and government networks whose host cannot exchange messages with host outside of the private network. These private networks are referred as intranets, as they use same type of hosts, routers, links and protocols as the public Internet.

Internet Standards

At the technical and developmental level, the Internet is made possible through creation, testing and implementation of Internet standards. These standards are developed by Internet Engineering Tasks Force (IETF).

RFCs

The IETFs standard documents are called as RFCs (Request for comments).RFCs started out as a general request for comments to resolve the architecture problems of the Internet. They define protocols such as TCP, IP, HTTP, and SMTP.

Service Oriented View:

Distributed Applications

The Internet allows distributed applications running on its end systems to exchange data with each other. These applications include remote login, electronic mail, web surfing, instant messaging, audio and video streaming, Internet telephony, gaming, peer-to-peer (P2P) file sharing and much more.

Communication services

Internet provides two services to its distributed applications

Connection Oriented Reliable service: It guarantees that data transmitted from a sender to receiver will eventually be delivered to the receiver in order.

Connectionless unreliable service: It does not make any guarantees about the eventual delivery.

Thus Internet is an infrastructure in which new applications are been constantly invented and deployed.

1.8.2 Mobile Phone Networks

The architecture of the mobile phone network has changed greatly over the past 40 years along with its tremendous growth.

First Generation: Transmitted voice calls continuously varying signals rather than sequences of digital bits. AMPS (Advanced Mobile Phone System) were the first generation system.

Second Generation: Switching to digital form of transmitting voice to increase capacity, improve security and offer text messaging.GSM (Global System for Mobile Communication) which was deployed in 1991 introduced the 2G system.

Third generation: The 3G systems were initially developed in 2001 and offer both digital voice and broadband digital services. UMTS (Universal Mobile Telecommunications System), also called WCDMA (Wideband Code Division Multiple Access), is the main 3G system that is being rapidly deployed worldwide. It can provide up to 14 Mbps on the downlink and almost 6 Mbps on the uplink. Future releases will use multiple antennas and radios to provide even greater speeds for users.

It is the scarcity of spectrum that led to the cellular network design shown in Fig. 1-30 that is now used for mobile phone networks. To manage the radio interference between users, the coverage area is divided into cells. Within a cell, users are assigned channels that do not interfere with each other and do not cause too much interference for adjacent cells. This allows for good reuse of the spectrum, or frequency reuse, in the neighboring cells, which increases the capacity of the network. In 1G systems, which carried each voice call on a specific frequency band, the frequencies were carefully chosen so that they did not conflict with neighboring cells. In this way, a given frequency might only be reused once in several cells. Modern 3G systems allow each cell to use all frequencies, but in a way that results in a tolerable level of interference to the neighboring cells. There are variations on the cellular design, including the use of directional or sectored antennas on cell towers to further reduce interference, but the basic idea is the same.

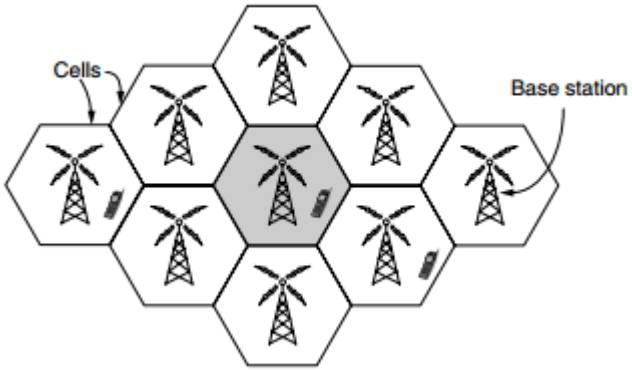


Figure 1.27 Cellular designs of mobile phone networks.

The architecture of the mobile phone network is very different than that of the Internet. It has several parts, as shown in the simplified version of the UMTS architecture in Fig. 1.28. First, there is the air interface. This term is a fancy name for the radio communication protocol that is used over the air between the mobile device (e.g., the cell phone) and the cellular base station. Advances in the air interface over the past decades have greatly increased wireless data rates. The UMTS air interface is based on Code Division Multiple Access (CDMA).

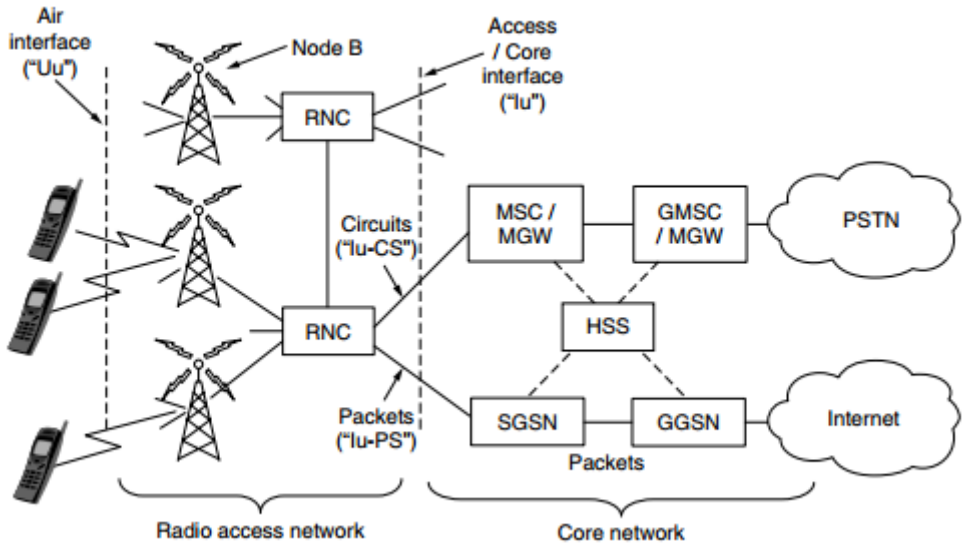


Figure 1.28 Architecture of the UMTS 3G mobile phone network.

The cellular base station together with its controller forms the radio access network. This part is the wireless side of the mobile phone network. The controller node or RNC (Radio Network Controller) controls how the spectrum is used. The base station implements the air interface. It is called Node B, a temporary label that stuck. The rest of the mobile phone network carries the traffic for the radio access network. It is called the core network. The UMTS core network evolved from the core network used for the 2G GSM system that came before it. However, something surprising is happening in the UMTS core network.

In a connectionless design, every packet is routed independently of every other packet. As a consequence, if some routers go down during a session, no harm will be done as long as the system can dynamically reconfigure itself so that subsequent packets can find some route to the destination, even if it is different from that which previous packets used.

With a connectionless network, if too many packets arrive at the same router at the same moment, the router will choke and probably lose packets. The sender will eventually notice this and resend them, but the quality of service will be jerky and unsuitable for audio or video unless the network is lightly loaded. Needless to say, providing adequate audio quality is something telephone companies care about very much, hence their preference for connections.

Older mobile phone networks used a circuit-switched core in the style of the traditional phone network to carry voice calls. This legacy is seen in the UMTS network with the MSC (Mobile Switching Center), GMSC (Gateway Mobile Switching Center), and MGW (Media Gateway) elements that set up connections over a circuit-switched core network such as the PSTN (Public Switched Telephone Network). Data services have become a much more important part of the mobile phone network than they used to be, starting with text messaging and early packet data services such as GPRS (General Packet Radio Service) in the GSM system. These older data services ran at tens of kbps, but users wanted more. Newer mobile phone networks carry packet data at rates of multiple Mbps. For comparison, a voice call is carried at a rate of 64 kbps, typically 3–4x less with compression. To carry all this data, the UMTS core network nodes connect directly to a packet-switched network. The SGSN (Serving GPRS Support Node) and the GGSN (Gateway GPRS Support Node) deliver data packets to and from mobiles and interface to external packet networks such as the Internet.

Another difference between mobile phone networks and the traditional Internet is mobility. When a user moves out of the range of one cellular base station and into the range of another one, the flow of data must be re-routed from the old to the new cell base station. This technique is known as handover or handoff

Figure 1.29 Mobile phone handover (a) Before (b) After

Either the mobile device or the base station may request a handover when the quality of the signal drops. In some cell networks, usually those based on CDMA technology, it is possible to connect to the new base station before disconnecting from the old base station. This improves the connection quality for the mobile because there is no break in service; the mobile is actually connected to two base stations for a short while. This way of doing a handover is called a soft handover to distinguish it from a hard handover, in which the mobile disconnects from the old base station before connecting to the new one

Starting with the 2G GSM system, the mobile phone was divided into a handset and a removable chip containing the subscriber's identity and account information. The chip is informally called a SIM card, short for Subscriber Identity Module. SIM cards can be switched to different handsets to activate them, and they provide a basis for security.

When GSM customers travel to other countries on vacation or business, they often bring their handsets but buy a new SIM card for few dollars upon arrival in order to make local calls with no roaming charges. To reduce fraud, information on SIM cards is also used by the mobile phone network to authenticate subscribers and check that they are allowed to use the network.

With UMTS, the mobile also uses the information on the SIM card to check that it is talking to a legitimate network. Another aspect of security is privacy. Wireless signals are broadcast to all nearby receivers, so to make it difficult to eavesdrop on conversations; cryptographic keys on the SIM card are used to encrypt transmissions. This approach provides much better privacy than in 1G systems, which were easily tapped, but is not a panacea due to weaknesses in the encryption schemes. Mobile phone networks are destined to play a central role in future networks. They are now more about mobile broadband applications than voice calls, and this has major implications for the air interfaces, core network architecture, and security of future networks. 4G technologies that are faster and better are on the drawing board under the name of LTE (Long Term Evolution), even as 3G design and deployment continues. Other wireless technologies also offer broadband Internet access to fixed and mobile clients, notably 802.16 networks under the common name of WiMAX. It is entirely possible that LTE and WiMAX are on a collision course with each other and it is hard to predict what will happen to them.

1.8.3 Wireless LANs: 802.11

802.11 networks are made up of clients, such as laptops and mobile phones, and infrastructure called APs (access points) that is installed in buildings. Access points are sometimes called base stations. The access points connect to the wired network, and all communication between clients goes through an access point. It is also possible for clients that are in radio range to talk directly, such as two computers in an office without an access point. This arrangement is called an ad hoc network. It is used much less often than the access point mode. Both modes are shown in Fig.1.30

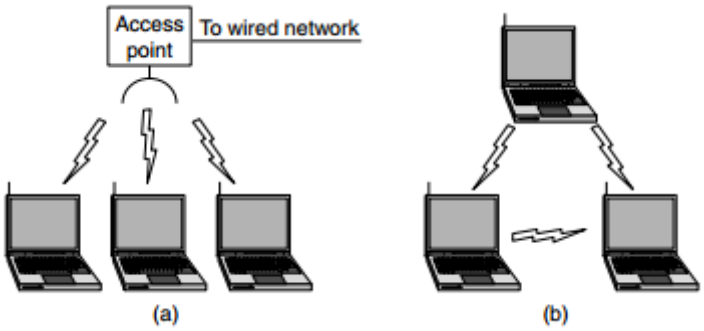


Figure 1.30 (a)Wireless Network with access point (b) Ad-hoc network

When two or more stations come together to communicate with each other, they form a Basic Service Set (BSS). The minimum BSS consists of two stations. 802.11 LANs use the BSS as the standard building block.

A BSS that stands alone and is not connected to a base is called an Independent Basic Service Set (IBSS) or is referred to as an Ad-Hoc Network. An ad-hoc network is a network where stations communicate only peer to peer. There is no base and no one gives permission to talk. Mostly these networks are spontaneous and can be set up rapidly. Ad-Hoc or IBSS networks are characteristically limited both temporally and spatially.

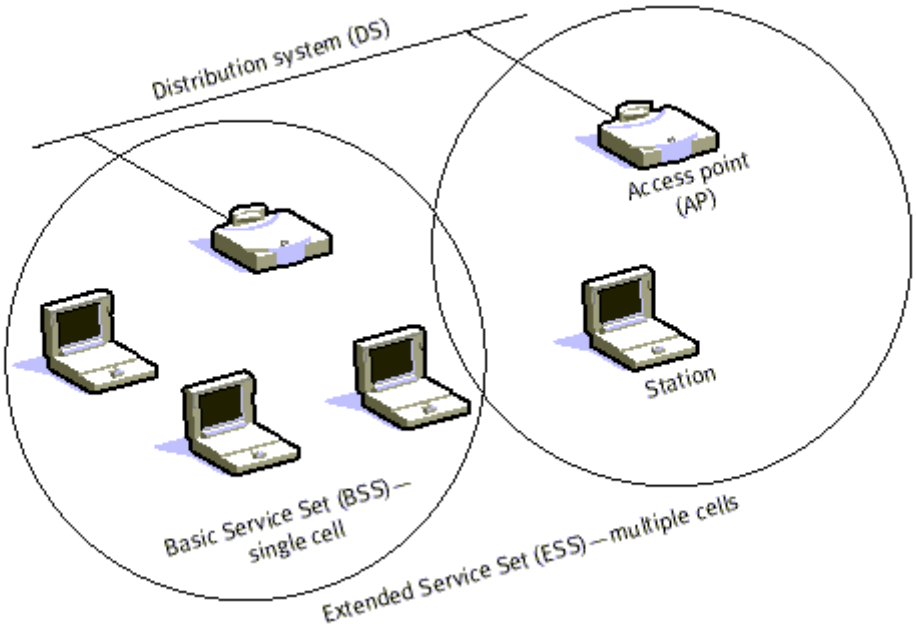


Figure 1.31 Infrastructure Mode

When BSS's are interconnected the network becomes one with infrastructure. 802.11 infrastructure has several elements. Two or more BSS's are interconnected using a Distribution System or DS. This concept of DS increases network coverage. Each BSS becomes a component of an extended, larger network. Entry to the DS is accomplished with the use of Access Points (AP). An access point is a station, thus addressable. So, data moves between the BSS and the DS with the help of these access points.

Creating large and complex networks using BSS's and DS's leads us to the next level of hierarchy, the Extended Service Set or ESS shown in Fig.1.31. The beauty of the ESS is the entire network looks like an independent basic service set to the Logical Link Control layer (LLC). This means that stations within the ESS can communicate or even move between BSS′s transparently to the LLC.

One of the requirements of IEEE 802.11 is that it can be used with existing wired networks. 802.11 solved this challenge with the use of a Portal. A portal is the logical integration between wired LANs and 802.11. It also can serve as the access point to the DS. All data going to an 802.11 LAN from an 802.X LAN must pass through a portal. It thus functions as bridge between wired and wireless.

The implementation of the DS is not specified by 802.11. Therefore, a distribution system may be created from existing or new technologies. A point-to-point bridge connecting LANs in two separate buildings could become a DS.
While the implementation for the DS is not specified, 802.11 does specify the services, which the DS must support. Services are divided into two sections

- Station Services (SS)
- Distribution System Services (DSS).

There are five services provided by the DSS

- Association
- Reassociation
- Disassociation
- Distribution
- Integration

The first three services deal with station mobility. If a station is moving within its own BSS or is not moving, the stations mobility is termed No-transition. If a station moves between BSS's within the same ESS, its mobility is termed BSS-transition. If the station moves between BSS's of differing ESS's it is ESS transition. A station must affiliate itself with the BSS infrastructure if it wants to use the LAN. This is done by Associating itself with an access point. Associations are dynamic in nature because stations move, turn on or turn off. A station can only be associated with one AP. This ensures that the DS always knows where the station is.

Association supports no-transition mobility but is not enough to support BSS-transition. Enter Reassociation. This service allows the station to switch its association from one AP to another. Both association and reassociation are initiated by the station. Disassociation is when the association between the station and the AP is terminated. This can be initiated by either party. A disassociated station cannot send or receive data. ESS-transition are not supported. A station can move to a new ESS but will have to reinitiate connections.

Distribution and Integration are the remaining DSS's. Distribution is simply getting the data from the sender to the intended receiver. The message is sent to the local AP (input AP), then distributed through the DS to the AP (output AP) that the recipient is associated with. If the sender and receiver are in the same BSS, the input and out AP's are the same. So the distribution service is logically invoked whether the data is going through the DS or not. Integration is when the output AP is a portal. Thus, 802.x LANs are integrated into the 802.11 DS.

Station services are:

- Authentication
- Deauthentication
- Privacy
- MAC Service Data Unit (MSDU) Delivery.

With a wireless system, the medium is not exactly bounded as with a wired system. In order to control access to the network, stations must first establish their identity. This is much like trying to enter a radio net in the military.
Before you are acknowledged and allowed to converse, you must first pass a series of tests to ensure that you are who you say you are. That is really all authentication is. Once a station has been authenticated, it may then associate itself. The authentication relationship may be between two stations inside an IBSS or to the AP of the BSS. Authentication outside of the BSS does not take place.

1.8.4 RFID and sensor network

Radio-frequency identification (RFID) is the wireless use of electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by electromagnetic induction from magnetic fields produced near the reader. Some types collect energy from the interrogating radio waves and act as a passive transponder. Other types have a local power source such as a battery and may operate at hundreds of meters from the reader. Unlike a barcode, the tag does not necessarily need to be within line of sight of the reader and may be embedded in the tracked object. RFID is one method for Automatic Identification and Data Capture

RFID tags are used in many industries, for example, an RFID tag attached to an automobile during production can be used to track its progress through the assembly line; RFID-tagged pharmaceuticals can be tracked through warehouses; and implanting RFID microchipsin livestock and pets allows positive identification of animals.

RFID tags can be either passive, active or battery-assisted passive. An active tag has an on-board battery and periodically transmits its ID signal. A battery-assisted passive (BAP) has a small battery on board and is activated when in the presence of an RFID reader. A passive tag is cheaper and smaller because it has no battery; instead, the tag uses the radio energy transmitted by the reader. However, to operate a passive tag, it must be illuminated with a power level roughly a thousand times stronger than for signal transmission. That makes a difference in interference and in exposure to radiation.

Tags may either be read-only, having a factory-assigned serial number that is used as a key into a database, or may be read/write, where object-specific data can be written into the tag by the system user. Field programmable tags may be write-once, read-multiple; "blank" tags may be written with an electronic product code by the user.

RFID tags contain at least two parts: an integrated circuit for storing and processing information, modulating and demodulating a radio-frequency (RF) signal, collecting DC power from the incident reader signal, and other specialized functions; and an antenna for receiving and transmitting the signal. The tag information is stored in a non-volatile memory. The RFID tag includes either fixed or programmable logic for processing the transmission and sensor data, respectively.

An RFID reader transmits an encoded radio signal to interrogate the tag. The RFID tag receives the message and then responds with its identification and other information. This may be only a unique tag serial number, or may be product-related information such as a stock number, lot or batch number, production date, or other specific information. Since tags have individual serial numbers, the RFID system design can discriminate among several tags that might be within the range of the RFID reader and read them simultaneously.

A **wireless sensor network (WSN**) (sometimes called a wireless sensor and actuator network , are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network

node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. A sensor network is shown in Fig.1.31.

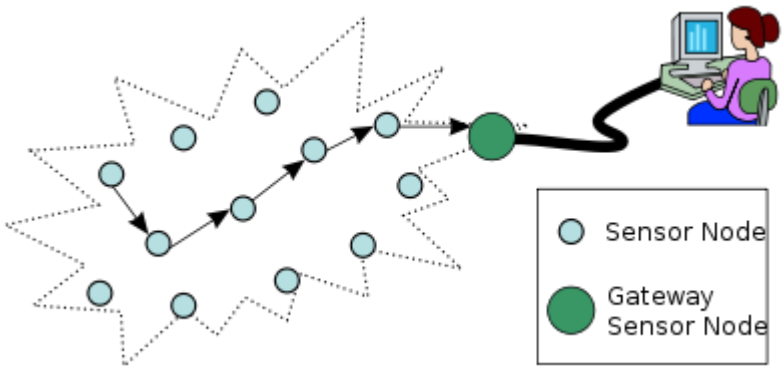


Figure 1.31 A typical multihop wireless sensor network

The application of WSN is as follows:

- Area Monitoring
- Health care Monitoring
- Environmental/earth sensing
    - Air pollution monitoring
    - Landslide detection
    - Water qulaity monitoring
    - Natural Disaster prevention
- Industrial Monitoring
    - Machine health monitoring
    - Data logging
    - Structural health monitoring

1.9 THE OSI MODEL:

The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust and interoperable.

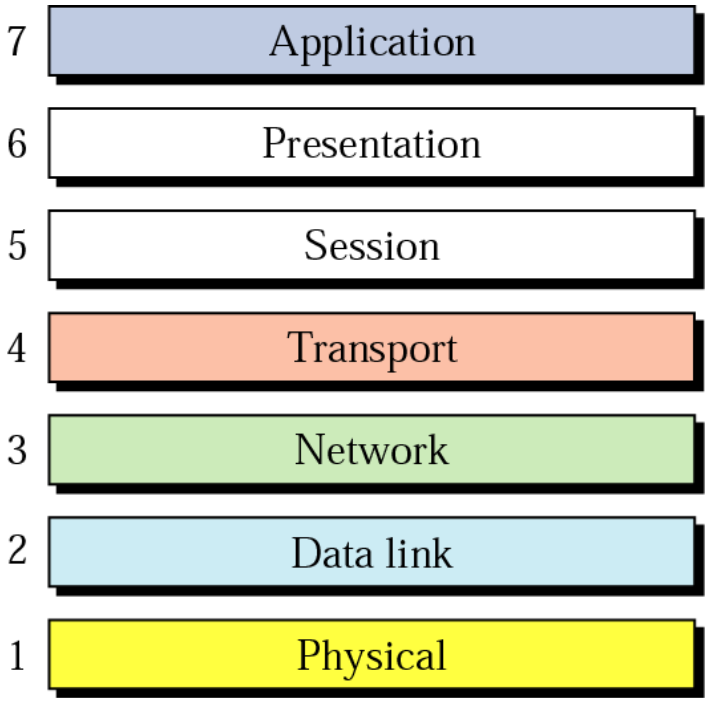


Figure 1.26 The seven layers of OSI model

The OSI model shown in fig.1.25 is based on the proposal developed by the International Standards Organization (ISO) as a first step towards international standardization of the protocols used in the various layers. The model is called the OSI (Open System Interconnection) reference model because it deals with connecting open systems, i.e., systems that are open for communication with other systems. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust and interoperable. The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network. The principles that were applied to arrive at the seven layers are as follows:

* A layer should be created where a different level of abstraction is needed.

* Each layer should perform a well-defined function.

* The function of each layer should be chosen with an eye toward defining internationally standardized protocols.

* The layer boundaries should be chosen to minimize the information flow across the interfaces.

* The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

1.9.1 Layered Architecture:

The OSI model is composed of seven layers: Physical, Data link, Network, Transport, Session, Presentation, Application layers. Fig 1.26 shows the layers involved when a message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes involve only the first 3 layers of the OSI model. Within a single machine, each layer calls upon the services of the layer just below it, layer 3 for ex. Uses the services provided by layer 2 & provides services for layer 4. Between machines, layer X on one machine communicates with layer X on another machine. This communication is governed by an agreed upon series of rules & Conventions called protocols. The processes on each machine that communicate at a given layer are called peer – to – peer processes. Communication between machines is therefore a peer – to –peer process using the protocols appropriate to a given layer.

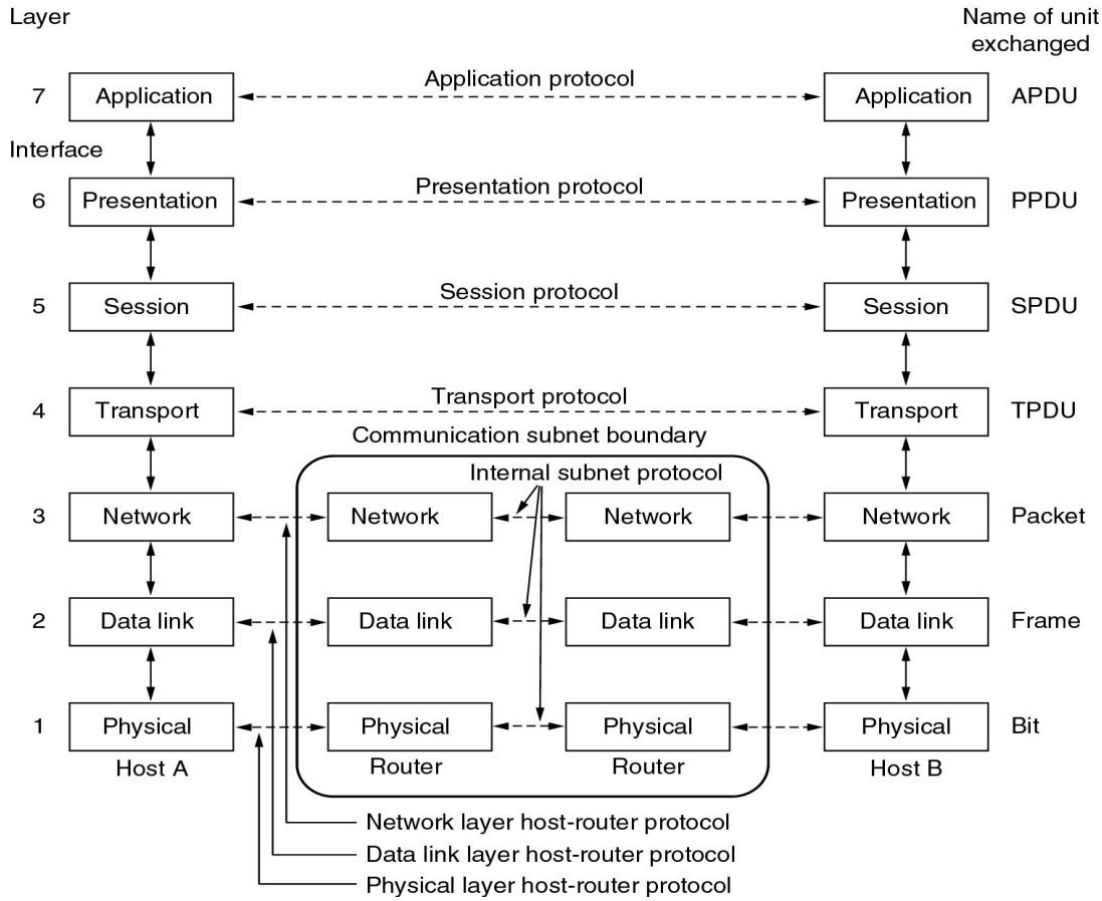


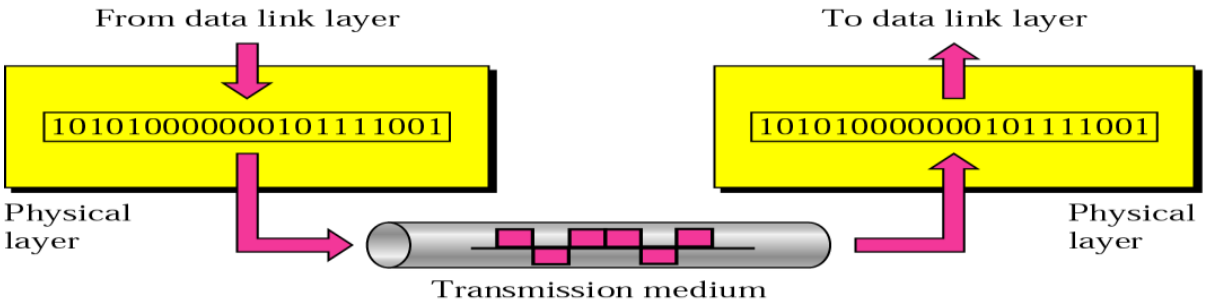
Figure 1.26 Interaction between the layers in the model

1.9.2 Layers in the OSI model:

i) Physical Layer:

The physical layer has as a main function to transmit bits over a communication channel as well as to establish and terminate a connection to a communications medium. It is also responsible to make sure that when one side sends a '1' bit the other side will receive '1' bit and not '0' bit.

Physical Layer is responsible for movements of individual bits from one node to the next

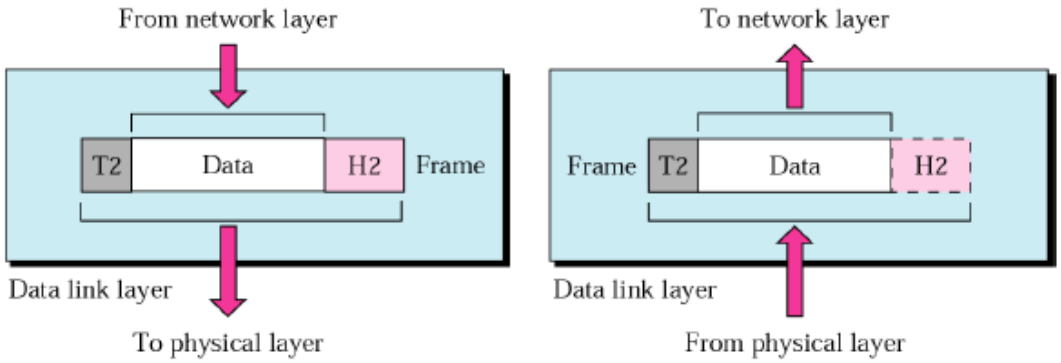


Physical characteristics of interfaces & medium, type of transmission medium.
• Representation of bits.
• Data rate.
• Synchronization of bits.
• Line configuration.
• Physical topology – Mesh, Star, Ring, Bus, Hybrid.
• Transmission mode – Simplex, Half-duplex, Full-duplex.

ii) Data Link Layer:

Data link layer provides means to transfer data between network entities. At the source machine it takes the bit streams of data from the Network Layer breaks into frames and passes them to the physical layer. At the receiving end data link layer detects and possibly corrects the errors that may occur during the transmission and passes the correct stream to the network layer. It's also concerned with flow control techniques.

Data link layer is responsible for moving frames from one node to the next.

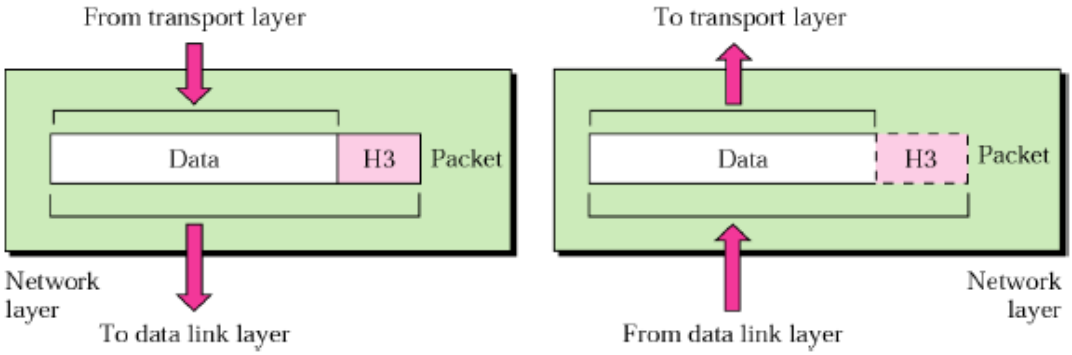


• Framing.
• Physical addressing.
• Flow control.
• Error control.
• Access control.

iii) Network Layer:

Network layer is responsible for the delivery of individual packets from the source host to the destination host.

This layer performs network routing, flow control and error control functions. Network routing simply means the way packets are routed from source to destination and flow control .prevents the possibility of congestion between packets which are present in the subnet simultaneously and form bottlenecks.

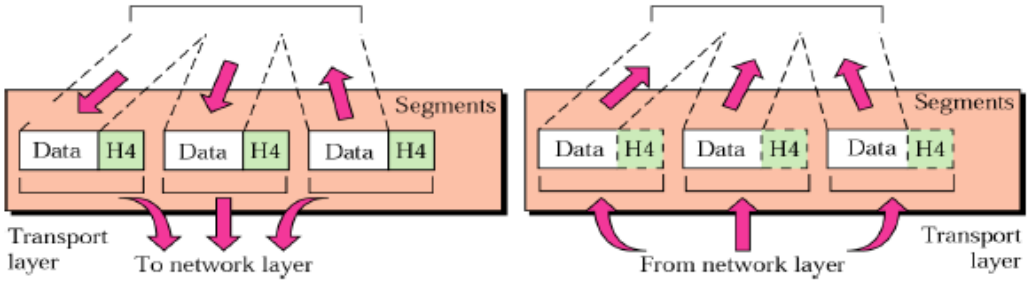


• Logical addressing.
• Routing.

iv) Transport Layer:

The Transport Layer has as a main task to accept data from the Session layer, split them up into smaller units and passes them to the Network layer making sure that all the pieces arrive correctly to the destination. It is the first end-to-end layer all the way from source machine to destination machine unlike the first three layers which are chained having their protocols between each machine. This is shown clearly in the diagram above.

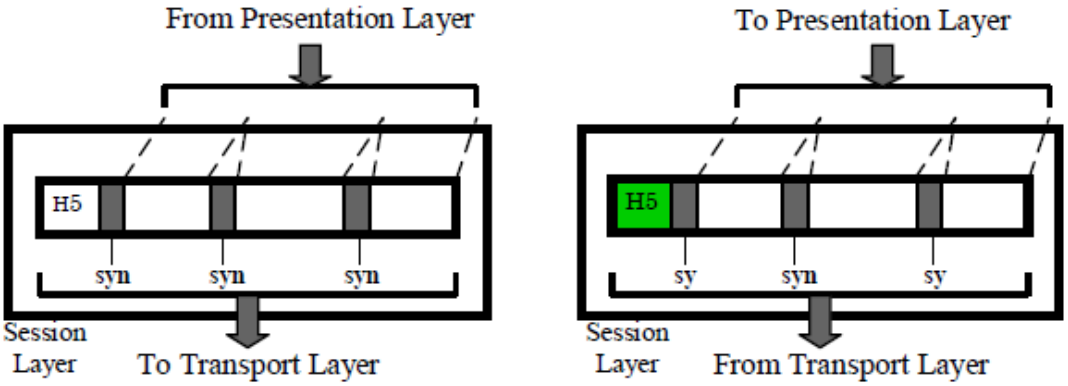
Transport layer is responsible for the delivery of a message from one process to another.



- Service-point addressing.
- Segmentation and reassembly.
- Connection control.
- Flow control.
- Error control.

v) Session Layer:

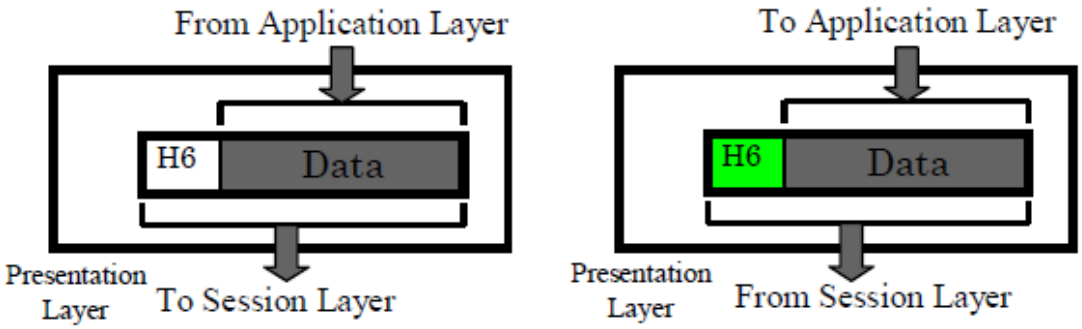
The session layer is responsible for dialog control and synchronization.



vi) Presentation Layer:

It is responsible to translate different data formats from the representation used inside the computer (ASCII) to the network standard representation and back. Computers use different codes for representing character strings so a standard encoding must be used and is handled by the presentation layer. Generally in a few words this layer is concerned

with the syntax and semantics of the information transmitted.

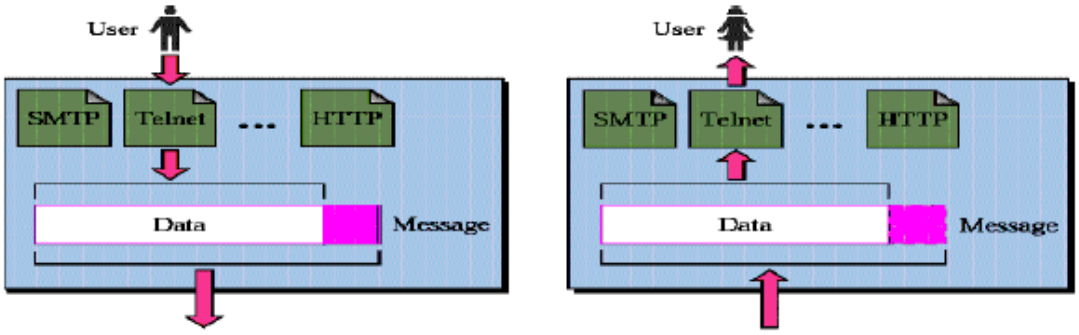


• Concerned with syntax and semantics of the information.
• Translation.
• Encryption.
• Compression.

vii) Application Layer:

The upper layer of this model performs common application service for the application processes meaning that software programs are written in the application layer to handle the many different terminal types that exist and map the virtual terminal software onto the real terminal. It contains a variety of protocols and is concerned with file transfer as well as electronic mail, remote job entry and various other services of general interest.

The Application layer is responsible for providing services to the user.



• Network virtual terminal.
• File transfer, access, and management.
• Mail services.
• Directory services.

1.10 TCP/IP Protocol suite:

The TCP/IP protocol suite has four layers as shown in figure 1.27.

- Host – to – Network
- Internet
- Transport
- Application.

Comparing TCP/IP to OSI model: the Host – to – Network layer is equivalent to the combination of physical and data link layers, the Internet layer is equivalent to the network layer, the Transport layer in TCP/IP taking care of part of the duties of the session layer, and the application layer is roughly doing the job of the session, presentation, & application layers.

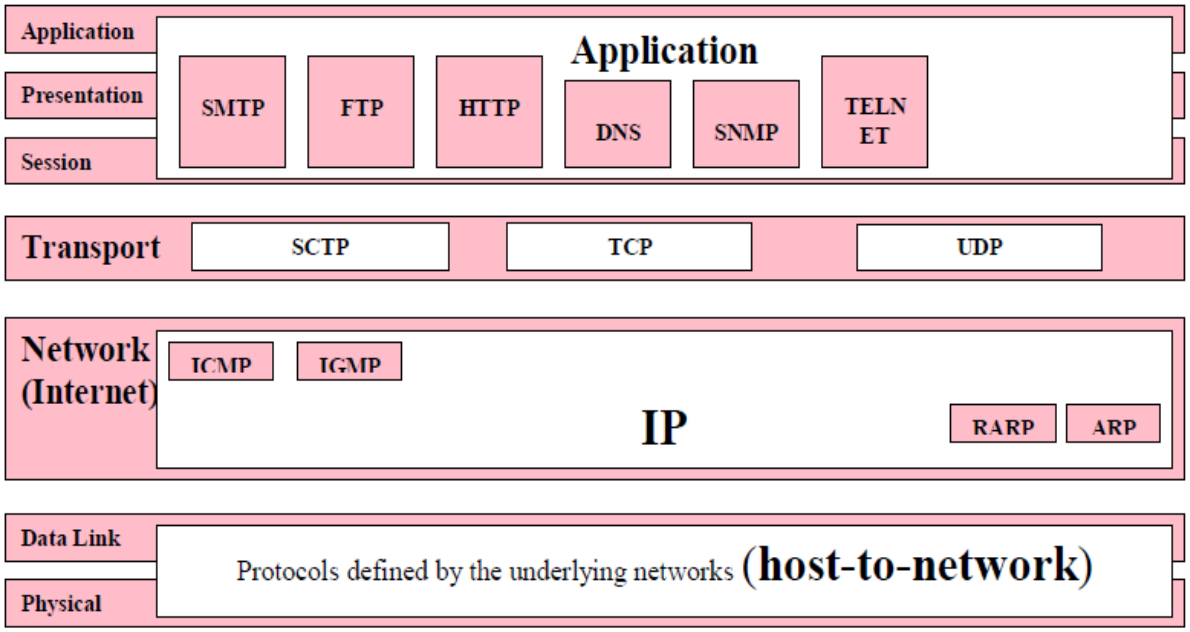


Figure 1.27 TCP/IP protocol suite

TCP/IP reference model was named after its two main protocols: TCP (Transmission Control Protocol) and IP (Internet Protocol). This model has the ability to connect multiple networks together in a way so that data transferred from a program in one computer are delivered safely to a similar program on another computer. The four layers are discussed as follows

(i) Host-to-Network Layer: It translates data and addresses information into format appropriate for an Ethernet Network or Token Ring Network. It uses a protocol (not specified due to lack of information concerned with this layer) in order for the host to connect to the network. Through this layer communication is achieved with physical links such as twisted pair or fiber optics carrying 1's and 0's.

(ii) Internet Layer: This layer is a connectionless internetwork layer and defines a connectionless protocol called IP. Its concerned with delivering packets from source to destination. These packets travel independently each taking a different route so may arrive in a different order than they were send. Internet layer does not care about the order the packets arrive at the destination as this job belongs to higher layers.

(iii) Transport Layer: It contains two end-to-end protocols. **TCP** is a connection oriented protocol and is responsible for keeping track of the order in which packets are sent and reassemble arriving packets in the correct order. It also ensures that a byte stream originating on one machine to be delivered without error on any other machine on the internet. The incoming byte stream is fragmented into discrete messages and is passed to the internet layer. With an inverse process, at the destination, an output stream is produced by reassembling the received massage.

(iv) UDP is the second protocol in this layer and it stands for User Datagram Protocol. In contrast to TCP, UDP is a connectionless protocol used for applications operating on its own flow control independently from TCP. It is also an unreliable protocol and is widely used for applications where prompt delivery is more important than accurate delivery such as transmitting speech or video.

(v) Application Layer: Is the upper layer of the model and contains different kinds of protocols used for many applications. It includes virtual terminal, TELNET for remote accessing on a distance machine, File Transfer Protocol FTP and e-mail (SMTP). It also contains protocols like HTTP for fetching pages on the www and others.

1.10.1 Addressing:

Four levels of addresses are used in an internet employing the TCP/IP Protocols shown in figure 1.28

i) Physical addresses
ii) Logical addresses
iii) Port addresses
iv) Specific addresses

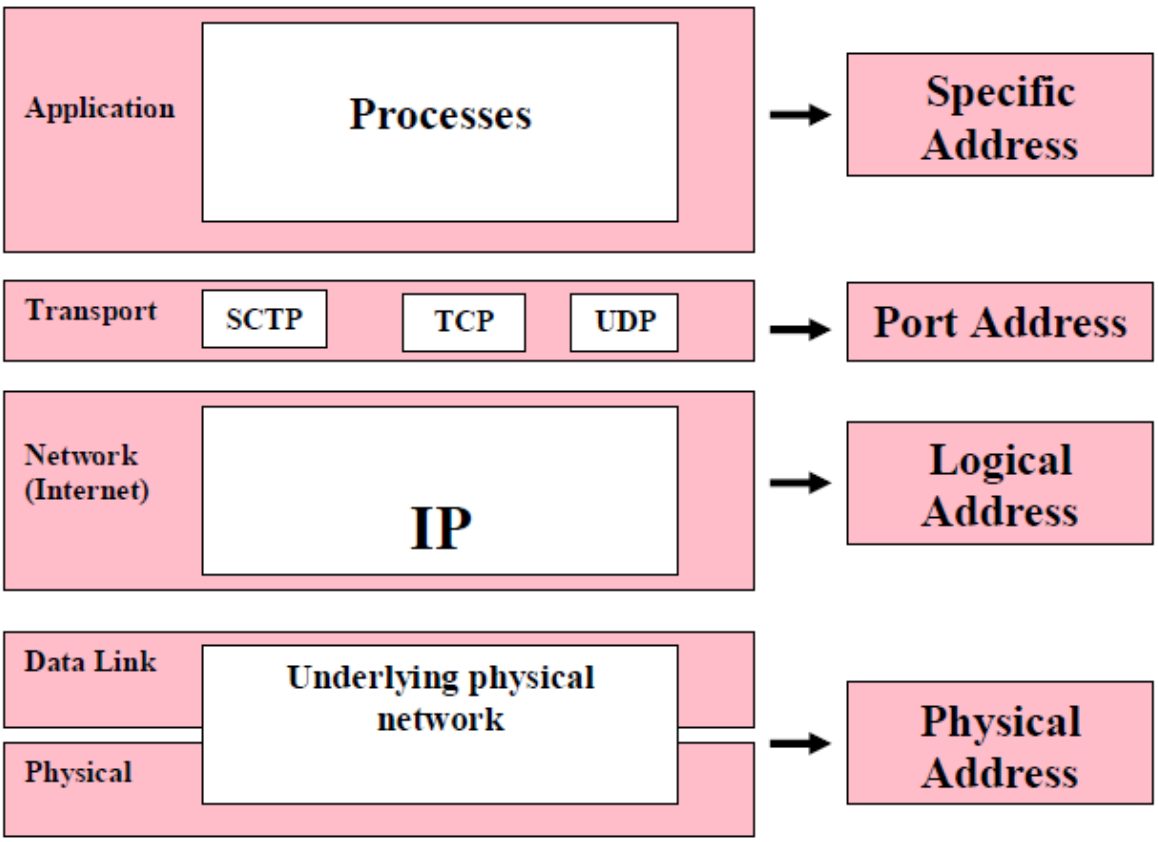


Figure 1.28 Four level of addressing schemes

1.11 World Wide Web (WWW)

The World Wide Web (WWW) is an open source information space where documents and other web resources are identified by URLs, interlinked by hypertextlinks, and can be accessed via the Internet. It has become known simply as the Web. The World Wide Web was central to the development of the Information Age and is the primary tool billions of people use to interact on the Internet.

Web pages are primarily text documents formatted and annotated with Hypertext Markup Language (HTML). In addition to formatted text, web pages may containimages, video, and software components that are rendered in the user's web browser as coherent pages of multimedia content. Embedded hyperlinks permit users to navigate between web pages. Multiple web pages with a common theme, a common domain name, or both, may be called a website. Website content can largely be provided by the publisher, or interactive where users contribute content or the content depends upon the user or their actions. Websites may be mostly informative, primarily for entertainment, or largely for commercial purposes.

The terms Internet and World Wide Web are often used without much distinction. However, the two are not the same. The Internet is a global system of interconnected computer networks. In contrast, the World Wide Web is one of the services transferred over these networks. It is a collection of text documents and other resources, linked by hyperlinks and URLs, usually accessed by web browsers, from web servers

1.12 Multimedia

Multimedia is content that uses a combination of different content forms such as text, audio, images, animation, video and interactive content. Multimedia contrasts with media that use only rudimentary computer displays such as text-only or traditional forms of printed or hand-produced material.

Multimedia can be recorded and played, displayed, dynamic, interacted with or accessed by information content processing devices, such as computerized and electronic devices, but can also be part of a live performance. Multimedia devices are electronic media devices used to store and experience multimedia content. Multimedia is distinguished from mixed media in fine art; by including audio, for example, it has a broader scope. The term "rich media" is synonymous for interactive multimedia. Hypermedia scales up the amount of media content in multimedia application.

1.12.1 Categorizations:

Multimedia may be broadly divided into linear and non-linear categories. Linear active content progresses often without any navigational control for the viewer such as a cinema presentation. Non-linear uses interactivity to control progress as with a video game or self-paced computer based training. Hypermedia is an example of non-linear content.

Multimedia presentations can be live or recorded. A recorded presentation may allow interactivity via a navigation system. A live multimedia presentation may allow interactivity via an interaction with the presenter or performer.

1.12.2 Characteristics of multimedia

Multimedia presentations may be viewed by person on stage, projected, transmitted, or played locally with a media player. A broadcast may be a live or recorded multimedia presentation. Broadcasts and recordings can be either analog or digital electronic media technology. Digital online multimedia may be downloaded orstreamed. Streaming multimedia may be live or on-demand.

Multimedia games and simulations may be used in a physical environment with special effects, with multiple users in an online network, or locally with an offline computer, game system, or simulator.

The various formats of technological or digital multimedia may be intended to enhance the users' experience, for example to make it easier and faster to convey information.