وزارة التعليم العالي والبحث العلمي

الجامعة المستنصرية

شبكات الحاسوب

Computer Network

3.500

نظري

علوم الحاسبات

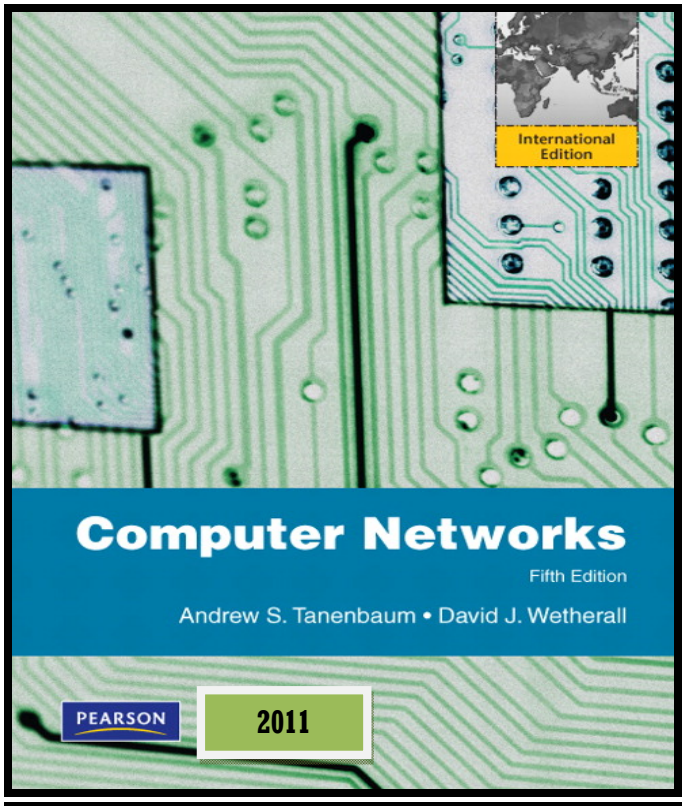
المرحلة الرابعة

مع تحيات ...

2014 - 2015

MUSTANSARYIAH UNIVERSITY

COLLEGE OF SCIENCES – DEPARTMENT OF CS



Computer Networks

® شبكات الحاسوب ®

DR. Bashar M. Ne'ma

2013-2014

Chapter 1

Introduction to Computer Networks

1-1 Introduction

This chapter defines the concept of computer networks, its components, functions, applications and others.

1-2 Definition of Computer Network

A computer network is a set of computers connected together via a data communication sub network for the purpose of sharing resources as shown in figure 1.1.

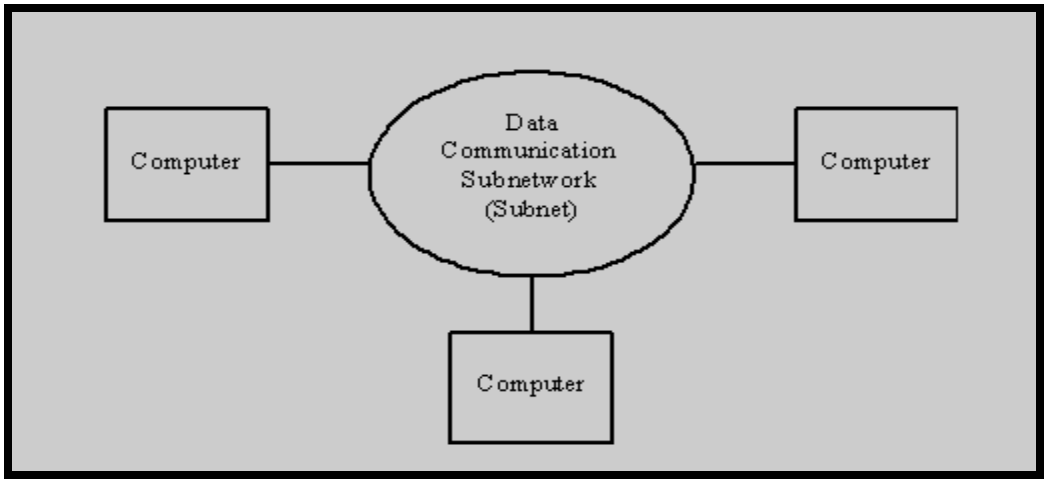


Figure 1.1 General Scheme of Computer Network

From this definition, we conclude that the main components of computer network are:

1- Computers: These are the objective devices of the network as they contain the main resources to be shared between them. The resources include hardware and software components such as: CPU, Memory, Storage, Files, Programs, Data bases, I/O devices, etc. It should be noted that the computers are usually called "hosts" and some of them can be replaced by other DTE (Data Terminal Equipment) devices such as: Printers, Scanners, Plotters, disk storage, etc. Also, the host itself is considered to be a DTE device.

2- Data Communication Subnetwork: This is responsible of transferring data between the different computers of the network. The structure of the subnet can be simple as in the case of small networks or can be complicated in case of large networks. The subnet, generally, contains; communication media, switches, routers, modems, etc.

3- Network Operating Software(NOS): This is a set of programs that controls all the components of the network. In each computer, there is a NOS and also in the switches and routers. The NOS can be an integral part of the device OS or as an independent part that can be added to the OS. the NOS is the most important part of a computer network as it is responsible of safe and secure transmission of data between computers and also of sharing the different resources so that the objectives of the computer network are realized.

1-3 Block Diagram of Computer Network

A more detailed block diagram can be drawn as in figure 1.2. In this diagram, we notice the following:

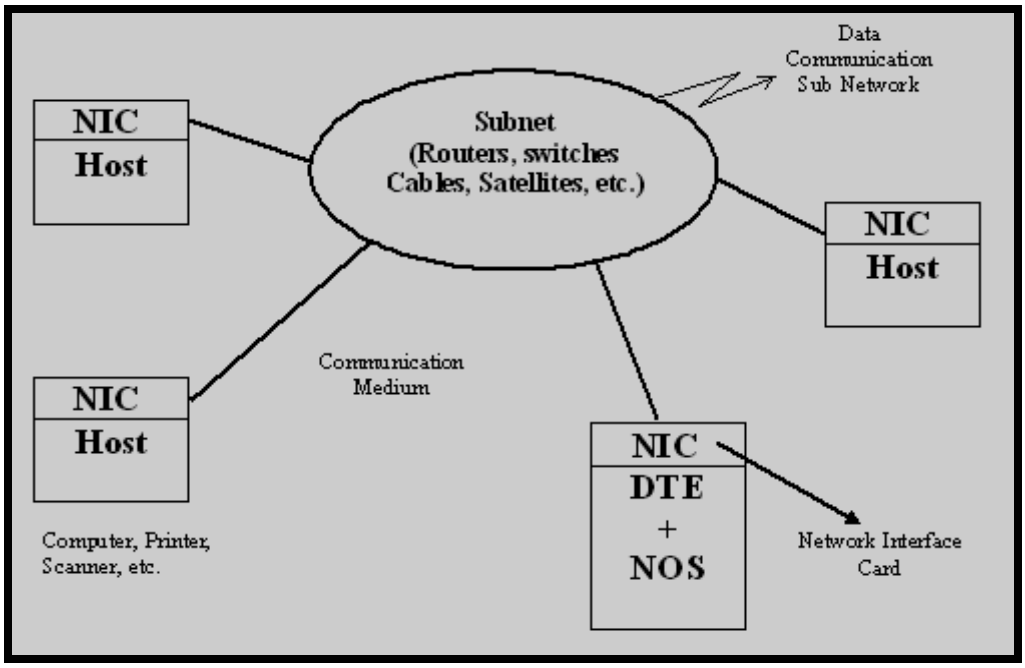


Figure 1.2 Block Diagram of Computer Network

1- **DTE can be computer, printer, scanner, etc.**
2- **NIC is necessary to connect any DTE to the subnet via a proper communication media.**
3- **NOS is present everywhere in the network as it is the main coordinator of its operation.**
4- **Subnet may include complicated communication devices such as: satellites, routers, optical fibers, wireless devices, telephone networks, etc.**

1-4 Topologies of Computer Networks

There are many topologies depending on the occupied area by the network, type of transmission medium, etc. The main configurations are as follows:

1-4-1 Linear (BUS) Network:

This is shown in figure 1.3 and has the following properties:

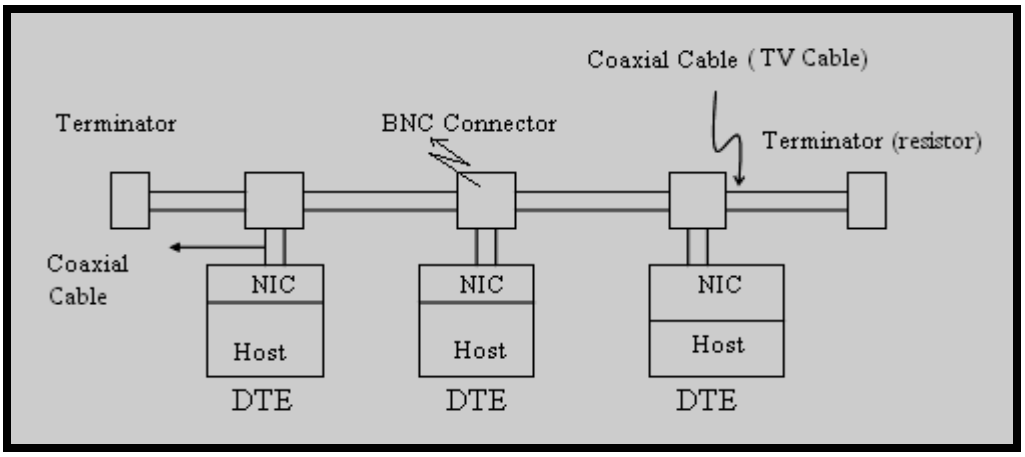


Figure 1.3 Linear Computer Network (LAN)

- **The occupied area is small and hence it is considered to be of type LAN i.e. Local Area Network.**
- **The data Communication subnet is very simple as it consists of TV cables and BNC connectors.**

- **Any signal transmitted from one host is received by all and hence it is necessary to prevent two hosts or more from transmitting simultaneously.**

1-4-2 Star Network:

This shown in figure 1.4 and has the following properties:

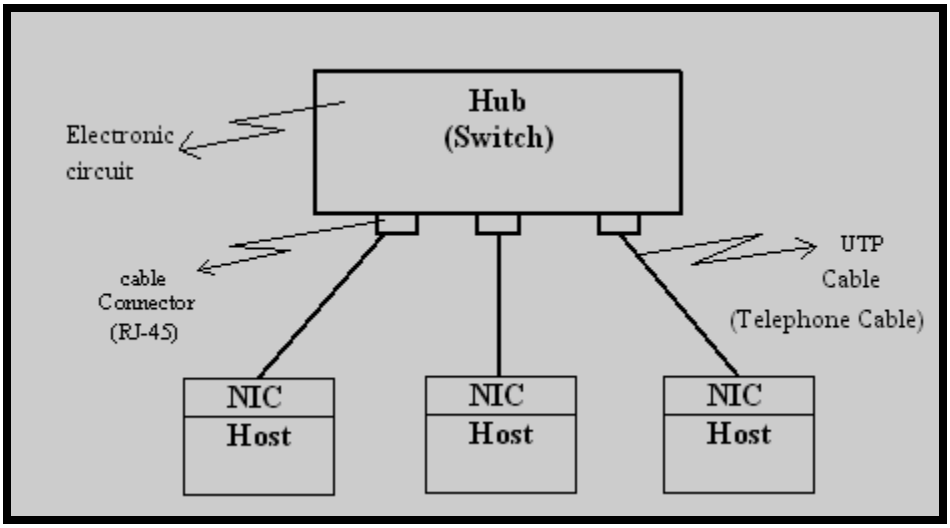


Figure 1.4 Star Network (LAN)

- **Occupied area is small and hence it is a LAN.**
- **Any host can be disconnected at any time without stopping the system (network).**
- **Subnet consists of electronic circuit and telephone cables of type UTP (Unshielded Twisted Pair).**

1-4-3 WAN Network:

The Wide Area Network occupies large area. The main component of this network is the "Router" as shown in figure 1.5.

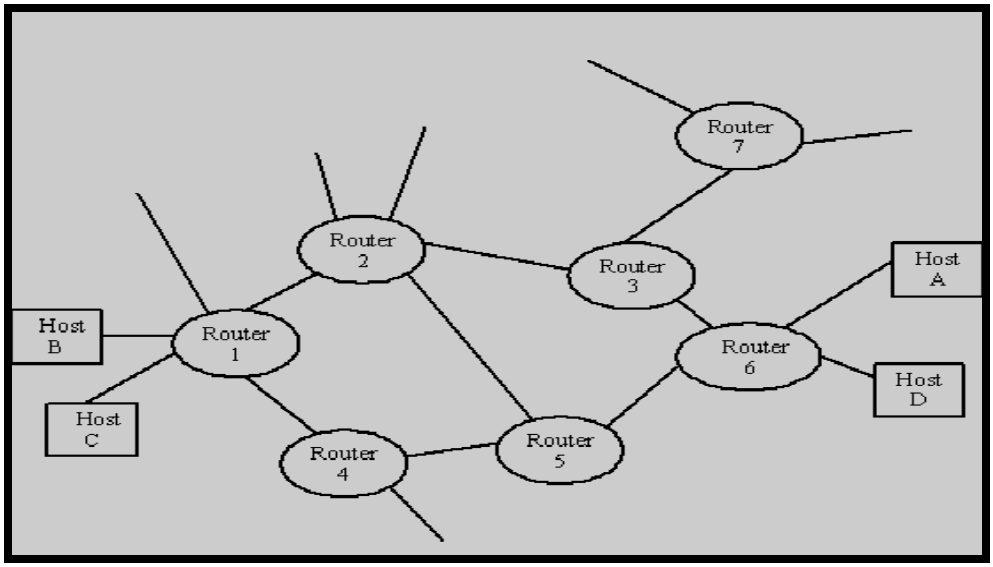


Figure 1.5 WAN Network

In this figure, we should note the following:

1. **The Router is usually a special computer i.e. dedicated computer for certain application.**
2. **Any router can be connected to other routers and host computers.**
3. **The data from host to host can travel in different paths which are determined by the routers according to "routing algorithms".**
4. **Each Router has proper NOS but does not have application programs or data.**
5. **The Routers can be in distant places and connected together by a proper communication medium.**
6. **The data communication subnet is a complicated structure of routers and communication media.**

1-4-4 Other Topologies:

There are many other topologies that will be studied in due time.

1-5 Network Application Programs:

In addition to NOS, each host has to have proper application programs that make use of the computer network; otherwise, the network would be, almost, useless. Some application programs are:

- **Internet browsers e.g. Microsoft Internet Explorer.**
- **Email programs e.g. Microsoft Outlook.**
- **Server programs that are available in some hosts to enable them to provide services to other hosts. A good example is a "Web server program" that sends web pages to users upon their requests.**

1-6 Application of Computer Networks:

The applications of computer networks are very wide starting from local laboratory to international level as the case of "Internet" network. The applications can be classified into main categories:

1-6-1 Peer to Peer Applications:

In this case, the hosts are similar in importance and they can share files and printers i.e. files can be transferred from one host to another according to sharing security policy assigned to each host by its user.
The hosts can be grouped together so that the access rights differ from one group to another. An example of grouping is the "workgroup" implemented in "windows".

1-6-2 Client-Server Application:

These are very popular where some hosts are equipped with proper hardware and software so that they become capable of providing services to other hosts. The hosts providing the services are called "Servers" and the others are called "Clients" some examples are:

1- **Web Service:** the server holds a lot of web pages that can be delivered to clients upon their requests as shown in figure 1.6.

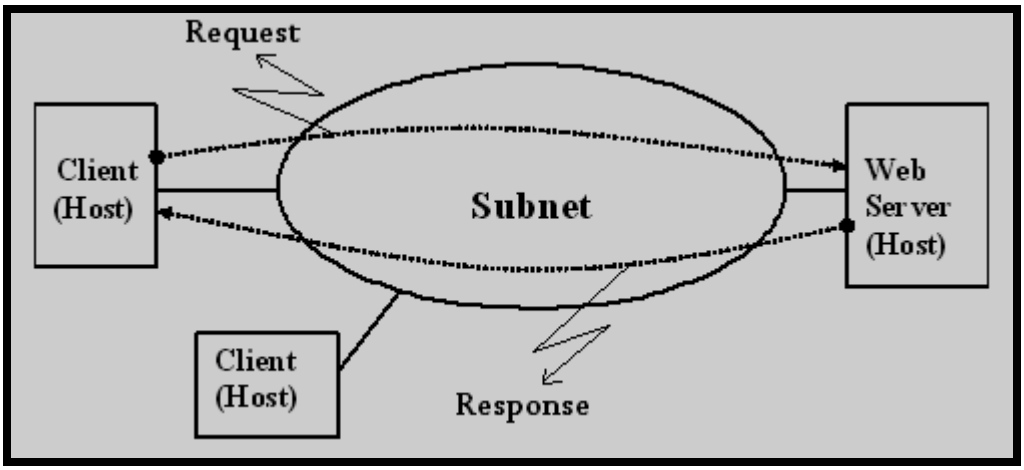


Figure 1.6 Web Service

2- **Email Service:** it is similar to Web service but instead of "Web Server" we use "Email Server".

3- **Chat service:** The server here is called "chat server".

4- **Database Service:** The server holds a proper data base controlled by a proper database management system "DBMS program". This server can provide services to clients as the case of "Al-Isra students' registration system".

5- **Banking System**
6- **Library system**
7- **Many others**

1-7 Classifications of Computer Networks:

The classification can be done in different ways according to the chosen criteria which can be: occupied area, topology, and transmission media.

1-7-1 Classifications Based on Occupied Area:

The area occupied by the network may vary from a small room, to the whole world; therefore, we have the following classes:

1- Local Area Network (LAN): This network has small dimensions as it occupies a room, floor, building, campus (i.e. several buildings). An example of this is the networks available in Al-ISRA University laboratories and buildings. The main LAN features are: High speed and low cost. The speed can be 1000 Mbps (Mega bit per second).

Note: To appreciate the speed, let us calculate how many books can be transferred between two computers in one second. Suppose that the book consists of 500 pages of text. Suppose each page includes:

40 lines * 80 characters = 3200 characters.

If the character is coded as one byte, then the whole book size will be coded as:

500 * 3200 * 8= 12.800.000 bits

This mean that the book is about 13 Mbits and hence it is possible to transfer (1000 / 13) books per second i.e. about 80 book/second.

2- Wide Area Network (WAN): The occupied area ranges from one county to the whole world. The main features are: low speed, high cost, use of routers, and use of complicated communication systems. The best example of WAN is the "Internet".

3- Metropolitan Area Network (MAN): The occupied area is one city and the features are between LAN and MAN.

1-7-2 Classifications Based on Topology:

This has been explained earlier.

1-7-3 Classifications Based on Transmission Media:

The transmission media used in building the network can be wires or wireless. The wires can be coaxial cables, UTP, Optical fibers.

The wired networks have been shown earlier when studying the topologies. The wireless networks may use infrared wave or radio waves. Some examples of wireless network are shown in figure 1.7.

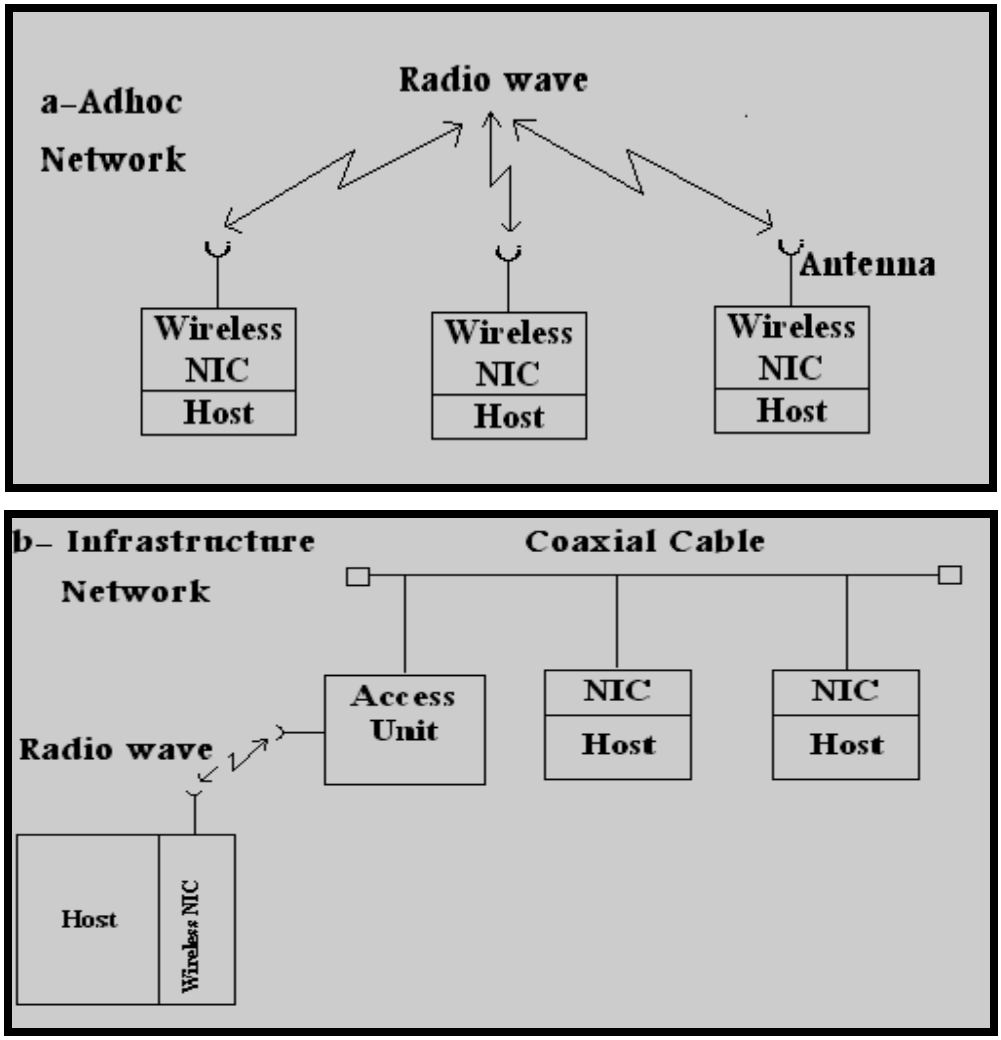


Figure1.7 Wireless Networks

1-8 Design of Computer Networks:

This includes hardware and software design. The network hardware includes all the electronic component, cables, connectors, radio waves, electrical signals, etc. All the hardware is usually called "physical layer" and normally designed by communication and computer engineers. The physical layer will be discussed later in more details.

The network software is usually called "Network Operating System NOS". The NOS design is a complicated task and hence it is divided into several parts and each part is implemented by a proper program. The popular name for NOS parts are "Layers", hence, it is right to say that the network layers are several programs exchanging data in already specified manner.

From the above discussion, we conclude that the computer network consists of layers as shown in figure 1.8. The design issues of these layers will be discussed later.

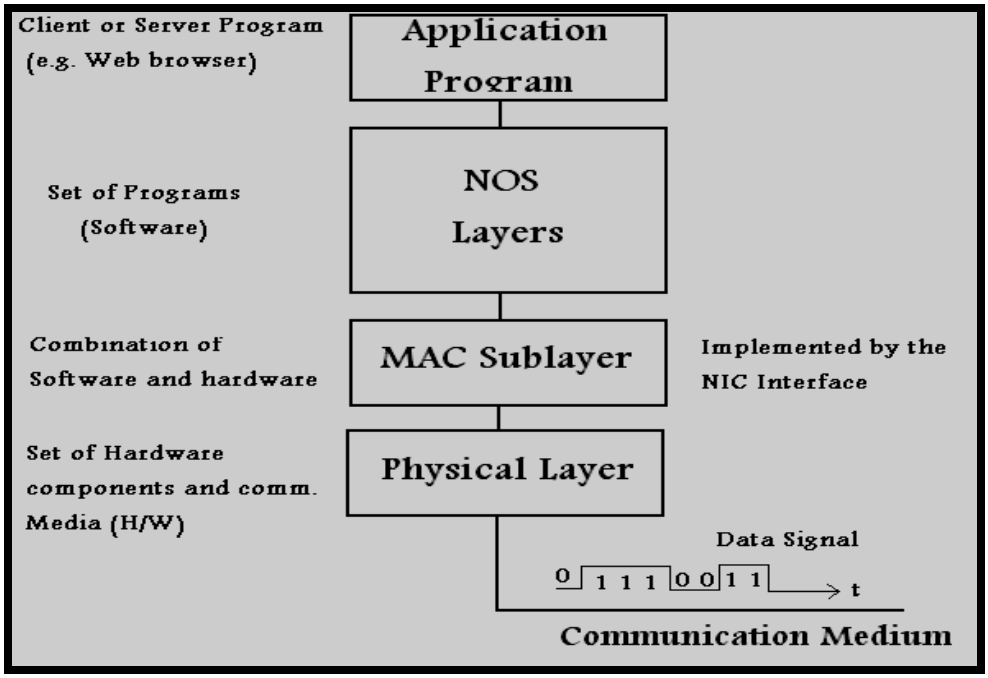


Figure 1.8 Network layers in Network Devices (Host, Router, Switch, etc.)

1-9 Computer Network Standards:

The popularity of computers networks resulted in the presence of network standards adopted by organizations and manufacturers. Some examples of these standards are:-

1- **TCP/IP: Used in Internet and can be used in LANS.**
2- **Ethernet: Used in Linear and Star LANs.**
3- **Token Ring: Used in ring LANs.**
4- **OSI: Adopted by ISO as guidelines for Network design.**
5- **Many Others: X.25, ATM, ISDN, etc.**

Chapter 2

Basics of Data Communication Systems

2-1 Introduction

As we have seen earlier, the data communication subnet is the core of computer network; therefore, it is necessary to study some communication basics as shown below.

2-2 Concept of Signal

A signal is parameters that may change its value with time e.g. voice, sound, current, voltage, scanned picture. The signal is represented as a function of time as shown below:

1- DC signal: It is characterized by a constant value for its amplitude as shown in figure 2.1. A good example of this signal is a battery voltage.

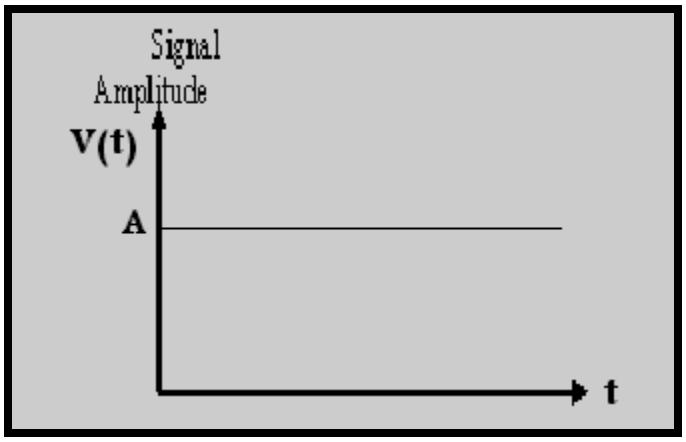


Figure 2.1 DC Signal, V (t) = A

2- AC signal: The signal amplitude changes with time in a periodic fashion and can be represented by a sinusoidal function as shown in figure 2.2.

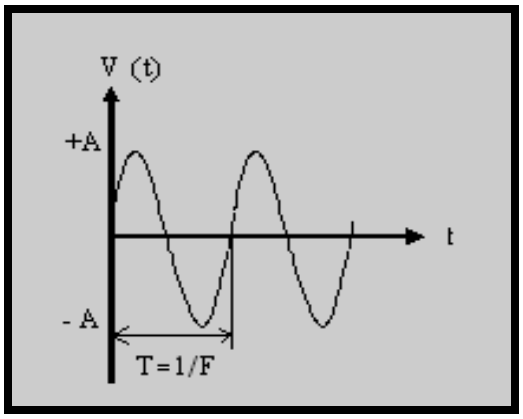


Figure 2.2 AC signal, V (t) = A sin (2π Ft)

The main parameter of this signal is its frequency F which represents the number of cycles per unit time. If the unit time is a "second" then F is measured in hertz "HZ". The AC signal is also called "sinusoidal signal". Example: AC mains volt.

3- Binary Signal: This signal has two values only as shown in figure 2.3. To make this signal carry data, it is necessary to specify a certain duration called "bit interval". If the bit interval is T then the data rate is 1/T which represents the number of bits per unit time (second). The "data rate" is also called a" bit rate". A good example is the signal sent by computer to a "Modem".

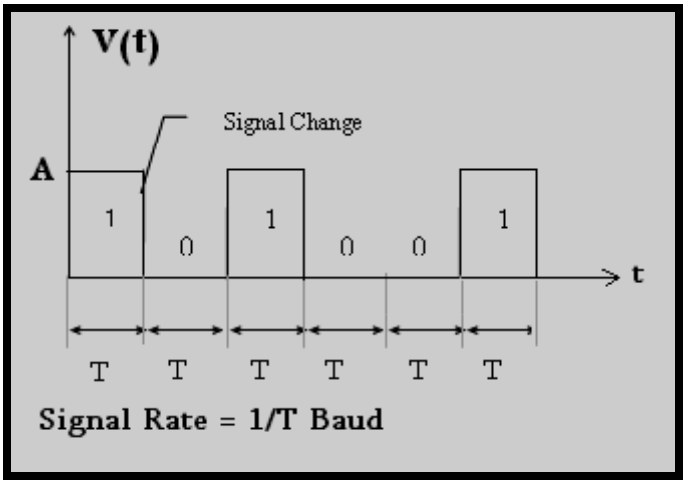


Figure 2.3 Binary Signal

4- General Analog Signal: This signal changes its amplitude in non-defined manner as shown in figure 2.4. A good example of this is the voice signal.

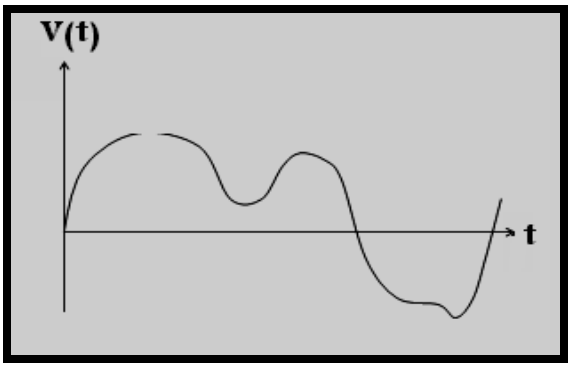


Figure 2.4 General Analog Signal.

2-3 Fouier Theorm

A scientist called "Fourier" proved mathematically that any signal is equivalent to a number of sinsoidal signals with frequencies ranging from F_{min} to F_{max} as shown in figure 2.5. The frequnency range is called Band Width "BW".

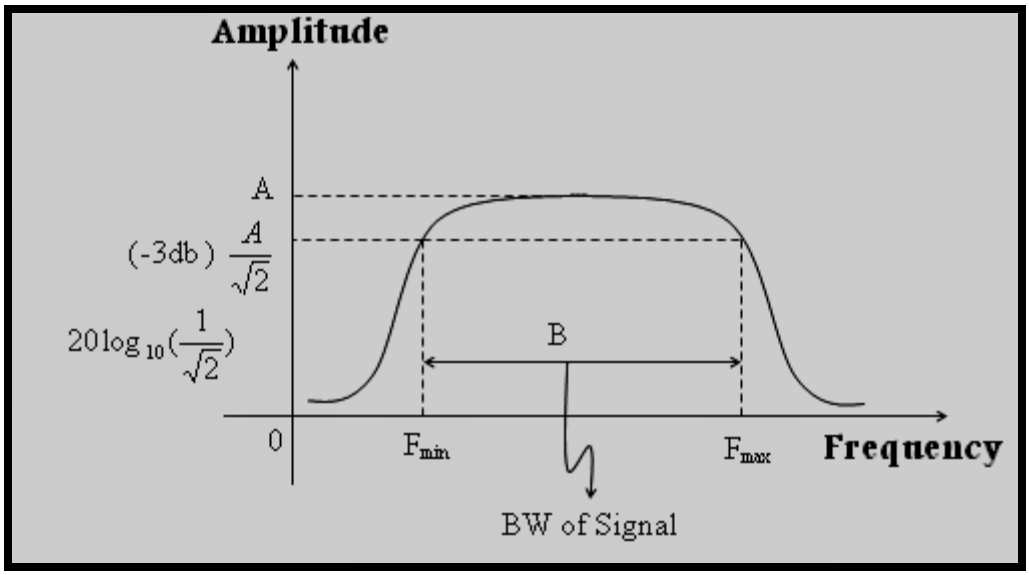


Figure 2.5 BW of signal

Example: suppose that we have a signal which is equivalent to:

V (t) = 5 sin (2π * 1000t) + 6 sin (2π * 2000t) + 7 sin (2π * 3000t) + 6 sin (2π * 4000t) + 4 sin (2π * 5000t)

It is clear that this signal consists of five sinusoidal signals called "Frequency Components" or simply "Frequencies" as shown in figure 2.6.

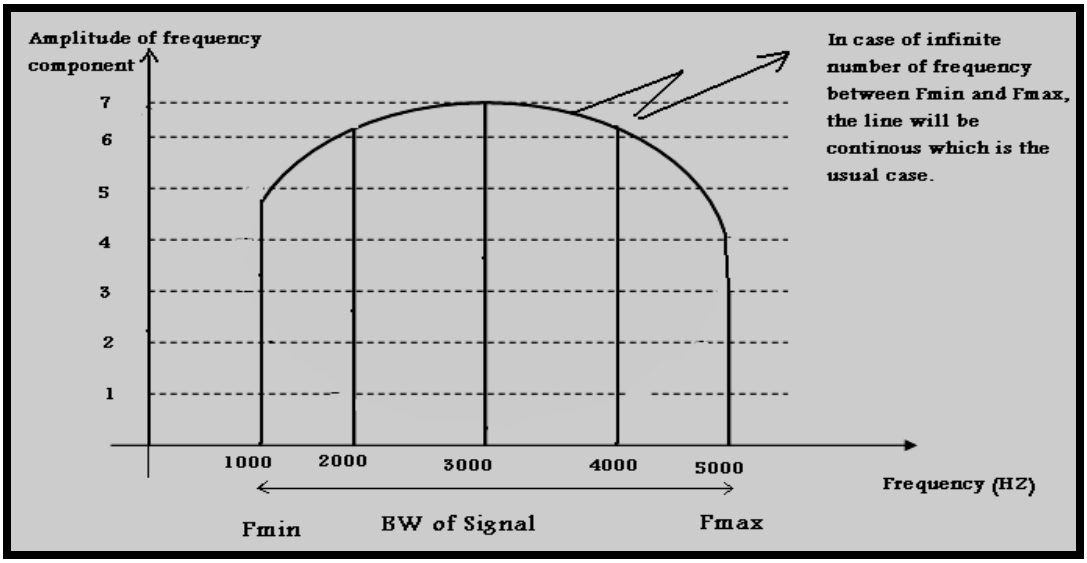


Figure 2.6 Signal Spectrum (Frequency components of Signal)

2-4 Properties Of Communication Medium

A communication medium is any material (or space) that allows certain type of signals to pass through it e.g. telephone wires allows electrical signal (voltage, current); air allows voice signal.

Usually, the signal carries information (data) and hence the communication medium is used for transferring data from a location to anther location.

The signal when passing through a communication medium suffers from:

1- **Noise: this is unwanted signal, causing interference to the original signal, and may destroy some or all the carried data. The noise may be generated internally by the medium due to environment changes or may be caused by other external signals passing around the medium e.g. the noise we hear in telephone line when a mobile device rings near it.**

2- **Attenuation Distortion: The signal is a kind of energy e.g. voice signal is a mechanical energy, electrical signal is electrical energy. When a signal passes through a medium then part of its energy is wasted e.g. the voice signal becomes very weak after traveling some distance. This means that the signal is attenuated by the medium and has to be amplified or regenerated (repeated) after traveling some distance. The most important fact is that the attenuation rate differs with frequency i.e. each frequency component of a signal suffers from attenuation in a different rate and hence the original signal may get distorted.**

3- **Delay Distortion: Each frequency component takes time to travel certain distance in a communication medium and this time is called "delay". The main problem is that the delay varies with frequency and hence the frequency components will not travel in the same speed and therefore will not arrive at a certain location together and this causes a signal distortion called "Delay Distortion".**

To show the effect of a communication medium, let us look at figure 2.7.

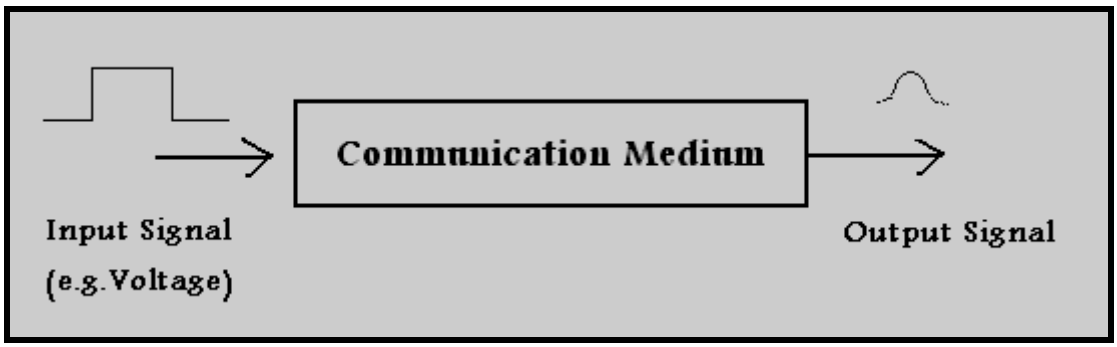


Figure 2.7 Effects of communication medium on signal

2-5 Band Width of Communication Medium

The properties of a communication medium means that any signal passes through it will get distorted, however, this distortion is very small when the signal frequencies (F_{min}, F_{max}) lie within certain limits (F_{low}, F_{high}) as shown in figure 2.8.

This means that if the frequency contents of a signal lies between F_{low} and F_{high} then the distortion is very small, therefore, F_{low} and F_{high} define what so called the "Pass Band" of a communication medium and its width is equal to (F_{high} - F_{low}).This width is called "BW" of medium.

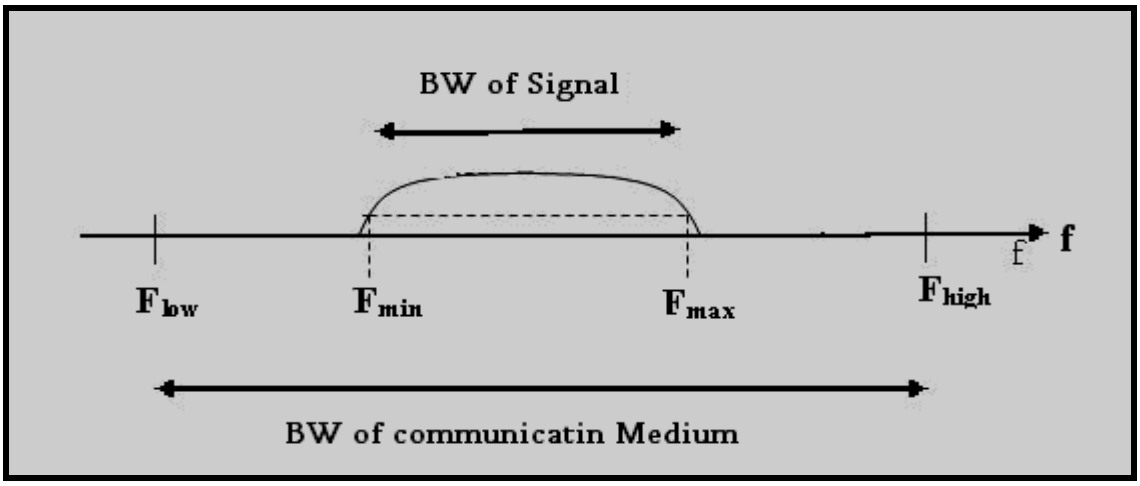


Figure 2.8 BW of signal and Medium

2-6 Concept of Modulation

Modulation means changing the properties of a sinusoidal signal so that it carries a data as shown in figure 2.9. The modulation has many types and two of them are shown in Figure 2.10.

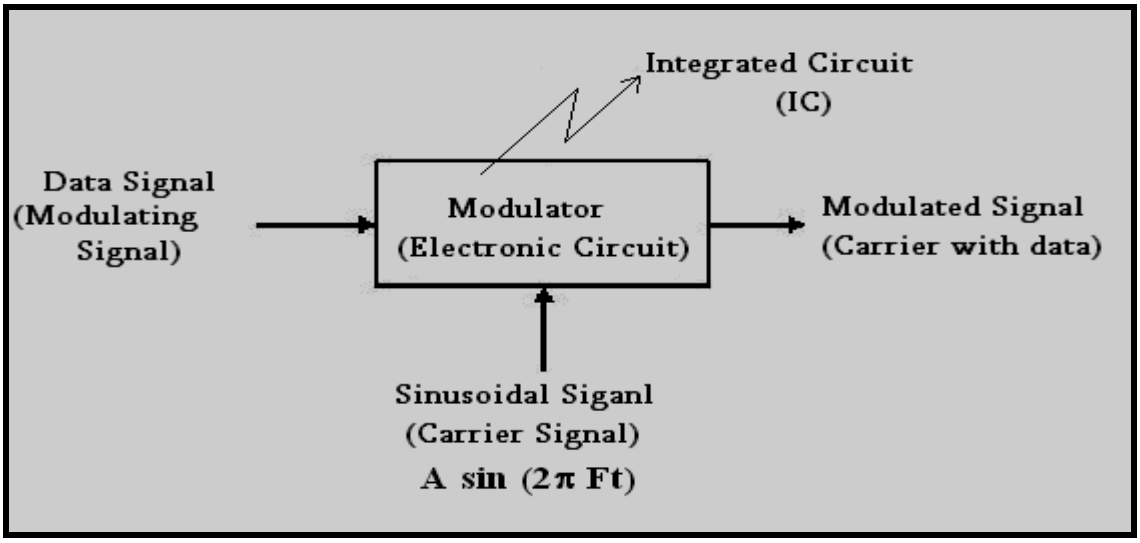


Figure 2.9 Modulation

The advantages of modulation are too many; however, we are going to mention the "frequency shift" property only as shown in figure 2.11

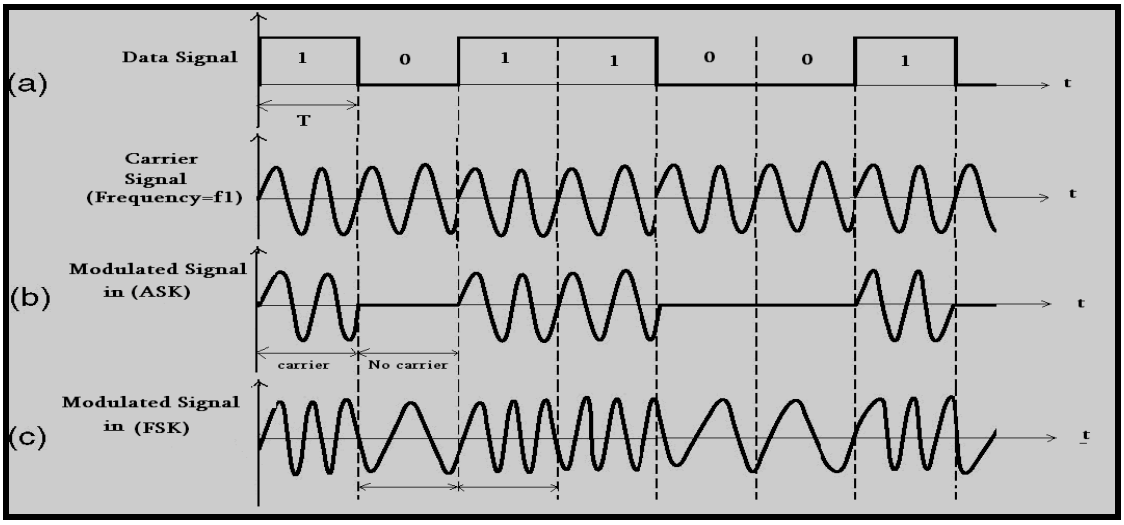


Figure 2.10 Amplitude Shift Keying (ASK) and Frequency Shift Keying (FSK) Modulations

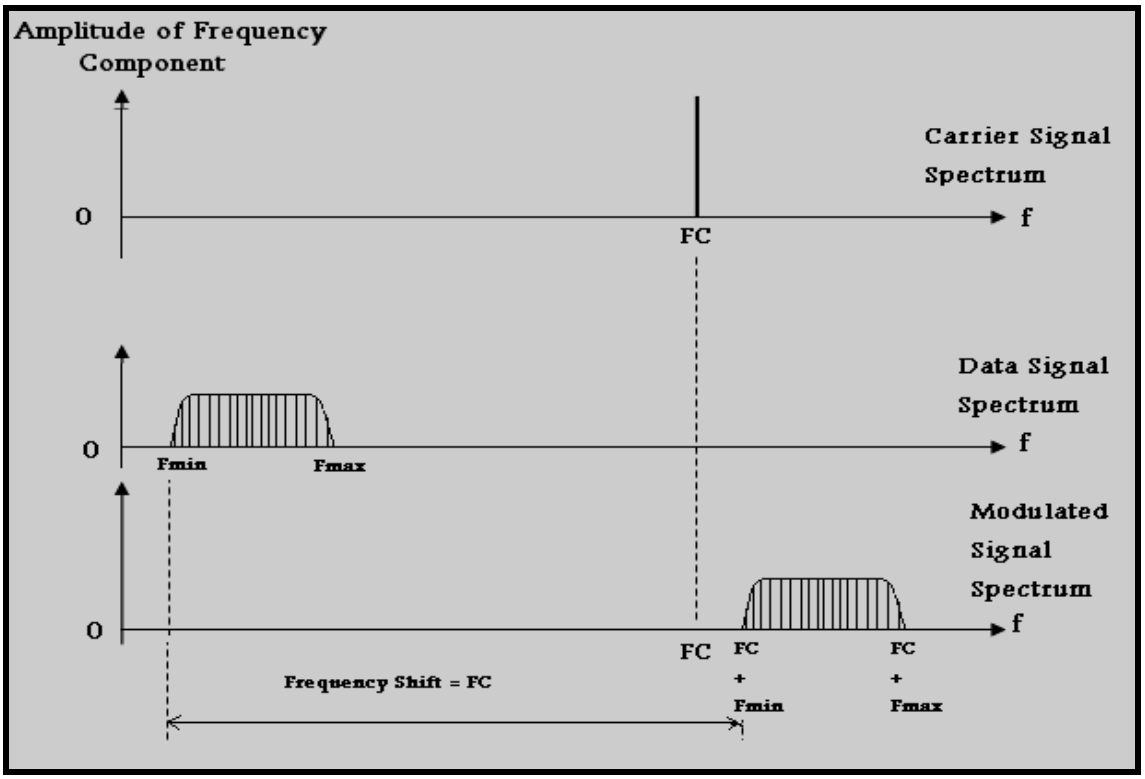


Figure 2.11 Frequency Shift in Modulation

The frequency shift property is used in a very important technique in communication called "Multiplexing" as will be explained later.

To extract the data signal from a modulated signal, we have to use demodulation technique as shown in figure 2.12

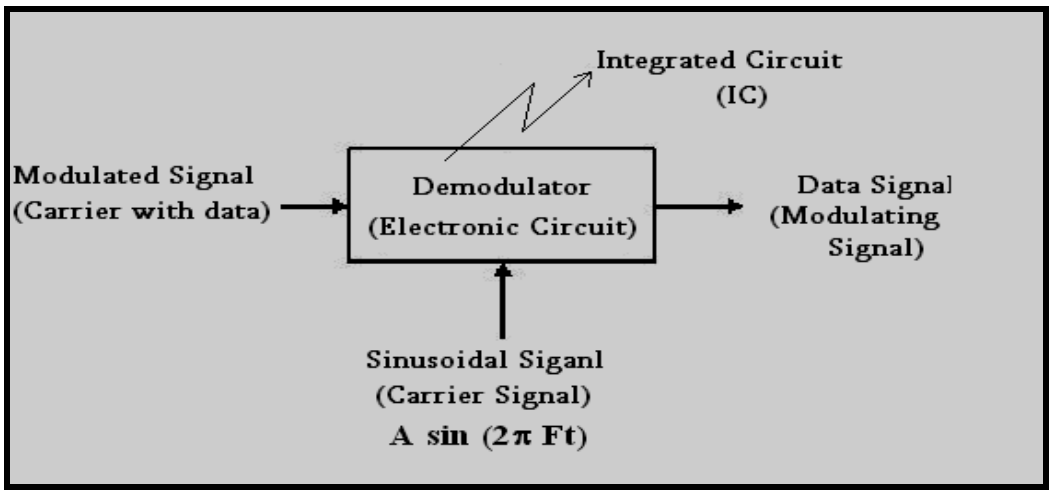


Figure 2.12 Demodulation

Usually, the modulator and demodulator exist in one device called "Modem" as abbreviation of "Modulator – Demodulator".

The applications of modems are very wide, not only for multiplexing, but, also, for other purposes such as adaptation of signal to become suitable to pass through a communication network as shown in figure 2.13.

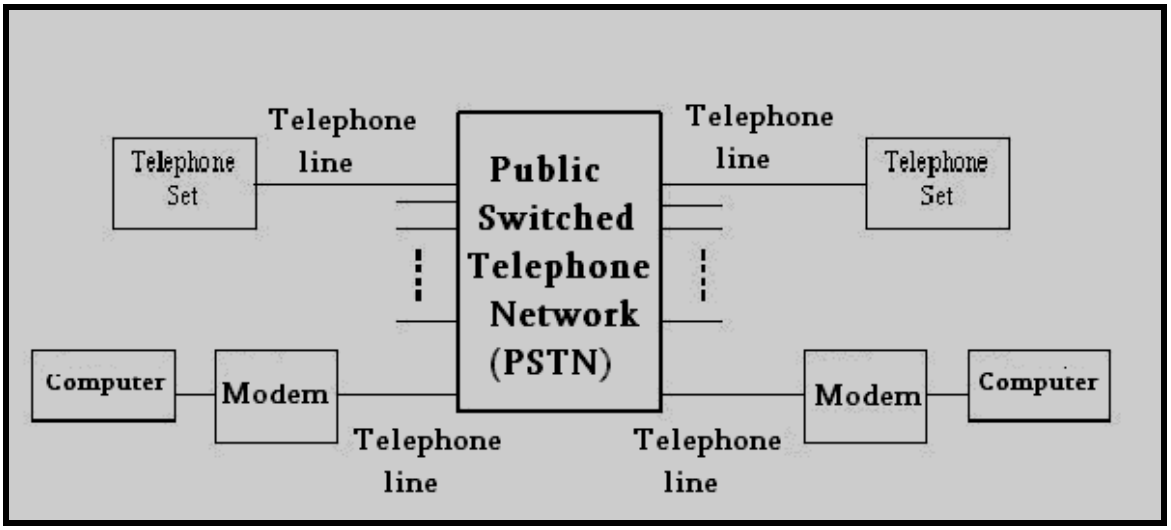


Figure 2.13 Communication between computers using Modems and PSTN

2-7 Multiplexing

If several signals with overlapped spectrums pass through a communication medium, then the receiver will not be able to extract any of them. To make this happening, it is necessary to adopt one of the following multiplexing techniques:

- **Frequency Division Multiplexing (FDM)**
- **Time Division Multiplexing (TDM)**
- **Wave Division Multiplexing (WDM)**
- **Code Division Multiplexing (CDM)**

Here, we are going to explain briefly the FDM where its block diagram is shown in figure 2.14.

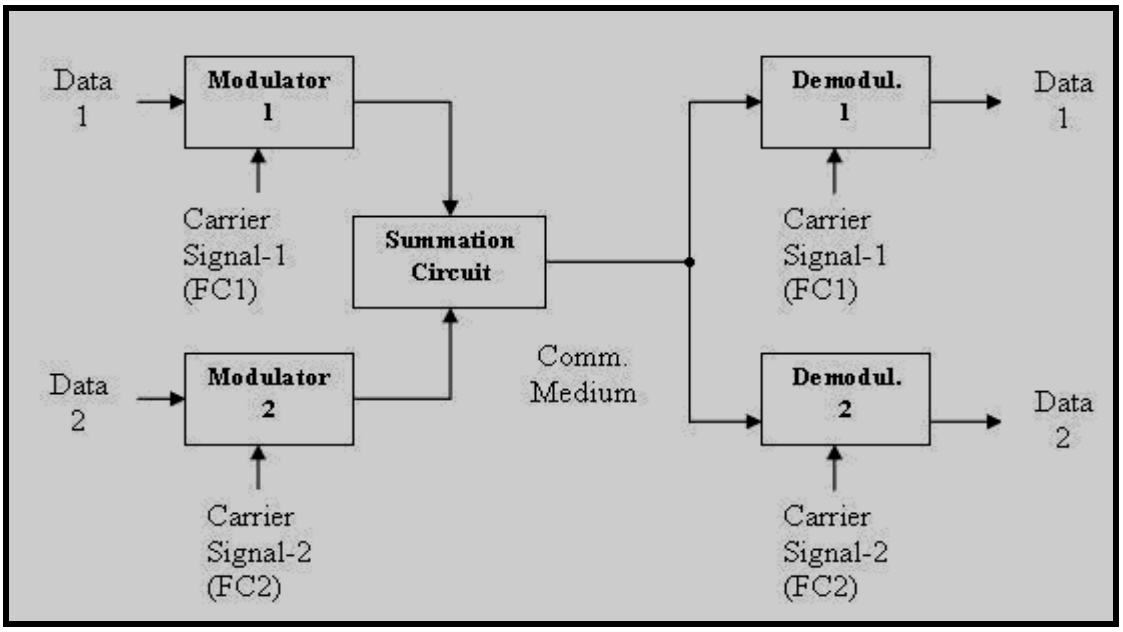


Figure 2.14 FDM Multiplexing

The receiver will be able to extract the data signals because the modulators shifted their spectrums so that they will not be overlapped as shown in figure 2.15.

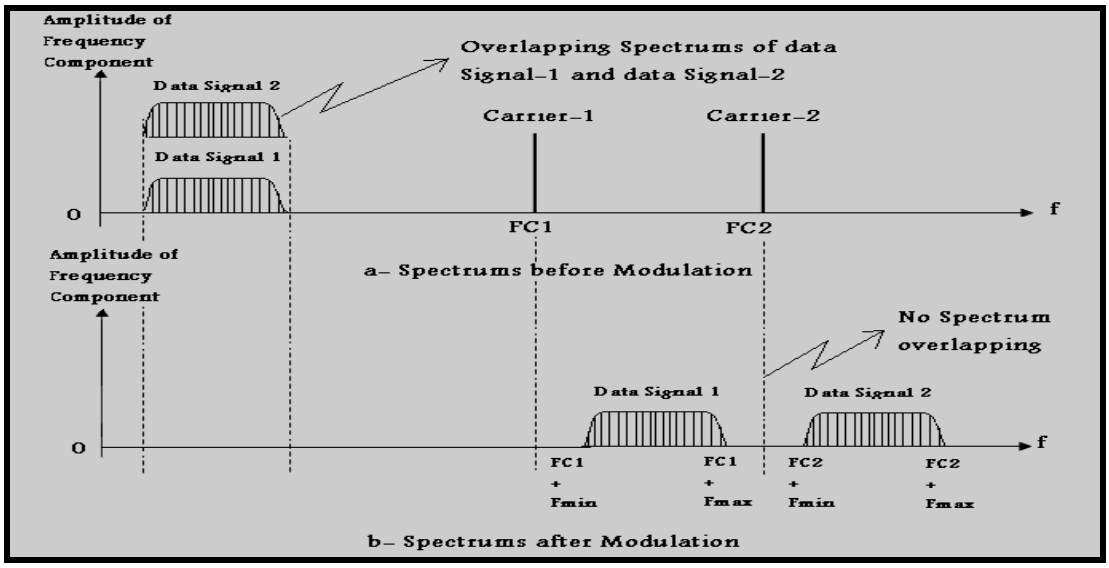


Figure 2.15 FDM Multiplexing

The action of spectrum shifting is equivalent to logically dividing the communication medium into several parts and each part is used to transfer one signal. This logical part is called a "channel" and, therefore, we can say that multiplexing creates channels in a communication medium and each channel is used to transfer one data signal as shown in figure 2.16

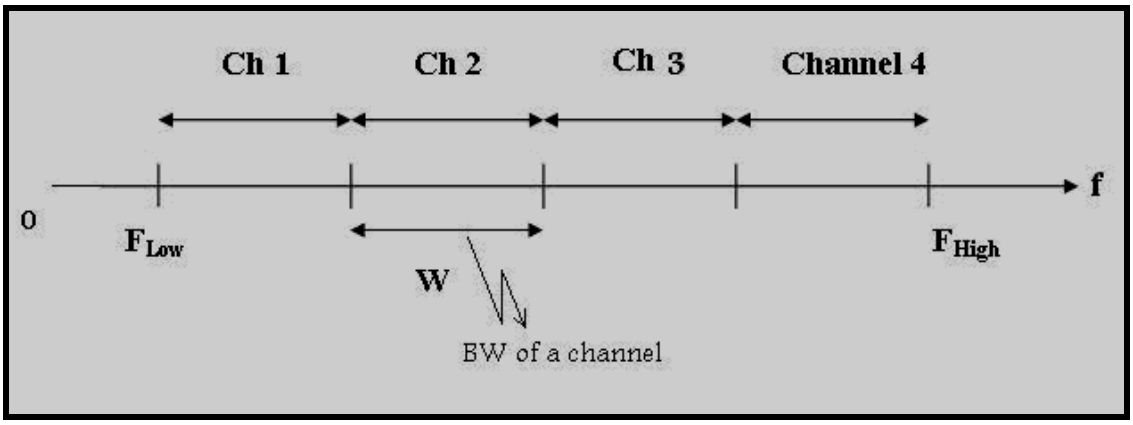


Figure 2.16 Channels of Communication Medium

2-8 Maximum Data Rate of a Channel

This rate can be calculated according to "Shannon's Theorem" as follows:

Maximum Data Rate = W $\log_2$ (1+ S/N) [bps]

Where:

W : is the BW of a channel in [HZ]

S/N: is the signal to noise ratio in channel.

This theorem implies that to get higher bit rate in channel, you have to improve signal to noise ratio and this can be done by selecting a proper modulation technique like (QPSK).

2-9 Communication Media (Transmission Media)

The main communication media that can be used to transfer (transmit) signals are:

- **Twisted pair used to transfer electrical signals.**
- **Coaxial cable used to transfer electrical signals.**
- **Optical fiber used to transfer optical signals.**
- **Radio waves used to transfer electromagnetic signals.**
- **Infrared waves used to transfer Infra red signals.**
- **Many others.**

For these media, we are going to study some of their properties such as bandwidth, bit rate, error rate, construction and others. It is worth saying that these properties are affected by length of media, diameter of media, type of media material, type of environment and surroundings, shape and construction of media.

2-9-1 Twisted pair (TP)

TP is the oldest and still the most common communication media. A TP consists of two insulated copper wires twisted together in a helical form as shown in figure 2.17. The purpose of twisting is to decrease the effect of surrounding electromagnetic field and also to decrease the effective radiation from the TP itself so that it dose not make crosstalk to other neighboring twisted pairs.

Twisted pairs are usually grouped together and protected by a plastic sheath (case of unshielded twisted pair UTP) or by a plastic sheath and braided wire shield (case of shielded twisted pair STP). The properties of TP depends on number of twists per unit length, therefore, we fined several categories as shown in figure 2.17.

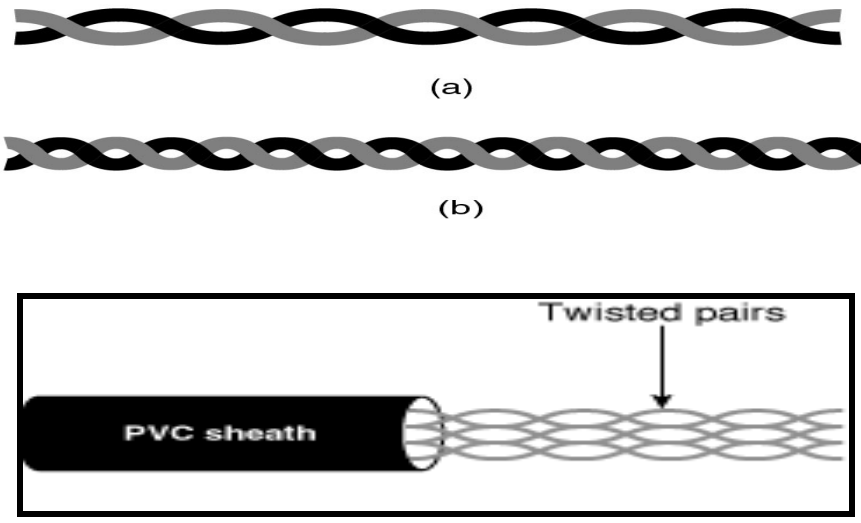


Figure 2.17 Twisted Pair (a) Category 3 UTP. (b) Category 5 UTP.

The main advantages of TP are:

1- **Easy to handle (cut, weld, connect, tap, twist, carry, etc.).**
2- **Low cost but it should be noted that Cat. 5 cables are more expensive than Cat. 3, also, STP is more expensive than UTP.**

The main disadvantages of TP are:

1) **Comparatively, narrow band width and hence low bit rate. For example, it is possible to transfer 10 Mbps for maximum distance of 100 meter on Cat. 3 UTP cable (on Cat. 5, it is possible to transfer up to 100 Mbps for the same distance of 100 meter) when used in LANs.**
2) **Comparatively, more affected by surrounding electromagnetic field which means more noise and hence less bit rate according to Shannon's theorem.**
3) **Comparatively, higher attenuation and hence "Repeater" devices are necessary on short distances of UTP cables.**

The main application of UTP cables are in telephone networks where Cat. 3 is used and, also, in LANs where Cat. 3 and Cat. 5 are used.

2-9-2 Coaxial Cable (Coax)

It is also two copper wires but constructed as shown in figure 2.18. This type of construction makes some of its properties better than TP and some worse.

The main advantages compared to TP are:

1) **Larger BW and hence higher bit rate, fore example, the thin coaxial cable can be used to transfer 10 Mbps for up to 200 meters in LANs.**
2) **Less affected by electromagnetic field and hence lower noise which means higher bit rate.**
3) **Less electromagnetic radiation and hence does not cause crosstalk in neighboring cables.**
4) **Less attenuation and hence repeaters are not needed on longer distances.**

The main disadvantages compared to TP are:

1) **More difficult to handle as it needs special connectors (BNC connectors) and has larger weight.**
2) **Higher cost.**

It should be noted that there are two types of coax:

- **Thin Coax of 0.5 inch diameter**
- **Thick Coax of 0.75 inch diameter**

The thin Coax is widely used in:

- **TV systems (cable TV, connect antenna to TV).**
- **MANs computer networks.**
- **Long distance telephone line (now is being replaced by fibers).**

It should be noted that the use of coax in MANs are due to:

- **The spread of cable TV systems in western cities and hence can be used for MANs.**
- **The coax has low attenuation and hence can be used without repeaters on city level.**

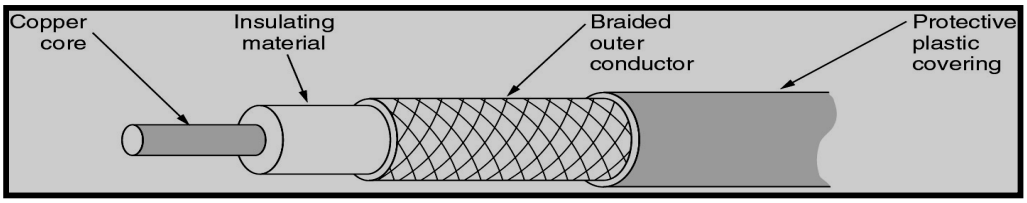
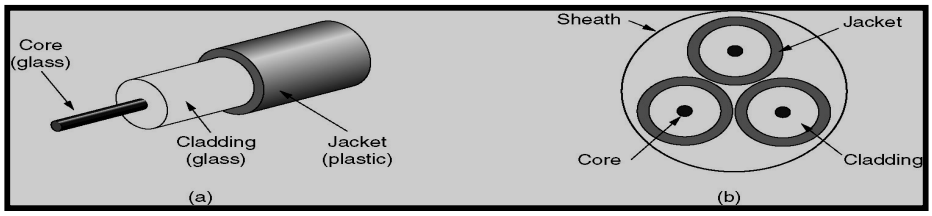
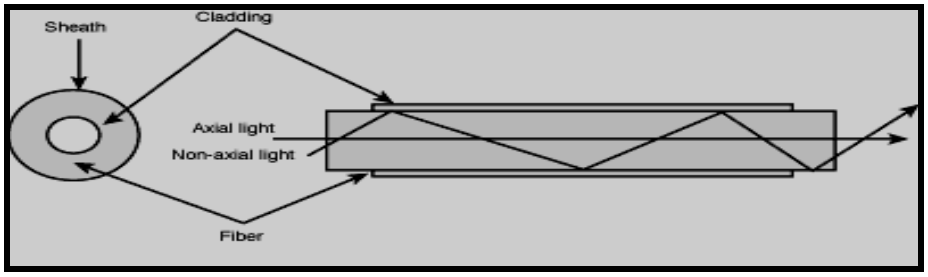


Figure 2.18 Coaxial Cable Constructions.

2-9-3 Optical Fiber (Fiber)

Here, we are using optical light to carry data signal instead of electrical current used in copper wires. The light itself is carried by a special transparent material (glass) surrounded by other materials as shown in figure 2.19. The light passes through the core via continuous reflections or in other forms depending on fiber type.





a- signal fiber b- Fiber cable cross-section (Contains 3 fibers)

c- Light transmission (Longitudinal cross-section)

Figure 2.19 optical fiber

The main advantages of optical fibers compared to copper wires are:

1) **Very high BW and hence very high bit rate (e.g. 1000 Mbps for more than 1000 meter).**
2) **Low attenuation and hence repeaters are less needed unless for very long distances (e.g. 200 km).**
3) **Not affected by electromagnetic interference which means less noise and higher bit rate.**
4) **Low error rate of order 10^{-5} bit i.e. 1 error bit every 10^{5} transmitted bit.**
5) **Light weight.**

However, there are some disadvantages such as:

1) **Difficult to handle (no tapping, small angle twist, difficult to connect) and hence requires special tools and expertise.**
2) **The need for electric-optic transducers as shown in figure 2.20.**
3) **More expensive.**

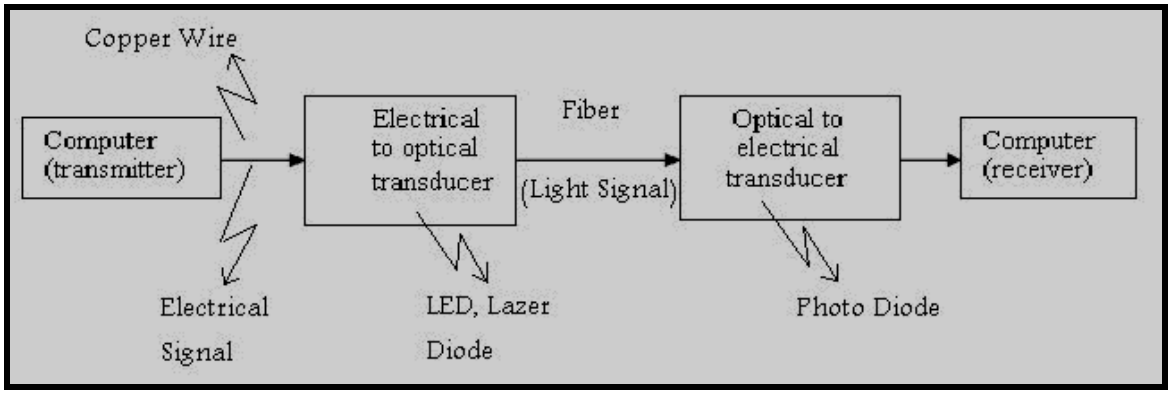


Figure 2.20 optical transducers

The specifications of fibers are getting better with the advance of technology and the need for them are getting higher due to the need for high bit rate, therefore, the application of fibers are growing all the time so that, in the future, the fibers will reach at our homes.

It is worth noting that one fiber only is needed to transfer the signal but in copper it is necessary to use two wires.

2-10 Modes of Communication

There are several modes of communication between two devices and can be summarized as follows:

1) **Simplex Mode: one device transmits and the other receives as shown in figure 2.21. A good example of simplex communication is the TV and Radio broadcast.**
2) **Full Duplex Mode: Each device can transmit and receive at the same time. A good example is two computers connected together via serial ports (COM).**
3) **Half duplex (semi duplex) Mode: Each device can transmit and receive but not at the same time. A good example is the telephone network.**

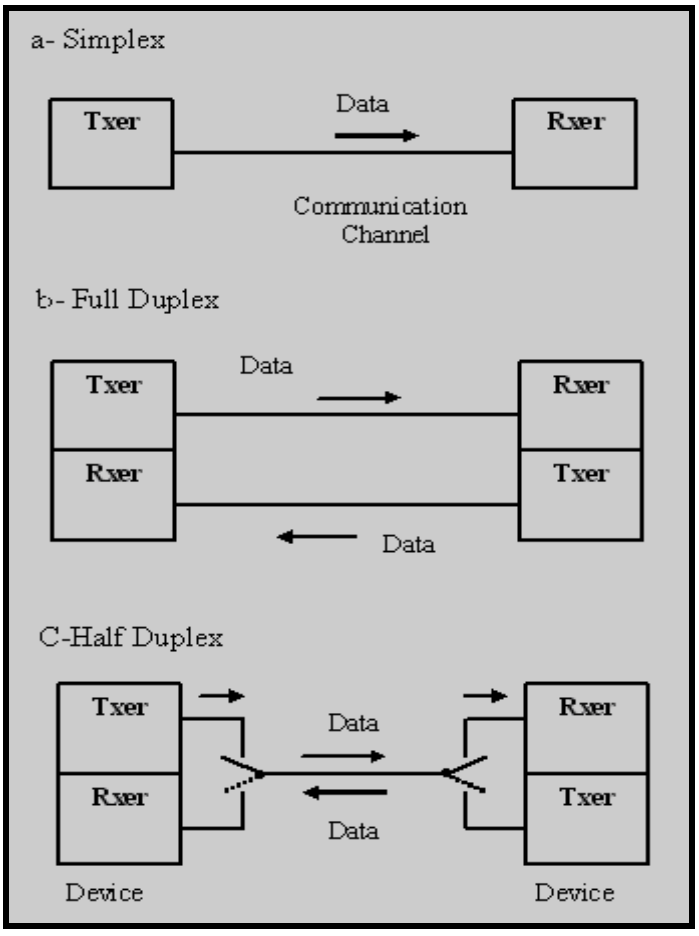


Figure 2.21 Communication Modes

(Txer – Transmitter, Rxer- Receiver)

It should be noted that the simplex mode can be modified so that the receiver can send "Acknowledge" messages to the transmitter as in figure 2.22.

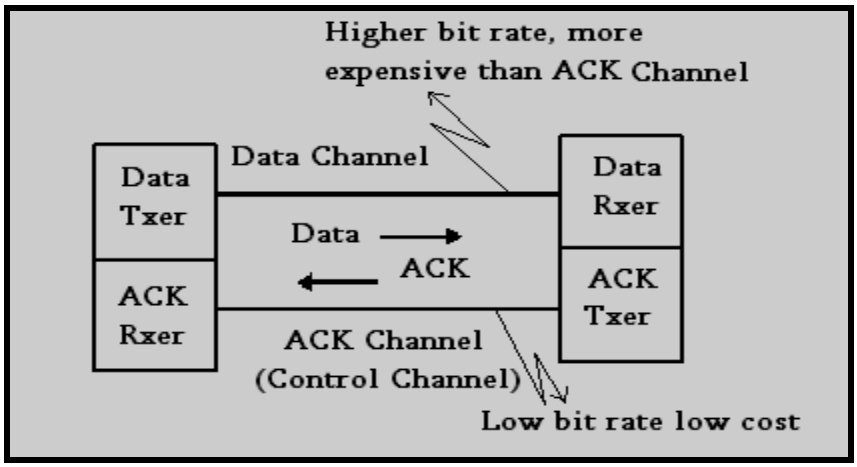


Figure 2.22 Simple Mode with ACK channel.

The ACK message includes "ACK" when the data are received correctly and "NACK" when received with errors.

Its is worth saying that data channel and ACK cahnnel may exist in the same communecation media using a proper multiplxing technique like FDM.

Chapter 3

Error Control

3-1 Introduction

The data suffers from errors when transferred from device to another via a communication channel.

The sources of errors are:

- **Noise in the channel due to internal properties of communication or due to external effect (e.g. electromagnetic interference or crosstalk).**
- **Faults in the electronic circuits that process the data signal.**

To solve this problem, we need error correction methods, error detection methods, and error control methods.

3-2 Error Correction

In simplex communication system, the receiver can't tell the transmitter to resend the data when errors are detected, therefore, the transmitter should send an addition data (error correcting code) in order to enable the receiver to correct the erroneous received data. There are many methods for error correction but we shall study one famous method called "Hamming" who is a communication scientist.

The Hamming method can be summarized as follows:

1. **Insert error bits in positions order 2^n and data bits in the others as follows:**

2^0	2^1		2^2			
1	2	3	4	5	6	7
C_1	C_2	D_3	C_4	D_5	D_6	D_7

2. **Make relation between D bits and C bits according to there position as follows (position of D equal sum of C positions):**

D bits	C bits
D_3	C_1, C_2
D_5	C_1, C_4
D_6	C_2 , C_4
D_7	C_1, C_2, C_4

3. **Calculate the values of C as XOR of related D bits as follows:**

$$C_1 = D_3 \oplus D_5 \oplus D_7$$

$$C_2 = D_3 \oplus D_6 \oplus D_7$$

$$C_4 = D_5 \oplus D_6 \oplus D_7$$

The C bits are sent with the data to the receiver in an agreed format between transmitter and receiver (e.g. $D_3 D_5 D_6 D_7 C_1 C_2 C_4$) .

4. **On reception, C bits are calculated again for real received data and then compared with real received C bits then we can find the position of erroneous bit as follows:**

Incorrect C	Erroneous Bit	Position
C_1	C_1	1
C_2	C_2	2
C_1, C_2	D_3	3
C_4	C_4	4
C_1, C_4	D_5	5
C_2, C_4	D_6	6
C_1, C_2, C_4	D_7	7

Once the position of erroneous bit is found, it can be inverted to make it correct.

In the previous example, we notice that the number of C bits is large when compared to D which means great loss of communication channel time, however, this impression will disappear if we consider longer data as in the following example.

2^0	2^1	2^2					2^3							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
C_1	C_2	D_3	C_4	D_5	D_6	D_7	C_8	D_9	D_{10}	D_{11}	D_{12}	D_{13}	D_{14}	D_{15}

***Note**: The error correction code is used, also, when storing data to hard disk in computer system.*

3-3 Error Detection

The principle of error detection can be summarized as follows:

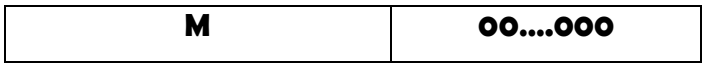
1) **Make some operations (processing) on the data and extract few bits that will be called "Error Detection Code" or "Error Code".**
2) **Send the data together with error code to the receiver.**
3) **Make the same above operations on the received data to extract the error code for received data.**
4) **Compare error code of received data with error code of original data, then if they are not identical, we conclude that errors are present; otherwise, we assume the data are received correctly.**

The type of operations and the number of bits in error code (length) determine the power of any method for detecting the errors.

There are many methods for error detection such as parity and checksum but, here, we are going to study the method being used in computer networks which is briefly called "CRC" i.e. "Cyclic Redundancy Check".

The CRC method can be summarized as follows:

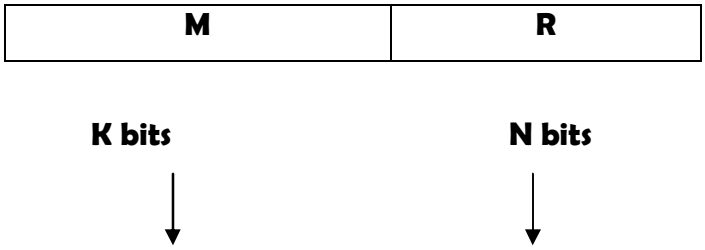
1. **Shift the data M to the left N times as follows:**



2. **Modulo 2- divide by the code P of (N+1) bits.**

3. **The remainder R of N bit length is the error code.**

4. **Send the following frame:**



5. **On receiving the frame, modulo-2 divide by P if the remainder is zero then the frame is correct, otherwise, there is error.**

To clarify this method, let us take the following example:

Find the error code if M= 1010001101 and P= 110101, then check the result.

Solution:

```
110101 | 101000110100000
       - 110101
         111011
       -  110101
          111010
      -    110101
            111110
          -  110101
              101100
        -    110101
              110010
           -  110101
              01110
```

Remainder = Error code

To check the result, we modulo-2 divide (MR) by P then we shall find that the remainder is zero. This means that if divide the frame (101000110101110) by (110101) the remainder will be zero.

Now it is necessary to note the following:

- **P should start and end with 1.**
- **Modulo-2 subtraction is XOR.**
- **Dividend is devisable when its number of bits equals the number of bits of divisor (of course in modulo-2 division).**
- **Most signification bit of dividend should be 1.**
- **P can be written in nicer fashion as a polynomial function P(x):**

$$P = \underset{X^5\ X^4\ X^3\ X^2\ X^1\ X^0}{1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1}$$

$$P(x) = X^5 + X^4 + X^2 + 1$$

That is why the CRC method is sometimes called "polynomial" and P is called "polynomial Code".

- **Value of P determines the power of the method for detecting the errors.**
- **There are standard values for P selected by simulation studies so that they can detect most of the errors.**

3-4 Error Control

There are many problems when two devices are communicating together such as:

- **The action to be taken when an error has been detected in the received data.**
- **The failure of receiver to detect the frame (frame loss) and hence data will not be detected at all (usually, because of noise burst)**
- **The loss of "ACK" messages sent from receiving device to transmitting device due to burst of noise (the transmitting device will not detect the start or end of "ACK" message).**
- **The breakdown of receiving device after sending "ACK" message and hence loss of stored data.**
- **The receiver may not be able to process or store all the data being sent to it and hence the control of data flow from transmitter to receiver has to be undertaken.**
- **Other problems.**

Many of these problems can be solved by adopting a proper error control method. The famous method is called "Automatic Repeat reQuest ARQ". The ARQ has several types as follows:

3-4-1 Idle ARQ

This method is applied in simplex systems with "ACK" channel. The Txer (Transmitter) dose not sends a new message until it receives "ACK" message from the Rxer.

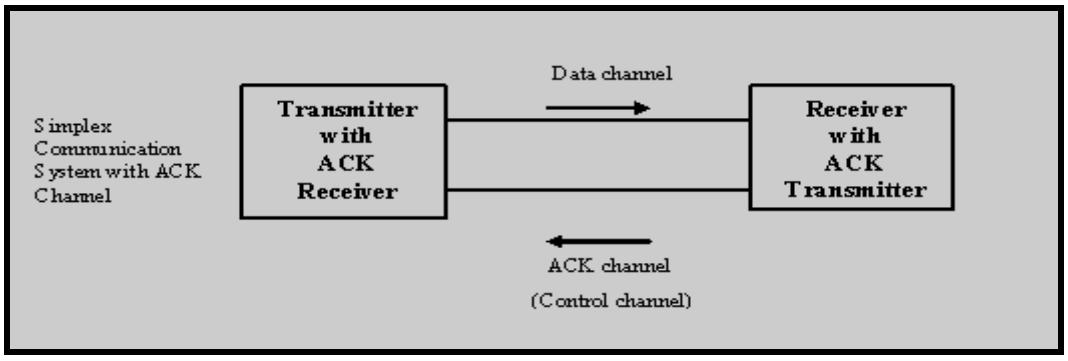


Figure 3.1 Idle ARQ

3-4-2 Simplex Continuous ARQ

This method is also used in the simplex communication system with ACk channel (also called control or supervisory channel). In this method, the Txer sends several fames holding sequence numbers without waiting for ACK messages as the case of Idle ARQ. When an error is detected, the Rxer sends NACK message with sequence number.

3-4-3 Duplex Continuous ARQ (Piggy -Backed)

This method is used in full duplex communication systems where data channel is present in each direction. The method is designed to work as follows:

1. ***Each side keeps two numbers which are:***
   - **Sequence number of frame to be transmitted next (called N(S)).**
   - **Sequence number of frame expected to be received (called N(R)).**
2. ***When a data frame is sent in either direction, it is made to carry a header with two sequence numbers:***
   - **Sequence number of frame being sent.**
   - **Sequence number of frame expected to be received.**

3-5 Effect of Error control on Flow Control

The error control methods, studied earlier, act as flow control methods as well because they prevent a transmitter from swamping a receiver with data frames.

The prevention comes as a result of stopping the transmitter from sending data frames with out receiving ACK frames in the proper time (the number of allowed sent frames without ACK are defined by the sliding window).

Chapter 4

Design Issues of Computer Networks

4-1 Introduction

There are many issues to be considered when designing a computer network such as switching, segmentation, addressing, routing, error control, and many others.

4-2 Switching

There are three main types of switching as shown below:

4-2-1 Circuit Switching

When you or your computer places a telephone call, the switching equipment within the telephone system seeks out a physical path all the way from your telephone to the receiver's telephone.

This technique is called circuit switching as shown in figure 4.1 the physical path is reserved fro the period of the call and can be used for voice conversation or for data transfer between two computers if they are connected to the via modems.

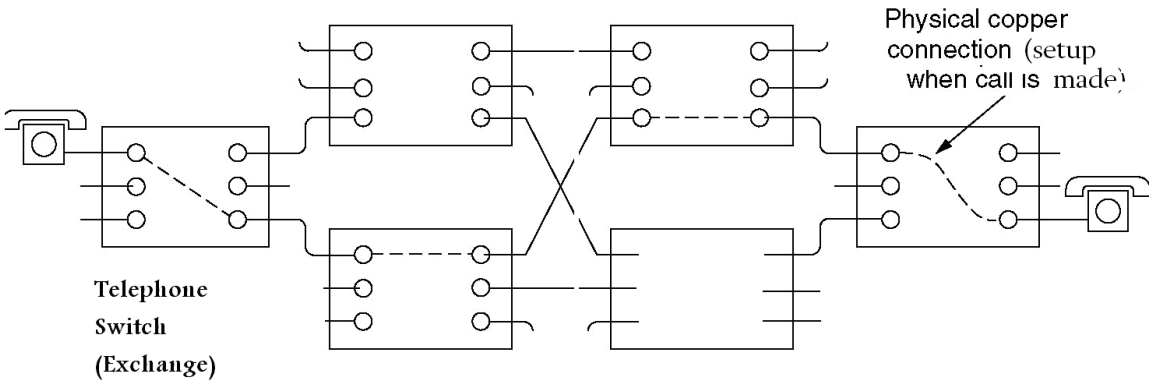


Figure 4.1 Circuit Switching

The main advantages of circuit switching are:

1. **No data delay between Transmitter and Receiver excluding the normal propagation delay (about 5 msec per 1000 km).**
2. **No congestion or routing problems at the nodes (exchanges).**
3. **Simplicity of the nodes.**

However there are many disadvantages:

1. **The time needed to set up the call (up to 10 sec).**
2. **The circuit between Transmitter and Receiver is reserved for one data transfers and can't be used for other data transfers even if the communicating devices are not sending for some time during the call. This means a waste of channel time and hence the cost will be high.**
3. **There is no error checking at the nodes which means loss of channel time.**
4. **The broadcasting is very difficult i.e. it is not easily possible for any Transmitter to send data to many Receivers at the same time.**

All these disadvantages opened the way to the other types of switching.

4-2-2 Message Switching

In this type of switching, no physical path is established in advance between sender and receiver. Instead, when a sender has a block of data to be sent, it is stored in the first switching office (i.e. router) and then forwarded later, one hop at time as shown in figure 4.2. Each block is received in its entirety, inspected for errors, and then retransmitted (store- and -forward technique).

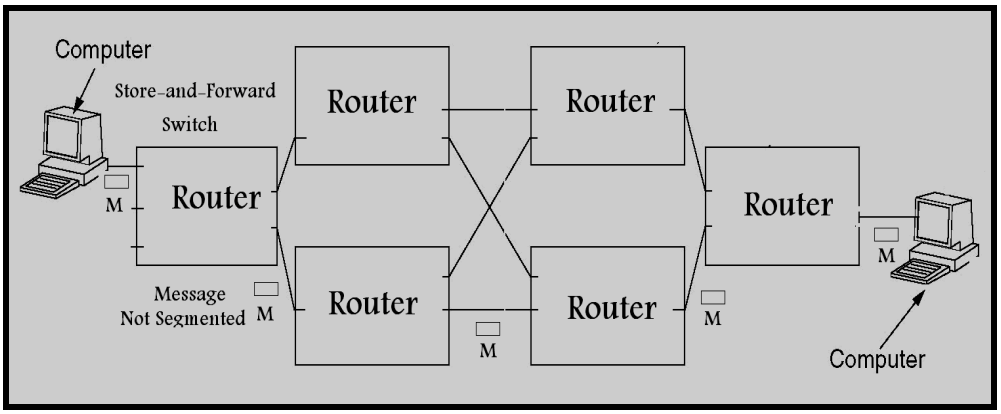


Figure 4.2 Message Switching

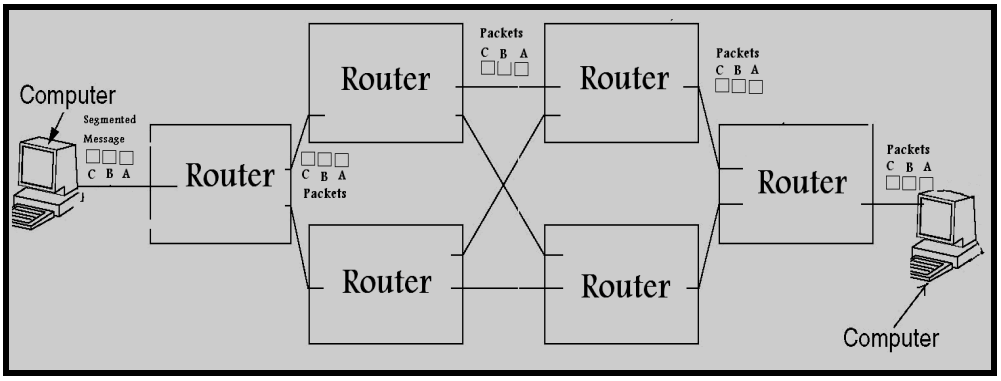
The disadvantages of circuit switching have disappeared here; however, there are new disadvantages, such as:

1. **When the message is long, then it will monopolize the channel for long time and this may cause long delays for other waiting messages to be sent on the same channel.**
2. **When the message arrives at the end receiver and an error is detected, then, the whole message has to be retransmitted which means loss of channels time.**

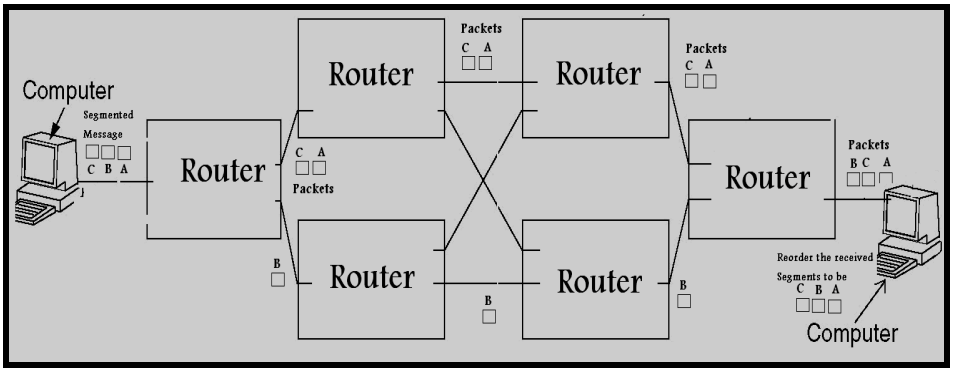
The above disadvantages can be avoided by segmenting the long messages into shorter sub messages (segments) and this is the case of packet switching.

4-2-3 Packet Switching

This is similar to message switching except of segmenting the long messages into smaller ones as will be shown later. The sub messages are usually called "Packets". The packets of certain message may follow the same path in the network (case of virtual circuit) or may follow different paths (case of Datagram) as shown in figure 4.3. It should be noted that packets are combination of original data and some extra control data (Header) necessary for reassembly at the receiver and for other purposes as will be explained later.



a- Virtual Circuit Packet Switching



b- Datagram Packet Switching

Figure 4.3 Packet Switching

The main advantages of packet switching are:-

1. **Absence of channel monopolization and hence better and effective use of channels which in turn means lower cost.**
2. **Priority scheme may be applied for packet transfer.**
3. **The erroneous packet can be retransmitted without retransmitting the whole message.**
4. **All message switching advantages and many others.**
5. **Fault tolerant because the packets have usually several paths which can follow to reach the destination.**

4-3 Segmentation and Assembly

As mentioned earlier, it is necessary to break long message into smaller sub messages. To enable the assembly of these sub messages in the Receiver, it is necessary to add to each of them an ID (Message Identification) and a "segment number" as shown in figure 4.4. These two items constitutes the "Header" which combined to original data to form the "packet". It should be noted that the term "packet" is used in different cases to indicate a combination of data and header (control data).

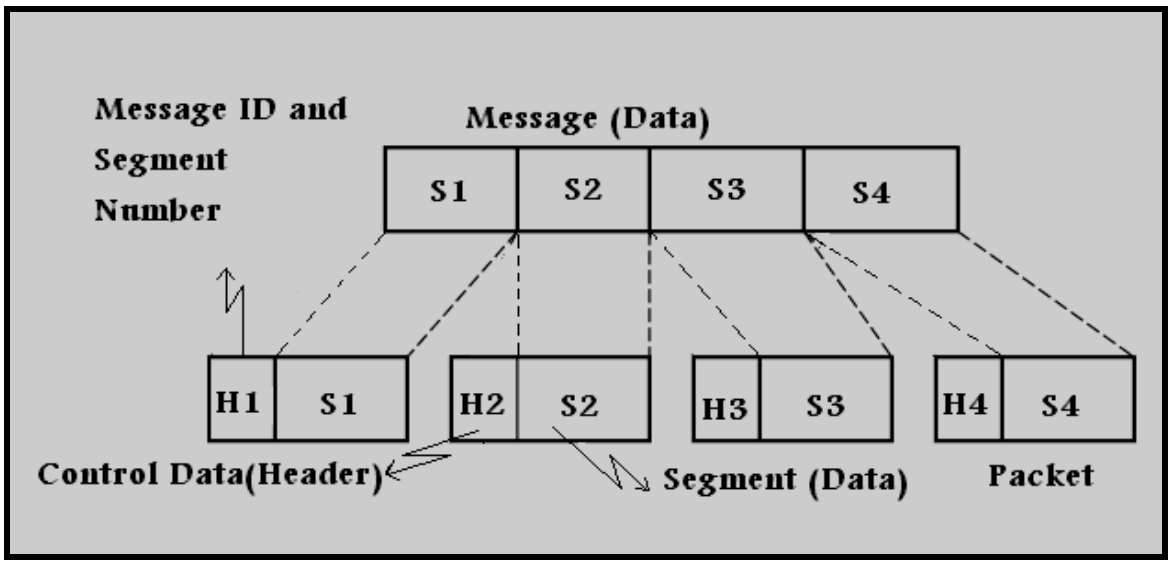


Figure 4.4 Segmentation

4-4 Addressing

A computer network is actually a set of computers running many processes (programs) and these processes are communicating together as shown in figure 4.5. *This construction leads to the use of following logical addresses:*

- **Host address to define one computer (host) in the whole (global) network. This address can also be called as "Global Address". In Internet, it is called IP address.**
- **Process address to define one process within the host i.e. it is "local address" and in Internet, it is called "port" number.**
- **Full address to define one process in the whole network and, hence, it is a combination of host and port addresses. The "Full address" is called in Internet as "Socket Number".**

It is important to say that in addition to these logical addresses which are assigned and can be changed by programs, there is another type of addressing called "physical addressing" which is defined by hardware and can't be changed. The physical address is usually unique on the world level and assigned electronically to each network interface card (NIC). The address uniqueness is achieved by international agreement between manufacturers.

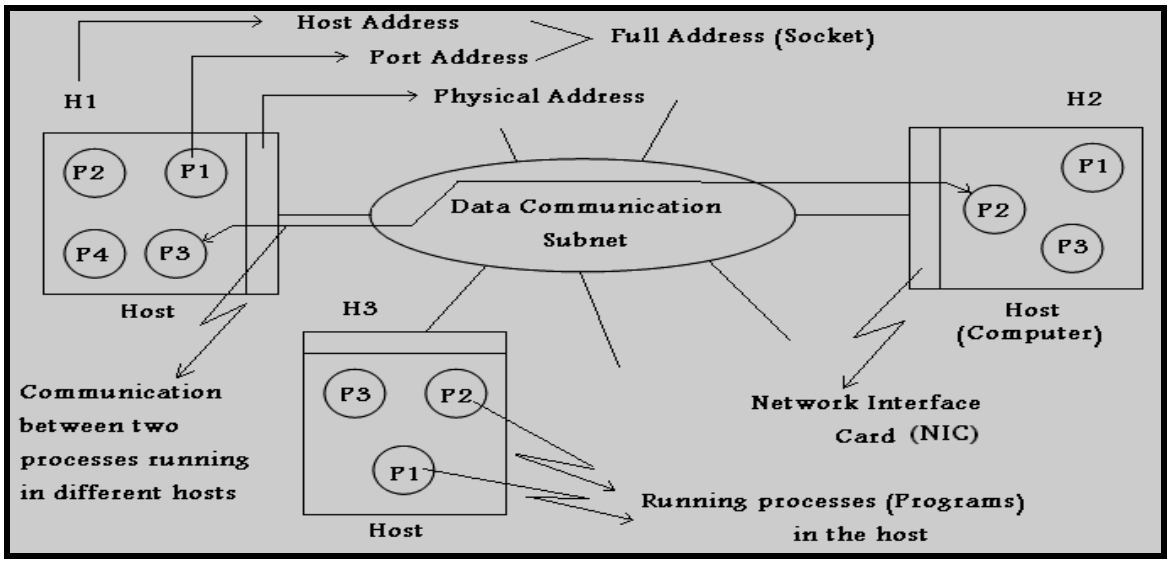


Figure 4.5 Addressing in Computer Network

4-5 Routing

The nodes in WANs are "Routers". The router has many functions but the main one is to select the best route for each received packet in order to allow it to arrive at its destination. The choice of route is usually implemented by a proper routing algorithm which satisfies the data transfer requirements.

The requirements may be less cost, high speed, secure path, etc. The routers are normally intelligent devices (dedicated computer) which can communicate together to collect the necessary information for routing decision. There are many routing algorithms which require separate study.

4-6 Multiplexing

This means the use of communication medium and communication channel for several data transfers for several conversations between processes. Multiplexing can be done in the "End" and in the "Intermediate" devices of the network.

4-7 Error Control

As mentioned earlier, it is necessary to use error detection codes and proper error control methods to solve the problems of errors in computer network. The error control is usually done on two levels:

1. **Neighbor to Neighbor level: The directly connected devices (adjacent) should implement error control to avoid transfer of erroneous data which eventually means the waste of communication channel time.**
2. **End to End level: The end communicating processes should also implement error control strategy to ensure that all the data sent by one process have actually arrived at the destination process. This error control level is necessary because the intermediate devices (routers) may have faults or break down. It is worth noting that the first level may also called "Link level" or "Hop level". Therefore, it is possible to say that if the data transfers across the links are correct, the overall transfer may be not correct as the intermediate node may destroy the packet which had been received correctly as shown in figure 4.6.**

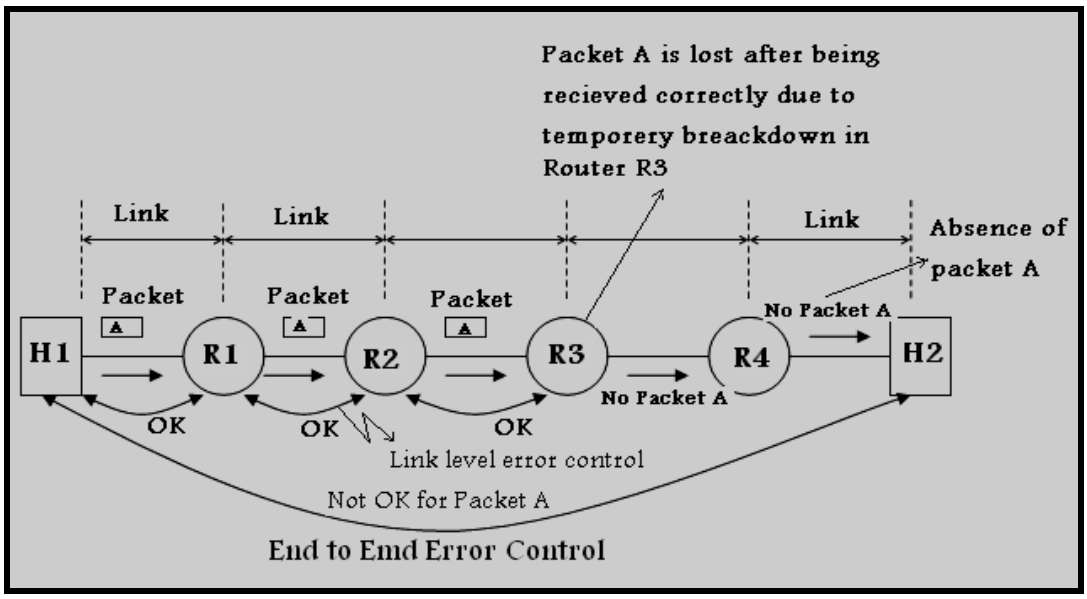


Figure 4.6 Error Control Levels

4-8 Flow Control

When sending data from end host to end host across several devices (routers), it is necessary to make sure that sender doesn't swamp receiver with data (flow control). The flow control has to be done on two levels:

- **Link level between directly connected devices.**
- **End to End level between indirectly connected devices.**

As we have studied earlier, the error control methods, actually, ensure flow control as well. This means that flow control is usually embedded in error control and thus we don't need to worry a bout.

4-9 Layers and Encapsulation

The Network operating system (NOS) in any network device comprises several programs arranged in certain way.

These programs are usually, resident in device memory and communicate together (exchange data) in an already defined method. The common used arrangement is the layered architecture as shown in figure 4.7. In this architecture, each program is called a "layer" and each layer is allowed to

communicate with the one above it and the one below it. When any layer in end host needs to send data to a peer layer in another end host, it has to add extra control data (header) to the original data. This header acts as instructions to the remote peer layer telling it what to do and how to do it. Also, the header might be necessary for the peer layers in the intermediate network devices to coordinate its operation with the end layers. The process of adding header to data is called "encapsulation" as shown in figure 4.7.

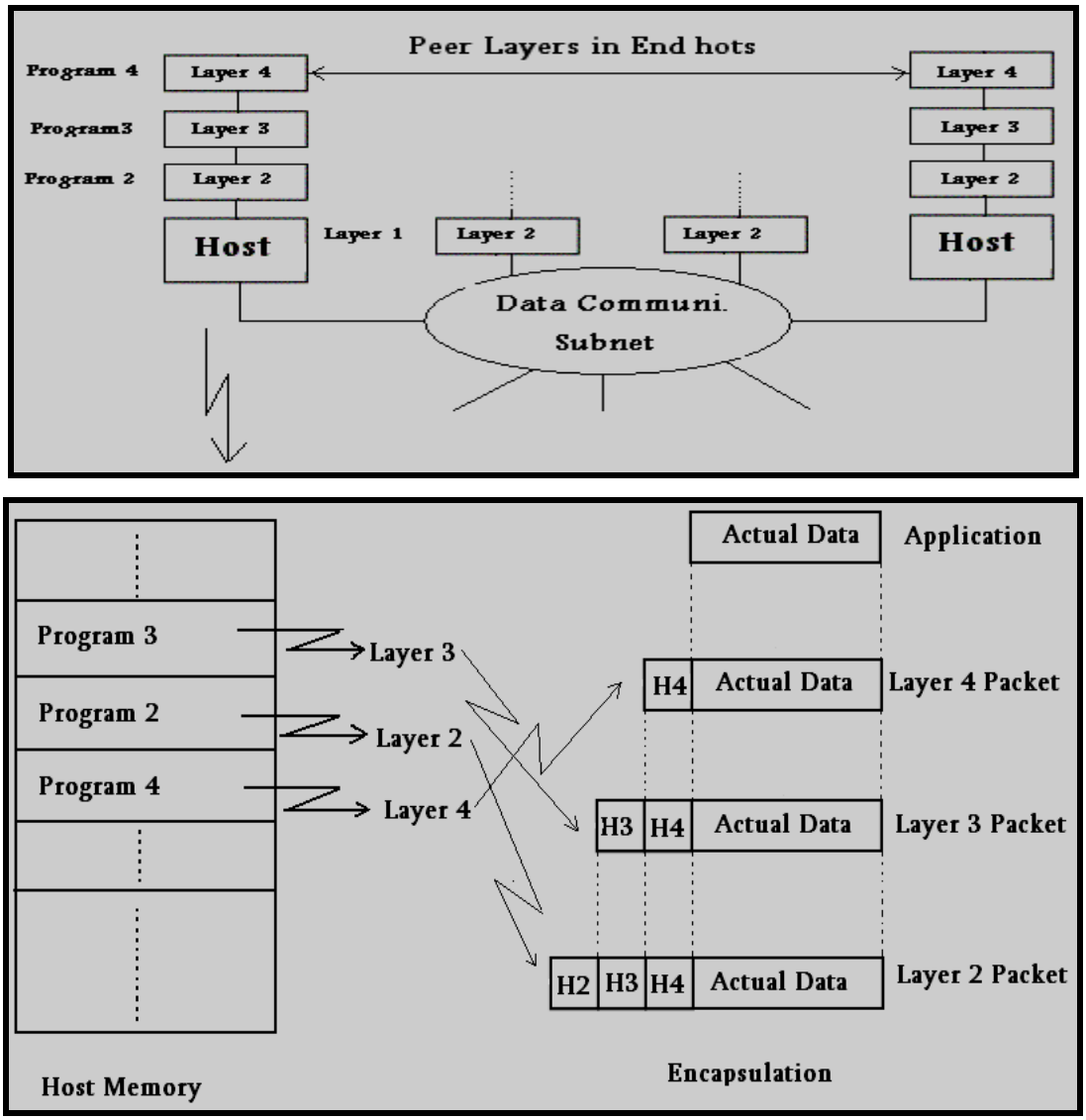


Figure 4.7 layers and Encapsulation

4-10 Synchronization

When data block is transferred between two devices connected directly together (link), the receiving device should be able to:

1. **Detect the start and end of each received bit (called bit synchronization).**
2. **Detect the start and end of each received byte (called byte synchronization).**
3. **Detect the start and end of each received block (called frame synchronization).**

These activities are realized by combination of hardware and software which are usually available in the Network Interface Card (NIC). The synchronization realization, however, requires addition of extra control data to the original data block and the result is called as a "Frame". Some frame formats will be shown later when LANs are studied.

4-11 Other Issues

There are many other issues such as security, priority, compression, etc., but will not be studied here.

Chapter 5

Local Area Networks (LANs)

5-1 Introduction

As mentioned earlier, LANs features are:

- **Occupied area is relatively small e.g. lab, floor, building, campus.**
- **Communication media length is relatively small and hence BW is large which means high data rate.**
- **Number of hosts may be very large (thousands of hosts), some of them act as servers.**
- **Simplicity of data communication subnet.**
- **LANs can be connected to WANs via proper routers.**

There are many standard LANs in use nowadays such as:

- **Ethernet (IEEE 802.3 standard)**
- **Token Bus (IEEE 802.4 standard).**
- **Token Ring (IEEE 802.5 standard).**
- **Wireless (IEEE 802.11 standard).**

In the following sections, we are going to study some of these standards.

5-2 Ethernet LAN

This type of LANs is widely used; therefore, we are going to study it in some details.

5.2.1 Medium Access Control (MAC)

The original Ethernet topology is the bus one shown in figure 5.1. In this configuration, we notice the followings:

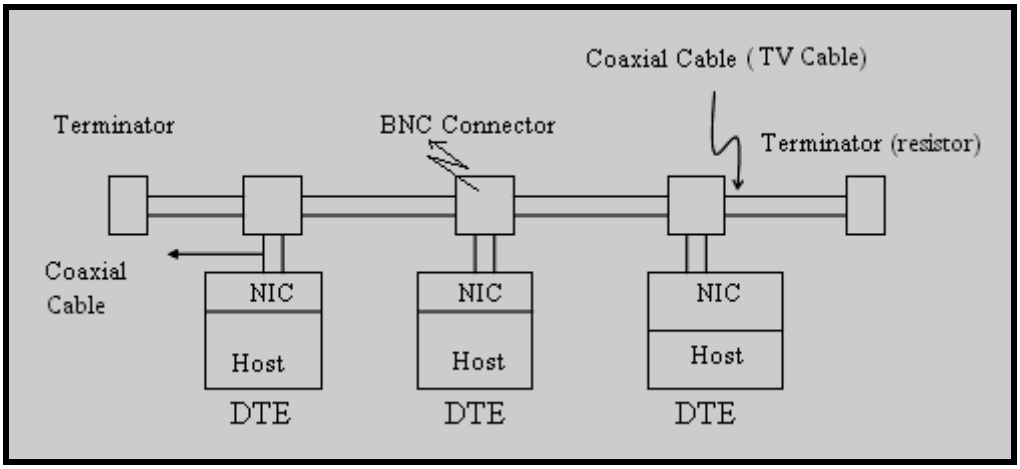


Figure 5.1 Linear Ethernet (10 base 2)

1. **If any host sends data then all other hosts can receive it (broadcast transmission) because the communication medium is common between all hosts.**
2. **If two hosts send data at the same time then the data of both will be destroyed because of the interference between the two electrical signals of the hosts.**

To make this network work properly, it is necessary to organize the hosts' transmissions so that minimum collisions occur. The required organization is realized by the CSMA/CD protocol (MAC protocol).

The Carrier Sense Multiple Access/Collision Detection protocol (CSMA/CD) works as follows:

1. **All hosts are in listening mode i.e. in receiving mode.**
2. **When any host needs to send data, it sense the line , if there is a signal then it retries again after random time interval but if there is no received signal then it can transmit one frame (packet) only.**
3. **While a host is transmitting, it should sense the line signal and compare the received data with the data being transmitted and if they are the same then it continues, otherwise, a collision has occurred and the host should stop transmission immediately and retries after random time interval.**

5.2.2 Ethernet Frame Format

When a host needs to send data to another host, it sends it first to its NIC card which encapsulates it in a proper frame and then sends it across the line. The frame format satisfies the requirements of synchronization, error detection, and physical addressing as shown in Figure 5.2.

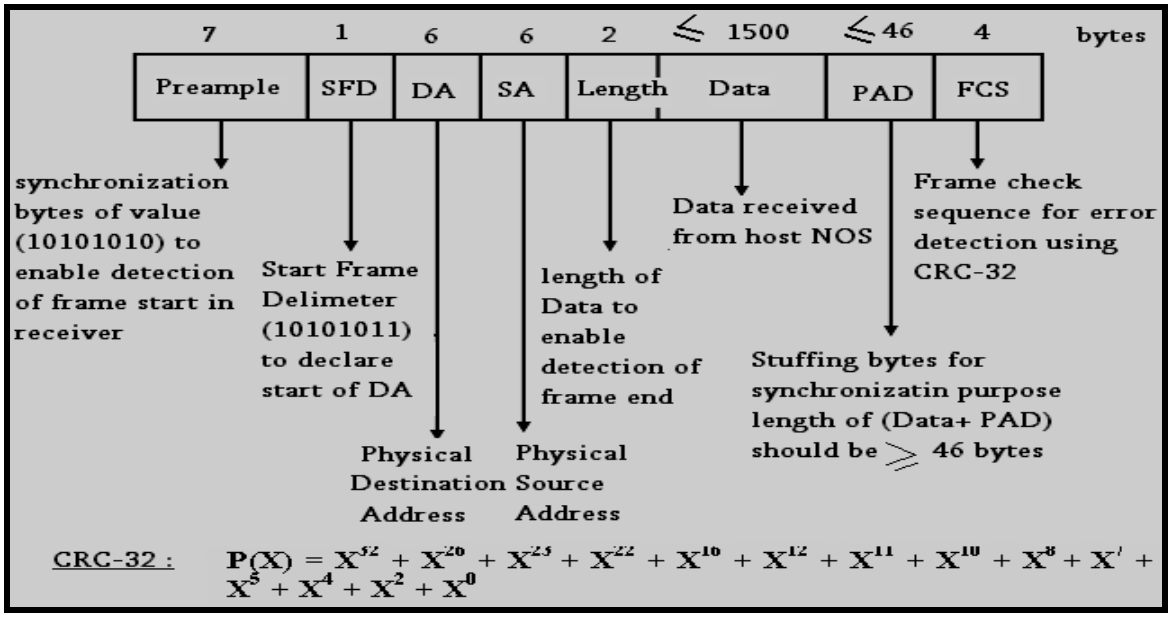


Figure 5.2 Ethernet Frame Format (ARQ is implemented by software in the host).

To enable bit synchronization, the data bits are encoded using "Manchester coding" as shown in figure 5.3.

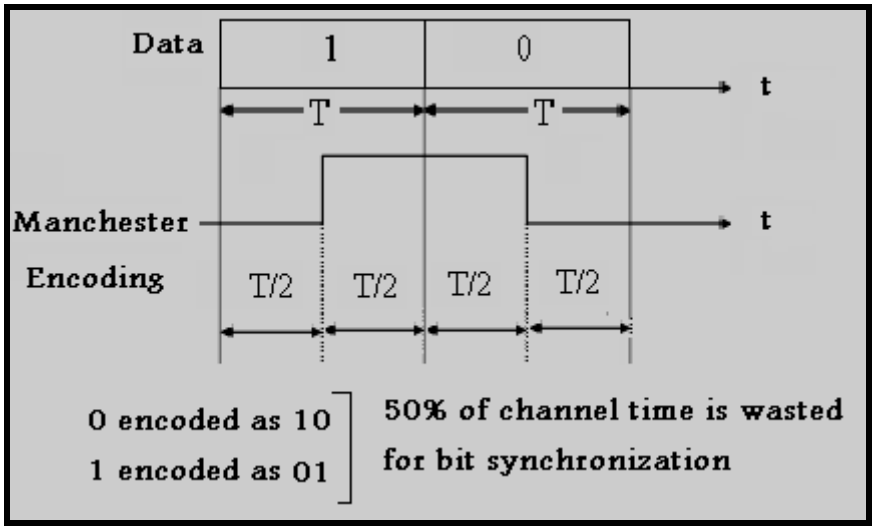


Figure 5.3 Manchester Encoding

5.2.3 Ethernet Types (cabling)

The Standard Ethernet types are:

10 Base 2, 10 Base 5, 10 Base T, 100 Base T, 100 Base F, 1000 Base F where:

- **"Base" means Based Band Signal i.e. binary signal encoded in Manchester.**
- **10, 100, 1000 means 10 Mbps, 100 Mbps, 1000 Mbps.**

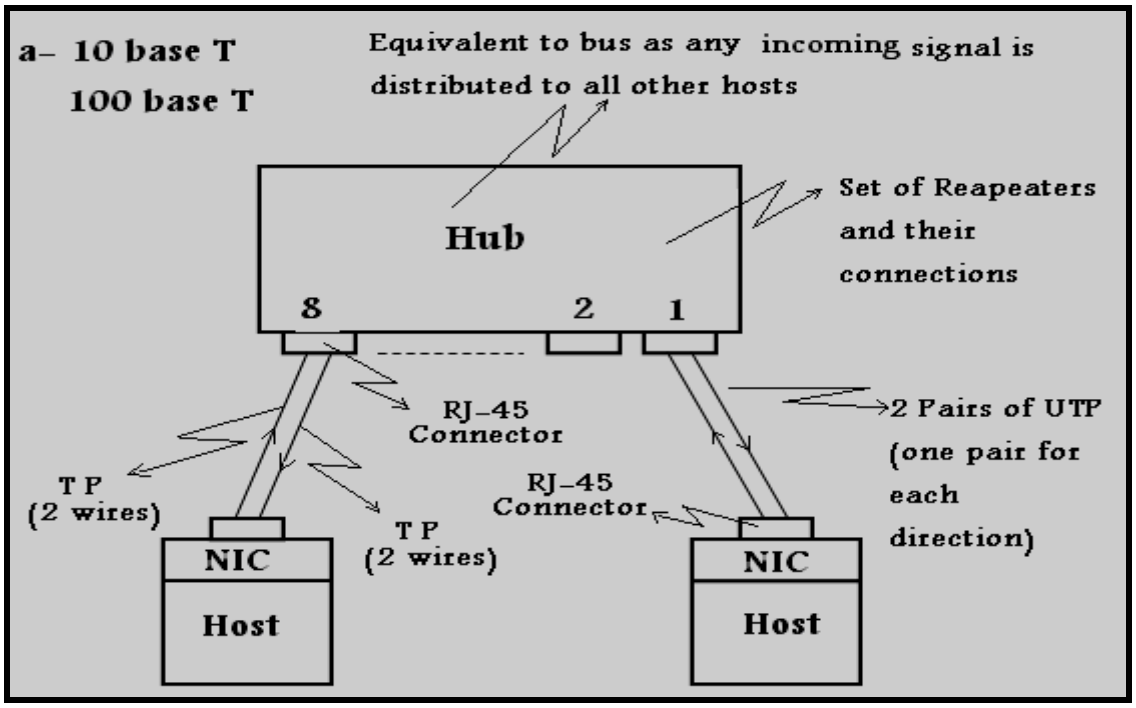
2 : 200 meter of thin coaxial cable (0.5 inch diameter)

5 : 500 meter of thick coaxial cable (0.75 inch diameter)

T : Twisted pair of cat 3 for 10 mbps and cat 5 for 100 mbps

F : Fiber optic

The topologies of these types are shown in figure 5.4.



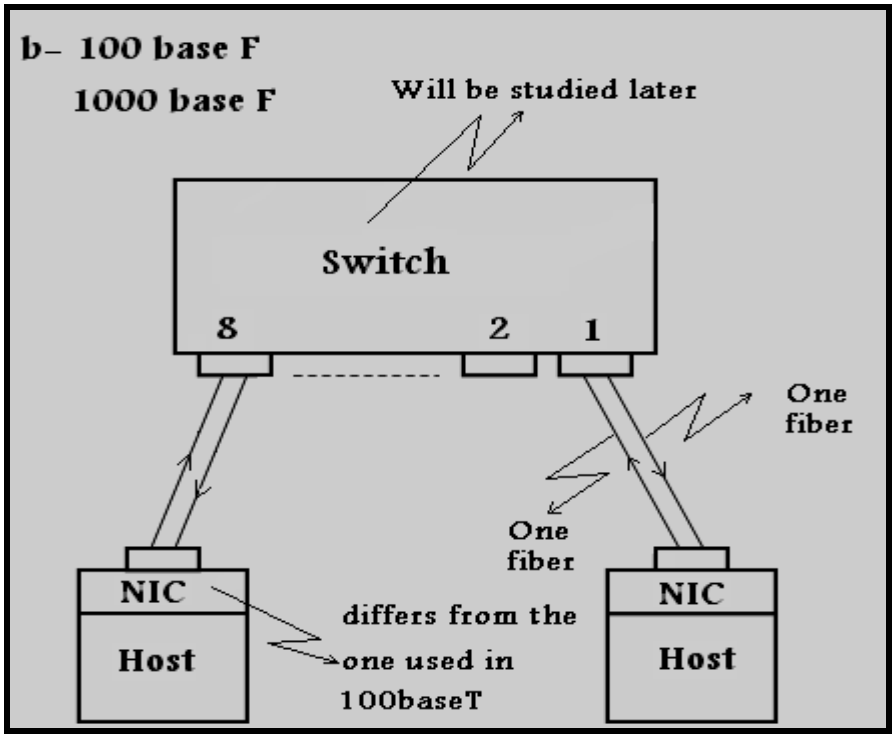


Figure 5.4 Ethernet Topologies (10 Base 2 is shown earlier)

5-2-4 Ethernet Devices

These devices are useful in building very large LAN consisting of thousands of hosts and spanning over several buildings with the capability to be connected to external networks. Examples of the devices are repeater, hub, switch, bridge, router, gateway, etc.

5-2-4-1 Repeater

It regenerates (amplify) the binary signal, so that it can travel longer distance as shown in figure 5.5.

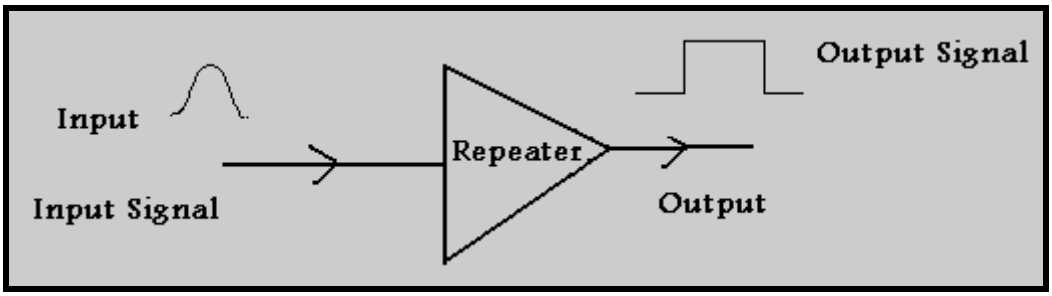


Figure 5.5 Repeater

5-2-4-2 Hub

It is a collection of repeaters and connectors so that we can get star topology in addition to repeater action as shown in figure 5.6.

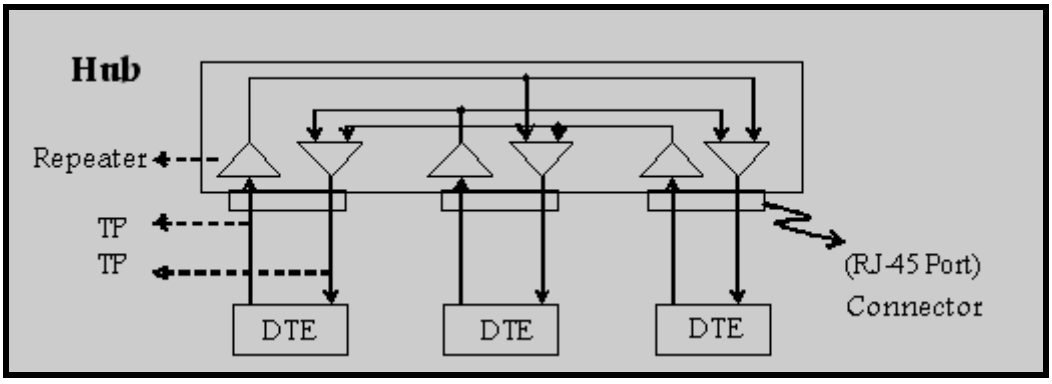


Figure 5.6 Hub Block Diagram.

The main advantage of Star connection is that any host can be disconnected without affecting network operation.

5-2-4-3 Switch

The switch outlook is similar to hub but there are extra functions. The main extra function is the switch capability to detect MAC addresses in Ethernet frame and sends data to destination port (host) only.

This function decreases collisions and allows multiple transfers to occur concurrently in a similar way to telephone switch (exchange). The switch device enabled the increase of number of hosts in LANs and also enabled the tree topology that can spans several buildings as shown in figure 5.4. It is important to note that there are many types of switches with different specifications.

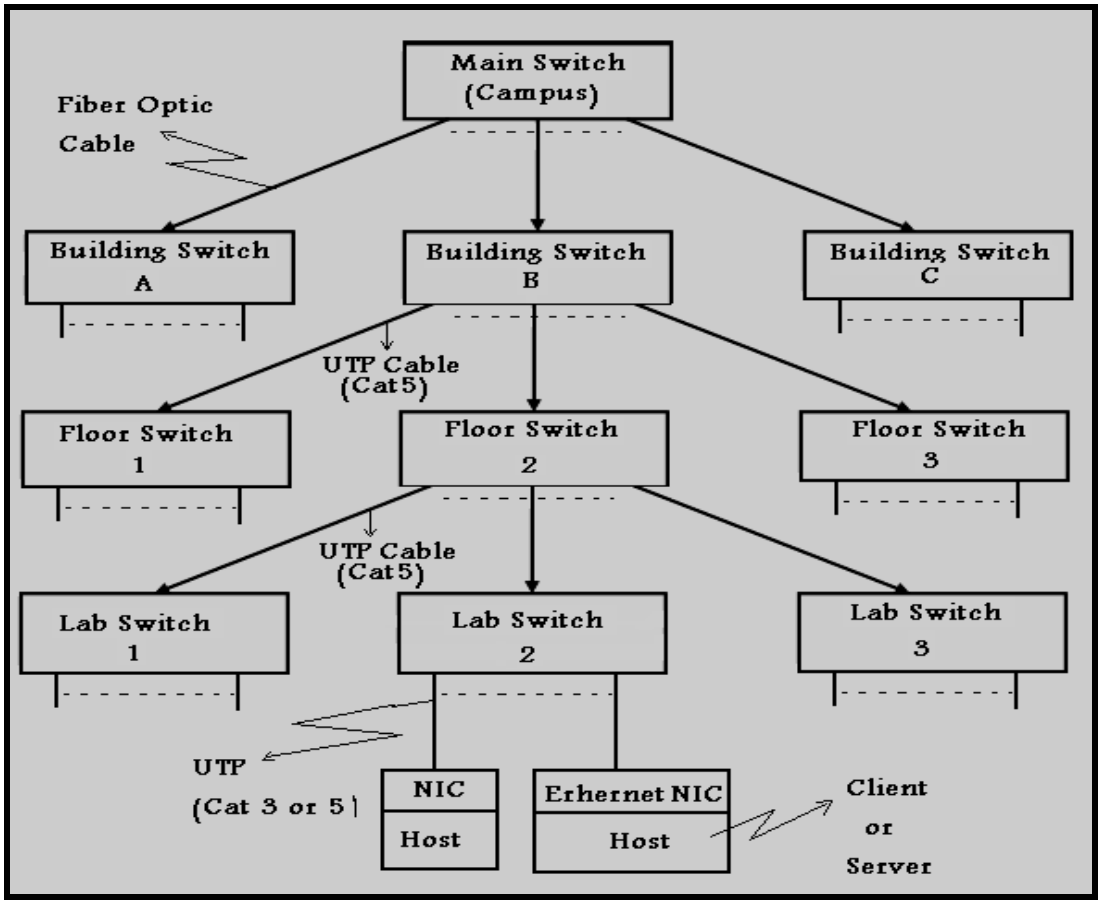


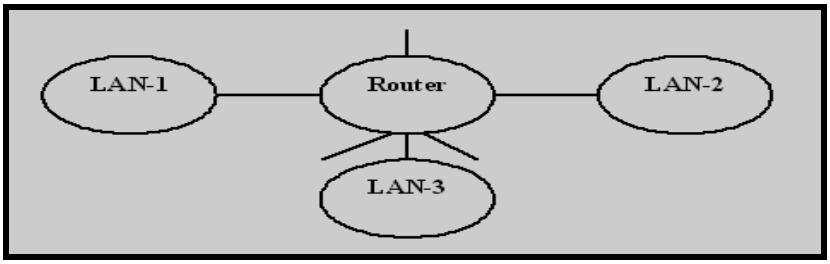
Figure 5.7 Tree Ethernet.

5-2-4-4 Router

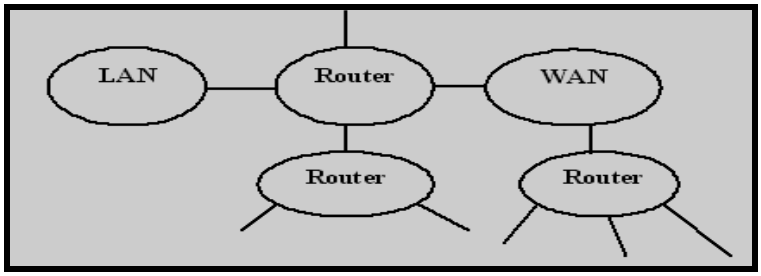
Router is a very fast computer which can do many things such as:

1. **Receiving frames from neighboring devices (linked device) and performing error control.**
2. **Detecting logical addresses inserted in the packet header and route the packet accordingly using a proper routing algorithm.**
3. **Capability to change frame format and packet format and hence can connect different LANs and WANs together as shown in figure 5.8.**
4. **Capability to communicate with other routers in the network to collect the necessary information for routing.**
5. **Other functions.**

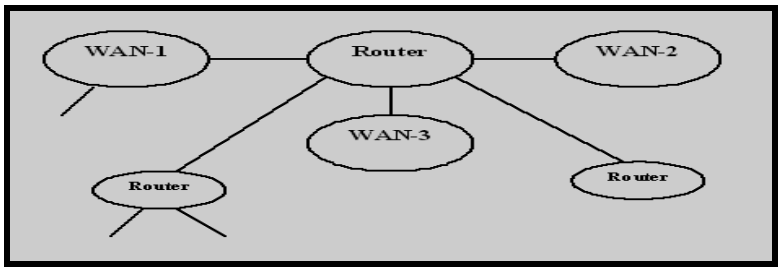
The Router is more expensive than other network devices and may need special training to use it properly. This means that it is not for use with Ethernet only but for many networks and applications as shown in figure 5.8.



a- Router for connecting different LANs



b- Router for connecting LAN to WAN

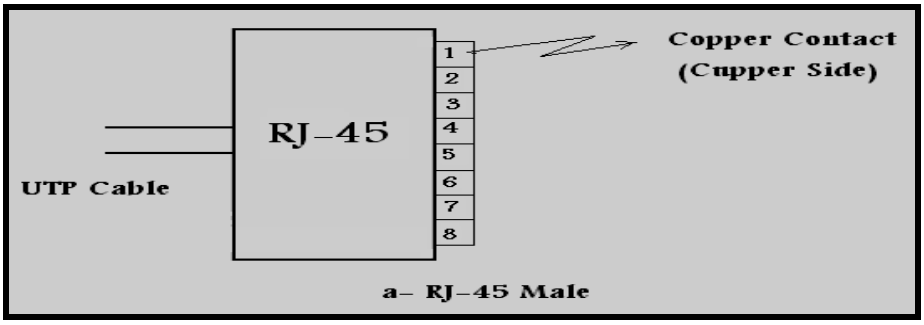


c- Router for connecting different WANs

Figure 5.8 Router Applications

5-2-5 Ethernet Wiring

The wiring of Ethernet is carried out according to a specified standard as in figure 5.9.



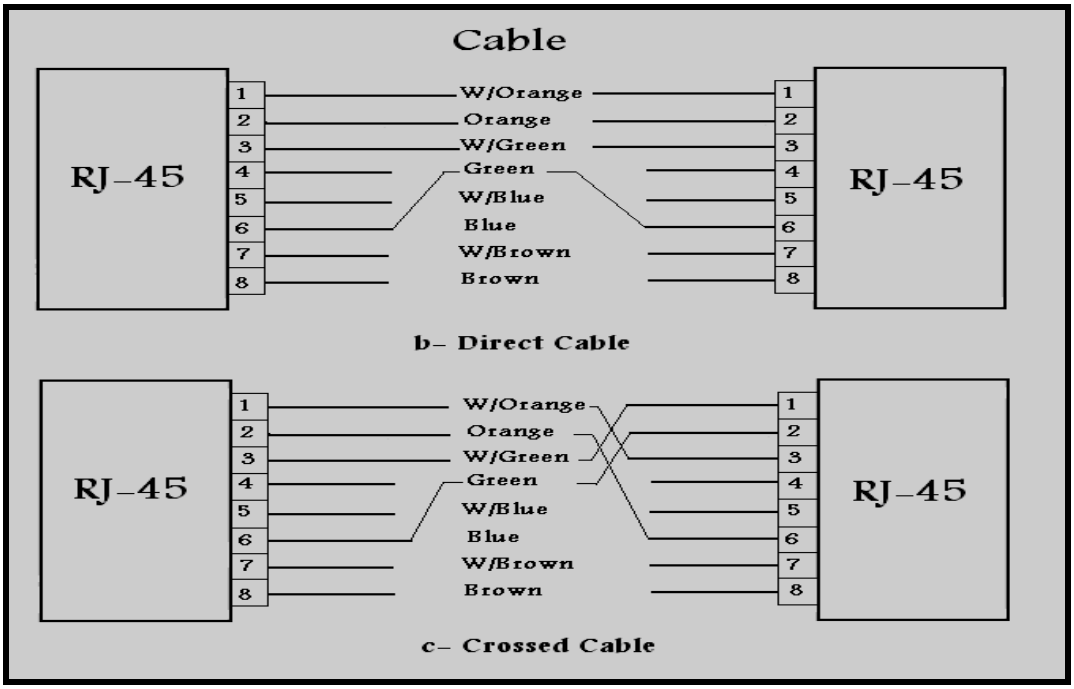


Figure 5.9 wiring of RJ-45 & UTP.

The applications of direct and crossed cables are shown in figure. 5.10. This type of connection is due to the different functions of contacts (wires) in each device as shown in figure 5.11.

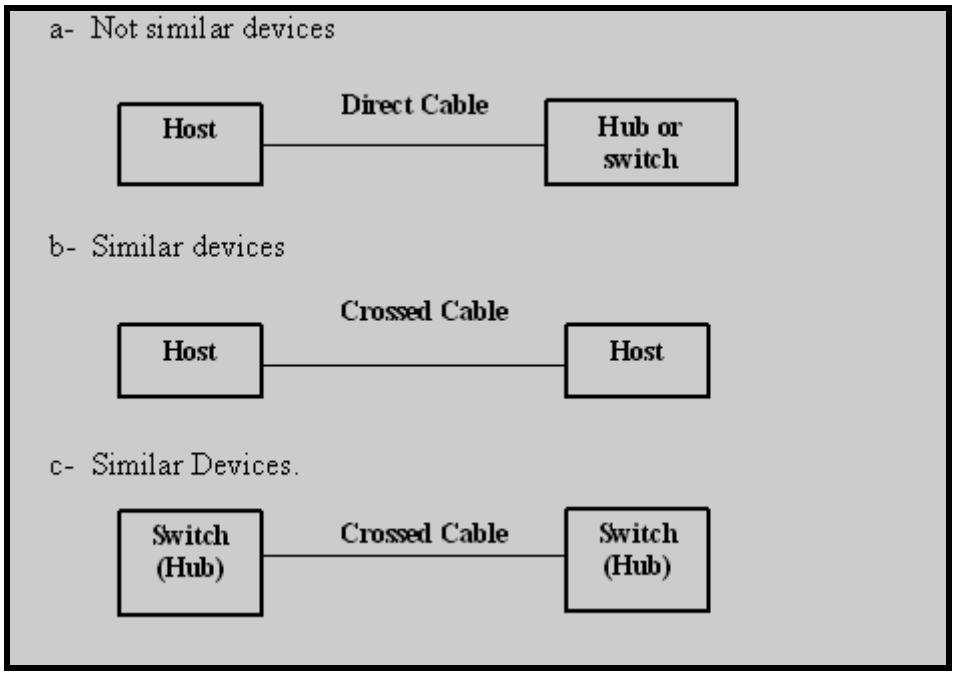


Figure 5.10 Applications of Direct and Crossed Cables.

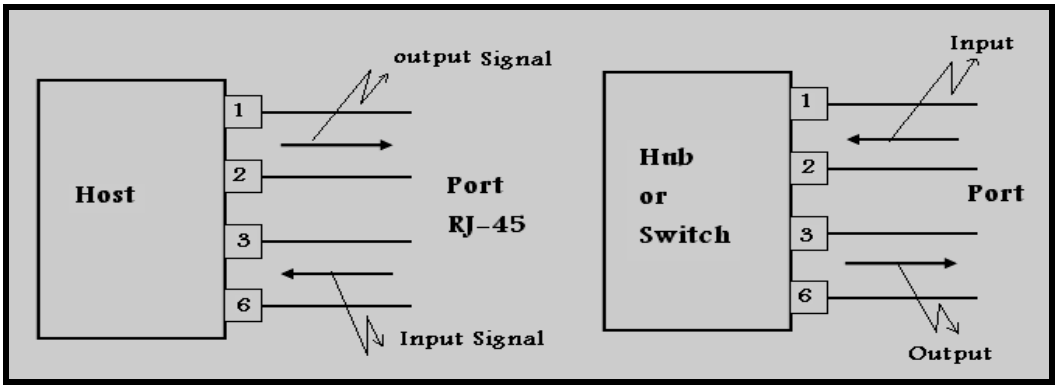


Figure 5.11 RJ- 4-5 ports

5-3 Token Ring LAN (IEEE802.5)

The topology of this LAN is shown in figure 5.12.

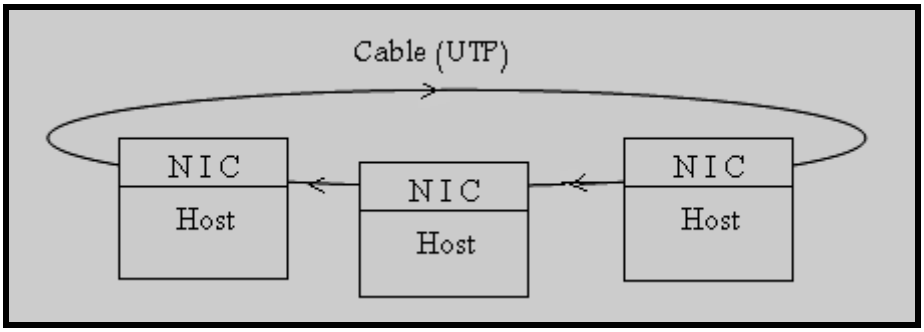


Figure 5.12 Token Ring LAN

The frames in this LAN pass from one NIC to the next one in circular fashion. If any NIC breaks down, the whole LAN will break down as well. This LAN uses two types of frames which are "Token" and "data" as shown in figure 5.13. The operation can be described as follows:

- **When no host is sending data, the token passes from NIC to NIC continuously.**
- **When any host needs to send data, it holds the Token and start sending data frames, for a specified time interval and then releases the Token.**

The other details will not be discussed here.

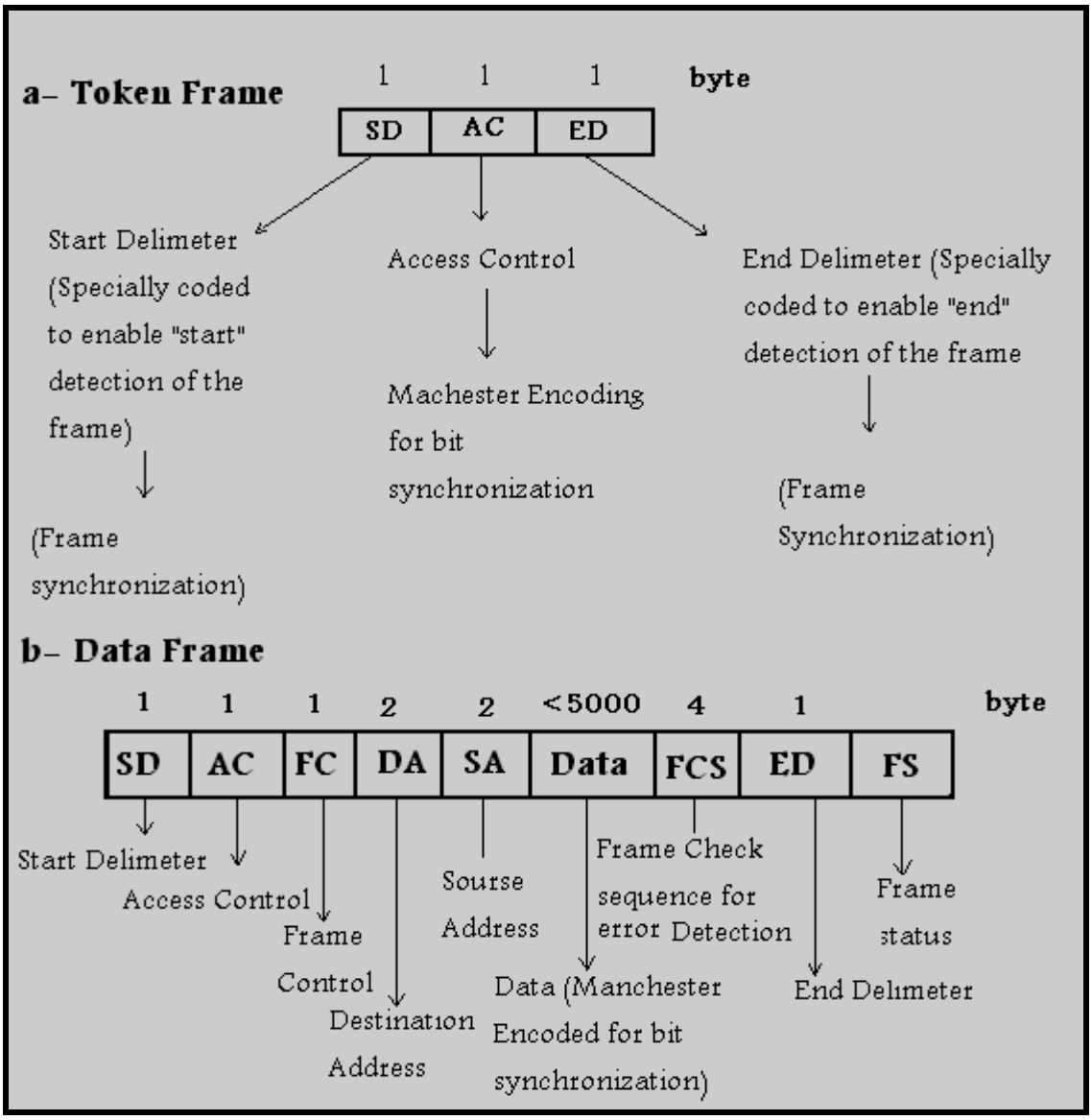


Figure 5.13 Frame Format in Token Ring.

5-4 Wireless LAN

These LAN, use "Radio Waves" or "Infra Red Waves IR" and have two main topologies (Adhoc and Infrastructure) as shown earlier in chapter 1.

The famous standard wireless LAN, are:

1- Hyper LAN:

- **European standard**
- **Range : 50 meter**
- **Bit rate : 10 – 20 Mbps**
- **Wave Radio**
- **Modulation QPSK**
- **MAC: CSMA/CD or CSMA/CA**

2- IEEE 802.11:

- **American standard**
- **Bit rat : 1- 10 Mbps according to type of wave and modulation**
- **Range : 100 meter**

The main features of wireless LAN, are:

- **Relatively low speed and short distance**
- **Easily accessed by outsiders and hence relatively low security.**

The main application of wireless LAN, are:

- **Portable computer networks (Adhoc).**
- **Portable to fixed network (Infrastructure).**
- **Fixed network where cables are not easily available.**
- **Demonstration LANs on fields.**
- **Others.**

5-5 Type of Transmission

The main types of data transmission in a computer network are:

1- **Broad cast: one host is sending while all other hosts are receiving as the case of 10base2 Ethernet LAN.**
2- **Point to Point: One host is sending and one is receiving as the case of communicating with a web server via WAN network.**
3- **Multi cast: one host is sending while a group of hosts are receiving (not all hosts).**

Chapter 6

OSI and TCP/IP standards

6-1 Introduction

A computer network may be looked at as a set of distributed programs communicating together across a proper hardware infrastructure.

The infrastructure is called as a "physical layer" while the programs are usually considered as several layers with proper names.

The work in TCP/IP standard started in early 1970s while OSI started later in early 1980s. Both standards are applicable in all types of networks (LAN, MAN, WAN). The TCP/IP is implemented in reality and the best example is the Internet.

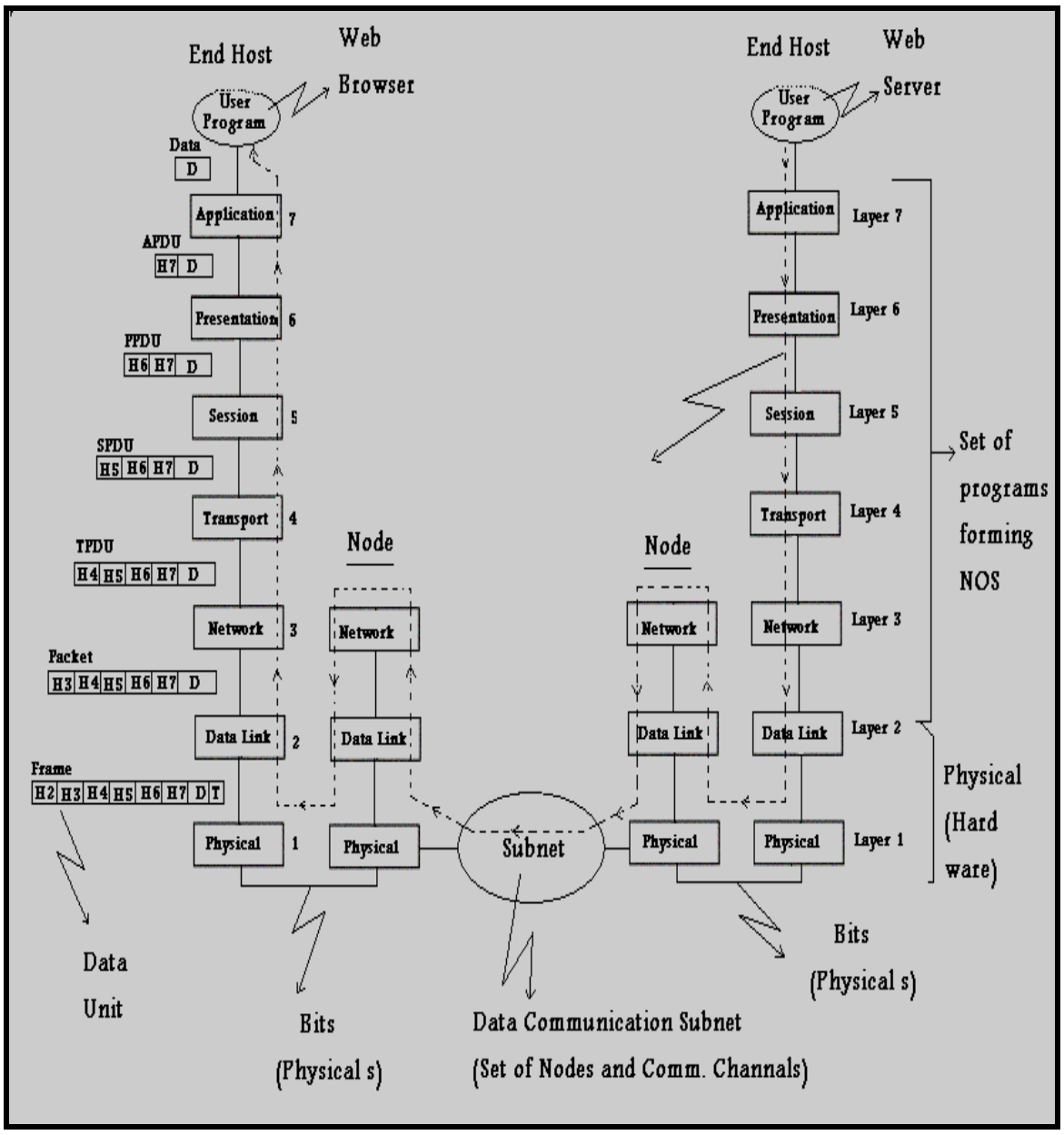
The OSI is not implemented and acts as theoretical guidelines for understanding and designing computer networks.

6-2 OSI Standard

The Open System Interconnection "OSI" standard was developed by the International Standard Organization (ISO) belonging to United Nations (UN). OSI is based on designing a computer network as seven layers as shown in fig 6.1 where we notice the followings:

1- **There are two type of devices:**
   - **End Host such as client computer or server computer.**
   - **Node which is intermediate device such as switch, router.**
2- **The network layers in end devices are seven while in intermediate devices are three.**

3- **Layers are basically "programs" resident in device computer memory. These programs implements the task assigned to the layers. The main feature of these programs is the way they interact with each other. From the figure, it is clear that each program has relations (Interface) with only two other programs.**
4- **Each layer provides service to adjacent upper layer and requests services from adjacent lower layer.**
5- **Data can pass in any direction. When passing in lower direction, it is encapsulated into data units i.e. proper headers are added. When passing in upper direction, the data unit is stripped off its headers. Also, it should be noted that in end hosts, either encapsulating or stripping off occurs to any data unit while in nodes, both operations occur.**
6- **The headers (H_7, H_6, H_5, H4) are not important for nodes and treated there as data but in hosts they are of essential importance.**
7- **The headers (H_3, H_2) are important in all devices (End and intermediate).**
8- **When a header is generated (produced) in any device, it will not be used by that device but by the adjacent or end device. This means that the header carries information necessary to tell the other device what to do. The header information can be called as "layer protocol information" e.g. H_3 carries "layer 3 protocol information".**
9- **Layers (7, 6, 5, 4) have "End to End protocols" while layers (3, 2) have "Adjacent to Adjacent protocol" or sometimes called "Node to Node".**
10- **The header contents and functions will be cleared after studying the layers' functions.**



NOS= Network Operating System, PDU= Protocol Data Unit

H= Header, T= Trailer, Node= Router or others

Figure 6.1 OSI Model of Computer Network

The functions of layers and their interfaces are quite complicated; therefore, we are going to summarize them very briefly as follows:

1-Physical Layer:

Non reliable bit transfer between adjacent devices using physical circuits and connections. This layer constitutes the physical infrastructure of computer network.

2-Data Link Layer (DLL):

Reliable frame transfer between adjacent devices. DLL consists of two sub layers:

- **Mac sublayer: responsible of frame detection (synchronization), physical addressing, and error detection. This sub layer is usually implemented in the Network Interface Card (NIC) and differs from network to another.**
- **LLC (Logic Link Control): responsible of error control, flow control, interface to network layer. LLC is implemented purely in software and it is part of NOS. LLC is not dependent on MAC sub layer.**

3-Network Layer:

Non reliable packet transfer between End hosts using proper routing algorithms. In this layer, logical addresses are introduced. Here, it should be noted that the reliability (error free) of links between adjacent devices dos not imply error free packet transfer between end hosts because the node may break down (power off, faults) after having sent "ACk" messages acknowledging the correct reception of packets.

4-Transport Layer:

Reliable packet transfer between End processes running in the "End Hosts". This layer uses the "Port Address" which defines the process identification within the host. Transport layers buffers application issues from data transfer issues.

5-Session layer:

Establishes sessions between end processes and control dialog between them using "Check Pointing" and other means. Check pointing enables the resumption of long file transfer from the point where it was stopped.

6-Presentation Layer:

Responsible of data format, data compression, encryption, and others.

7-Application Layer:

Provides means for user application programs to access the network environment.

Finally, it is worth noting that design issues, studied earlier, have to be considered during network design.

6-3 TCP/IP Standard

This standard was developed by USA ministry of defense for its network which was called as "ARPANE". This standard is very popular, used in LANs and WANs, and particularly used in "Internet".

TCP/IP came before OSI, however, there is a good similarity as both adopted the layered architecture (see figure 6.2).

<table>
<tr><th>OSI Layer</th><th>TCP/IP Layer</th><th>TCP/IP Protocol</th><th>TCP/IP Address</th></tr>
<tr><td>Application
Pressentation
Session</td><td>Application</td><td>FTP, SMTP,
HTTP, TELNET</td><td>None</td></tr>
<tr><td>Transport</td><td>Host to Host
(Transport)</td><td>TCP
UDP</td><td>Port
Address</td></tr>
<tr><td>Network</td><td>Internet
(Interworking)</td><td>IP
ARP</td><td>IP
Address</td></tr>
<tr><td>Data Link
Physical</td><td>Host to Network
(Network Interface)</td><td>Ethernet
Token Ring
X.25</td><td>Physical
Address</td></tr>
</table>

Figure 6.2 TCP/IP and OSI Models

There are famous protocols already implemented in TCP/IP such as TCP, IP, UDP, HTTP, SMTP, FTP, TELNET, etc. Some of these protocols will be studied below. The addressing scheme uses the following types of addresses:

1- Physical address: assigned physically (electronically) by the NIC's manufactures. Each address defines one host in the network.
2- IP address: logical address assigned by network administrator or NOS to define one host in the network (global address).
3- Port address: logical address assigned automatically by NOS to define one process (user application program) in the host (local address).
4- Socket: Combination of IP address and port address and hence it define one process in the whole network (Full address).

6-3-1 IP Protocol (Internet Protocol)

It ensures non reliable packet transfer between end hosts using the format shown in fig 6.3.

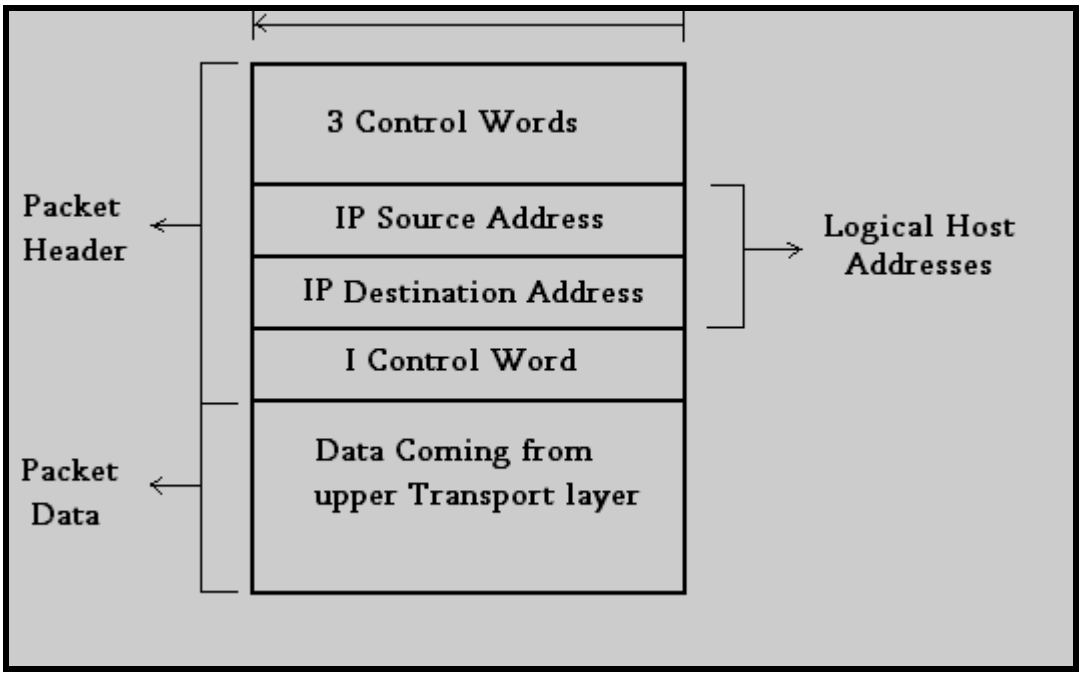


Figure 6.3 IP Packet Format

IP protocol operates in the network (Internet) layer and uses IP addresses for source and destination. IP addresses are essential for operation of the routers when used in the network.

6-3-2 TCP Protocol (Transmission Control Protocol)

It ensures reliable packet transfer between end processes in the end hosts. This protocol uses port addresses as shown in figure 6.4. TCP is connection oriented Protocol as it uses the concept of "Virtual call" where the data path is determined (reserved) before starting data transfer and then all data packets follow that path only.

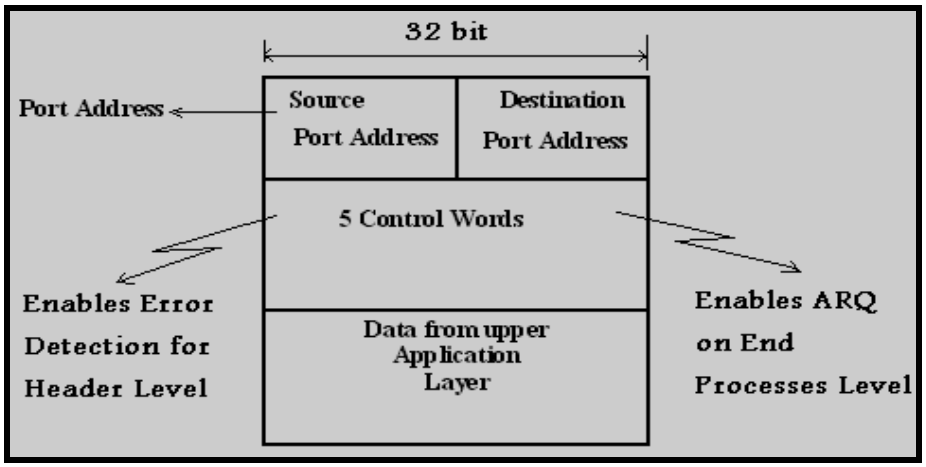


Figure 6.4 TCP Data Unit Format.

6-3-3 UDP (User Datagram Protocol)

This protocol is connectionless i.e. no path is reserved beforehand for data transfer. Each sent data packet may follow any path assigned by the routers. UDP is called "Datagram" protocol and it is responsible of transferring the data packet between end processes, however, this transfer is not reliable as "ACK" messages are not used.

6-3-4 ARP Protocol

The Address Resolution protocol "ARP" is capable of finding the physical addresses corresponding to IP addresses. This means that if we know IP address then we can find the corresponding physical address used in MAC sub layer. ARP relies in its operation on "Broadcasting Messages" i.e. messages that are sent to all devices.

There is reverse protocol (RARP) which enables user to find IP address if the physical address is known.

6-3-5 Other Protocols

- **HTTP: Hyper Text Transfer Protocol used for Web applications.**
- **SMTP: Simple Mail Transfer Protocol used for Email applications.**
- **FTP: File Transfer Protocol used for Download applications.**
- **TELENT: Used for "Remote Login" applications where a remote user can login to a multi-user computer system and works as if he was a local user.**
- **Many Others.**

6-3-6 Data Units in TCP/IP

These data units are shown in figure 6.5. From this figure, we notice that the out put frame from any host includes original data and control data. The control data are set of headers acting as command messages to neighboring node (router) and to end process in the end host. When a frame is received by a router, the control data (H_H, H_I, T) are used but the rest (H_T, H_A) are not used, however, all control data are used in the end host. It is worth noting that a router will strip off (H_H, H_I, T) during reception and rejoin them (encapsulate) during transmission but with different values.

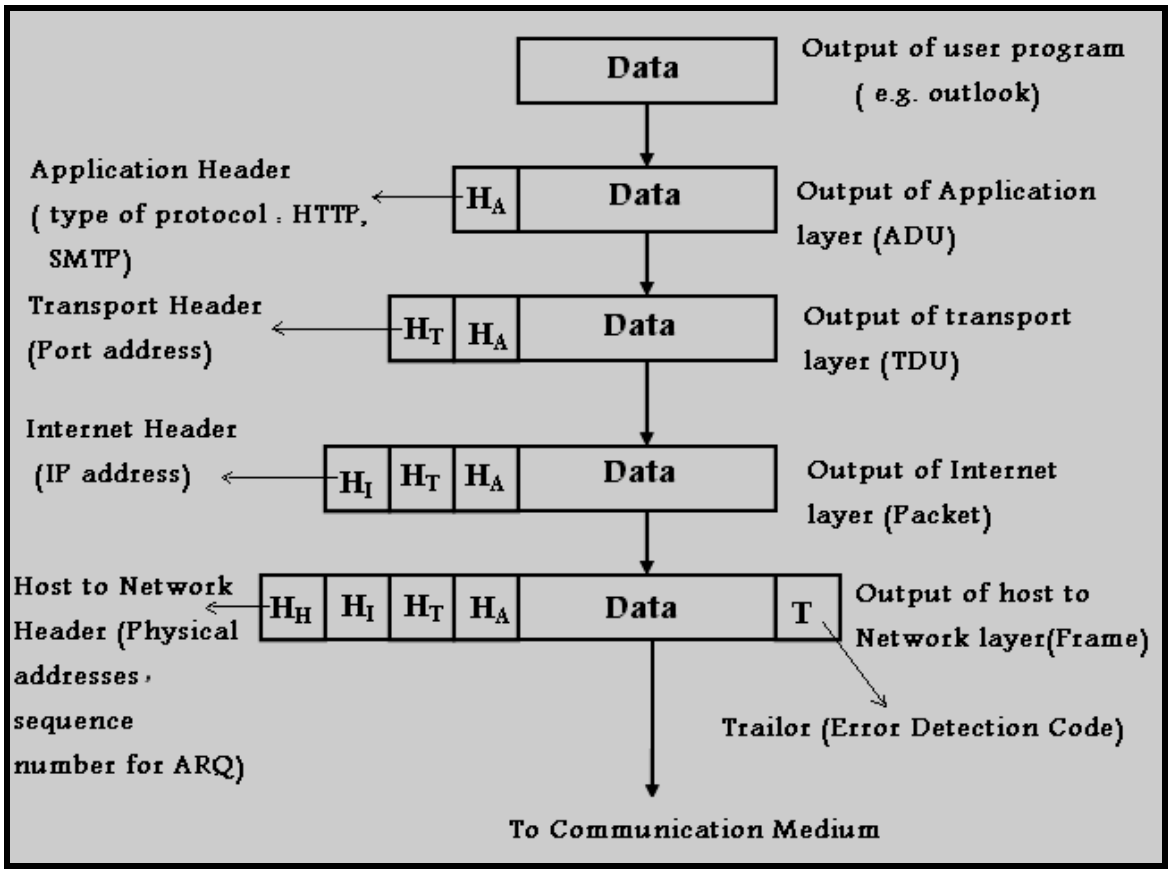


Figure 6.5 Data Units (DU) in TCP/IP.

6-4 General Relationships of Layers and Devices

When manufacturing a network device, it is designed to operate in certain layer. This means that the device will make use of headers belonging to that layer and the ones underneath.

For example, a hub is designed to operate in physical layer and hence it does not make use of any header at all, while, a router is designed to operate in layer 3 and hence it makes use of H_3 and H_2.

The switch is designed usually to operate in layer 2 and hence it makes use of H_2 but not of H_3 and higher.

Also, it is worth noting that, generally, when a device receives a data unit it stips off the headers to be used, however, it had to encapsulate them again during transmission but with different values.

6-5 Relationship of NOS and Layers

As mentioned earlier, each layer (except physical layer and MAC sub layer) is implemented by a program. The whole implementation of layers (set of programs) constitutes the NOS. The NOS in a host can be an integral part of its operating system (OS) or can be loaded as separate components communicating with original OS as shown in figure 6.6.

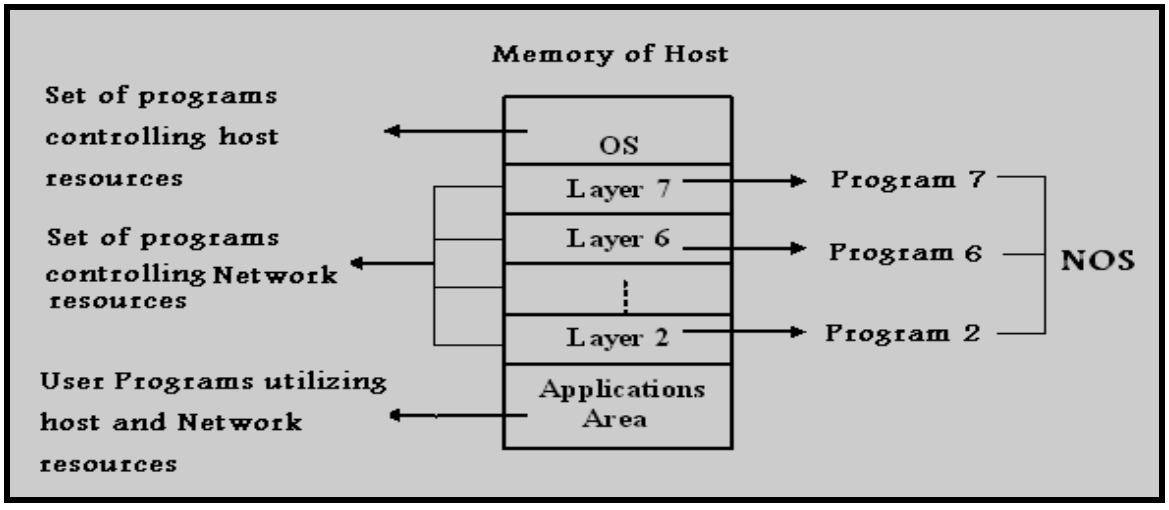


Figure 6.6 NOS and OS

The NOS in a host differs according to host functions i.e. whether it acts as a client, a server, or several servers as shown in figure 6.7. In this figure we notice the followings:

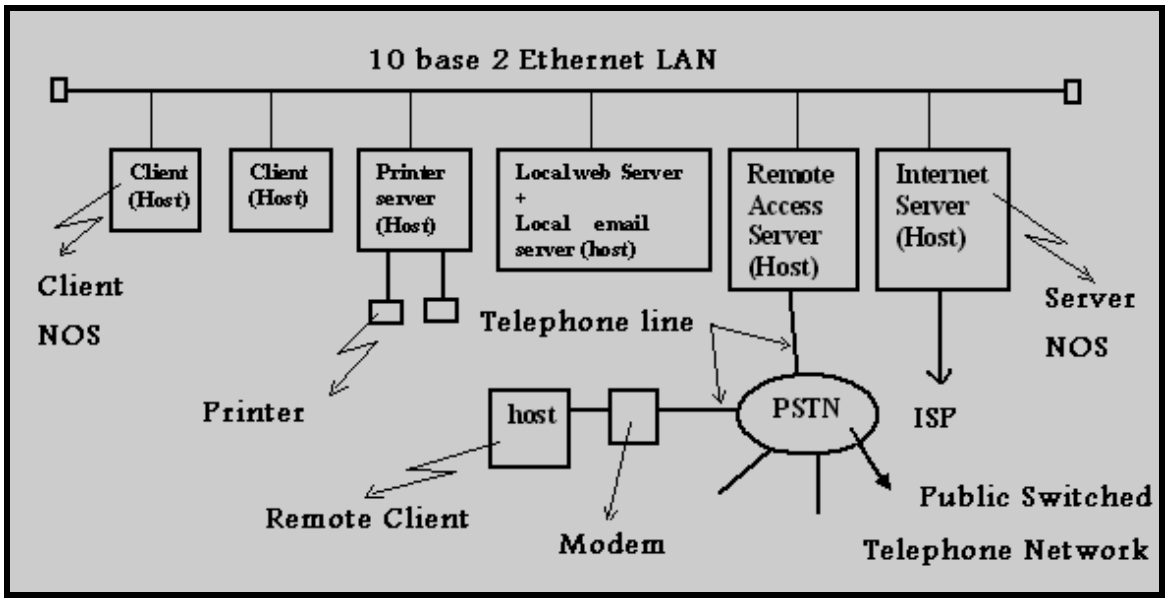


Figure 6.7 Types of NOS in Hosts.

1- **There are many types of servers i.e. server NOS such as:**

- **Web Server: Allows storage and retrieval of web pages for local and remote users (clients).**
- **Email Server: Allow storage and retrieval of emails for local and remote users (clients).**
- **Internet Server: Allows local clients to access outside Internet via Internet Service Provider (ISP).**
- **Remote Access Server (RAS): Allows remote clients to access LAN via telephone lines.**
- **Print Server: Allows several printers to be connected to one host which then can provide print service to local and remote clients.**

2- **More than one server can be resident in one host and hence it acts as several servers at same time.**

Chapter 7

TCP/IP Protocol and IP Addressing

7.1: Introduction:

Transmission Control Protocol/Internetwork Protocol (TCP/IP) is a set of protocols, or protocol suite, that defines how all transmission are exchanged across the internet. Named after its two most protocol, TCP/IP has been in active use for many years and has demonstrated its effectiveness on a worldwide scale.

7.2: TCP/IP Components:

In 1969, a project was funded by the Advanced Research Project Agency (ARPA), an arm of the U.S. Department of Defense. ARPA established a packet-switching network of computers linked by point-to-point leased liens called Advanced Research Project Agency Network (ARPANET) that provided a basis for early research into networking.

TCP/IP and the concept of internetworking developed together. TCP/IP concepts can be described as follow:

- Operate as ***Single Network Connecting many Computers*** of any size and type.
- There are many ***HOSTS*** (A, B, C,…). A ***HOST*** on TCP/IP is a computer.
- ***Routers*** or ***Gateways*** (solid circles in Figure below).
- Separate Physical Networks (larger Ovals containing Roman numbers).

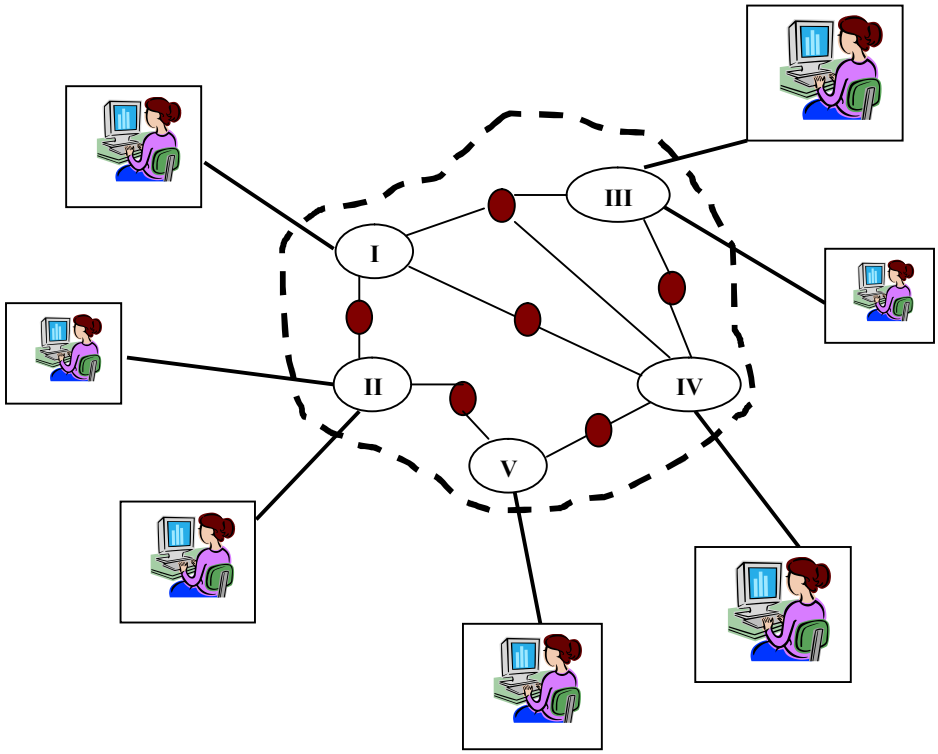


Figure 5.1: An Internet seen by TCP/IP.

7.3: How TCP/IP WORK?

In this section, we will describe the TCP/IP protocol layers and the function of each layer as follow:

Application Layer:

Transport Layer:

Internet Layer:

Network Access Layer( ):

7.4: IP Addressing:

Any network can be managing make that transmission operation via protocol TCP/IP must be has a unique number to describe and illustrate it, this number called "NETWORK ADDRESS". Every device which is a member in the network also must have a unique address to define it and distinguished from other devices, this number called (IP-Address).

The most important idea, we must understand HOW this address can be created or established, which can be used later to access a required network, then access requires device.

IP address has 32-bits in length and written using 4 integer decimal numbers separated by "dot". Each part named "Octet" and has 8-bits (1-byte). These 4 separated parts can be divided into two groups, The First one refers to "Network ID" and the second part refers to the "Host ID" as in figure below:

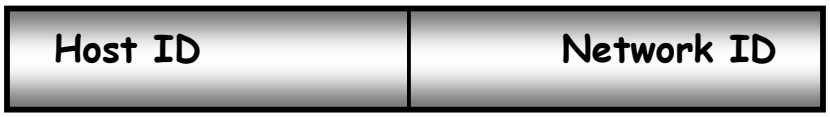


Figure 5.2: IP Address

In a specific network (same network), many devices has the same part which refers to "Network ID", the difference only the part that refers to Host or device address.

In addition, the Network ID in IP address may be difference dependent on the "Network Class" which can be describes as follow:

- **Class A addressing.**
- **Class B addressing.**
- **Class C addressing.**
- **Class D addressing.**
- **Class E addressing.**

Each class can be recognized from other via the First byte (MSB) in each IP address.

7.4.1: Class A Addressing:

The description of this class can be as follow:

- The first BIT from First BYTE always contain "0" zero.
- The first BYTE specified to "**NETWORK NUMBER (ID)**", the rest (24-bits) specified to the "**Device/Host address**" in this network.
- We can address (2^{24} -2 = 16777214) device. We subtract 2 from whole number, because we must reserve the 1^{st} which represent "**Network address**" and final number which represent "**Broadcast address**". This type of classes used to do addressing for **VERY Large Networks.**
- We can define 2^7 =128 Network except (Number (0) Unused) and (Number 127) which used for special used named (Back Test). Therefore the remaining number of networks can addressing is 126 different networks.

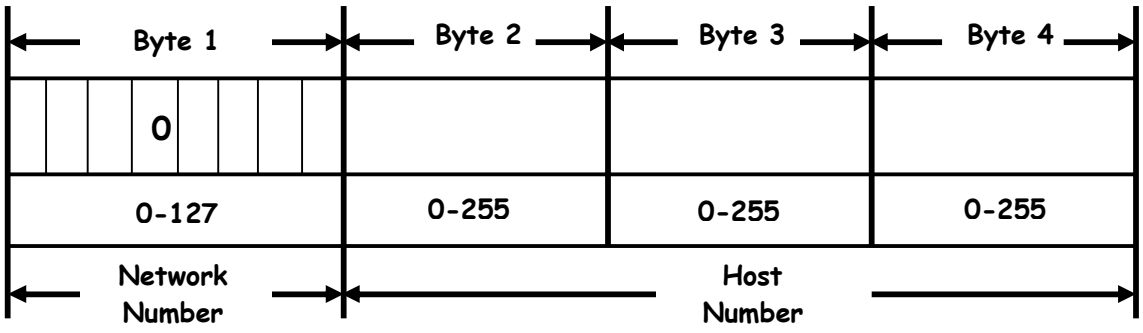


Figure 7.4: Class A addressing.

EXAMPLE: 75.4.10.8

75 : represent Network Number.

4.10.8 : represent the device/Host number belongs to the network

7.4.2: Class B Addressing:

The description of this class can be as follow:

- ☒ The first two BITS from First BYTE always contain "10" one-zero.
- ☒ The first 2-BYTE specified to "**NETWORK NUMBER (ID)**", the rest (16-bits) specified to the "**Device/Host address**" in this network.
- ☒ We can address (2^{16} -2 = 65534) device. This type of classes used to do addressing for **Large Networks**.
- ☒ We can define 2^{14} =16384 Network with range (128-191), therefore the first byte for this range and the second byte between (0-255).

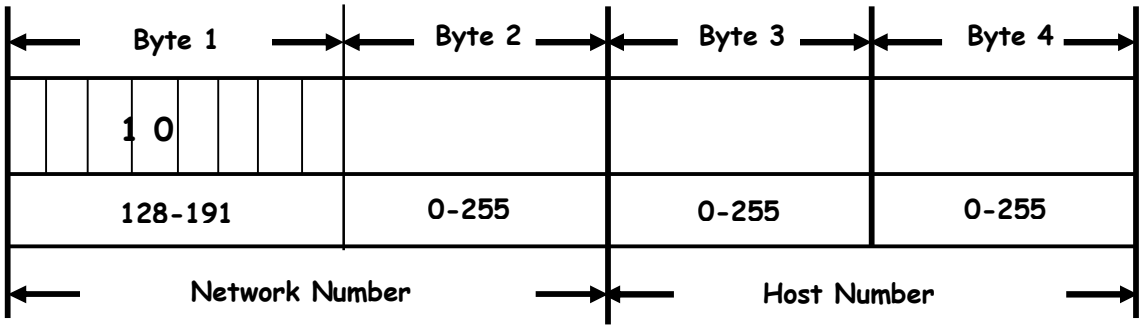


Figure 7.5: Class B addressing.

EXAMPLE: 139.144.50.56

139.144 : represent Network Number.

50.56 : represent the device/Host number belongs to the network.

7.4.3: Class C Addressing:

The description of this class can be as follow:

- ☒ The first Three BITS from First BYTE always contain "110" one-one-zero.
- ☒ The first 3-BYTE specified to "**NETWORK NUMBER (ID)**", the rest (8-bits) specified to the "**Device/Host address**" in this network.
- ☒ We can address (2^8 -2 = 254) device. This type of classes used to do addressing for **small Networks.**
- ☒ We can define 2^{21} =2097152.
- ☒ As in other classes, the first byte from Network ID used to identify the network with range (192-223).

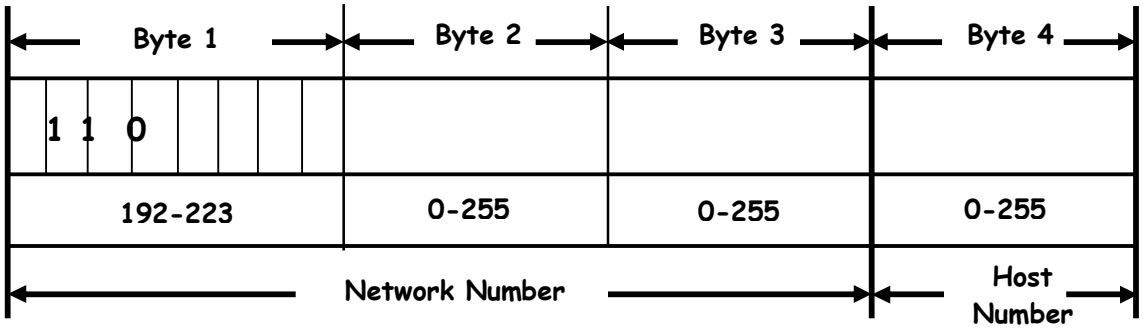


Figure 7.6: Class C addressing.

EXAMPLE: 193.5.2.7

193.5.2 : represent Network Number.

7 : represent the device/Host number belongs to the network.

7.4.4: Class D Addressing:

This type used in broadcasting operations for a group of users named "**Multicasting Group**". Each group contains a unique **Host** or more or the group is empty. The first **4-Bits** in this addressing always contain "**1110**" and the rest refers to the specific group which this host belong it. In this class, there is no part for the Network Address.

Addresses for this class in range: (224.0.0.0)-(239.255.255.255).

7.4.5: Class E Addressing:

This type used to do specific experiments by the Internet NIC; therefore this class is not used in designing networks. The first **4-Bits** in this addressing always contain "**1111**".

I.e. the addresses in this class start in range: (240.0.0.0)-(254.255.255.255).

NOTES: General Notes about the three main classes (A, B, and C).

- ☒ The numbers in these classes are International registered numbers.
- ☒ There are other numbers not registered for these classes can be described as follow:
  - **Class A:** from (10.0.0.0) to (10.255.255.255)
  - **Class B:** from (172.16.0.0) to (172.31.255.255)
  - **Class C:** from (192.168.0.0) to (192.168.255.255)

7.5: Subnet Mask:

Every device in the network need to a number created form 32-bits in addition to the IP named subnet mask.

The subnet Mask either an automatic number (default) which used when the network not partitioned into small networks OR may be a number putted by the network administrator when the network portioned into small networks.

The subnet mask use binary numbers to represent this mask. **1** for each part has a relation with ***NETWORK ID*** and the **0** used for the ***DEVICE/Host ID***.

The subnet mask number relates to compute the Network Number and the Broadcast Address as follow:

- **Compute Network Number**: this can be done via the **ANDING** between the **IP Address** and the **Subnet mask number.**

Example#1: if the subnet mask number is 190.15.30.180, find the Network Number?

Solution: we must find the class i.e. this number from **class B**? How?

Network ID : 190 .15 .0 .0

Broadcast Number : 190 .15 .255 .255

- **Compute Broadcast Number**: this can be done via the **ORING** between the **IP Address** and the **Subnet mask number.**

Example#2: if the subnet mask number is 30.140.250.140, find the Network Number?

Solution: we must find the class i.e. this number from **class A**? How?

Network ID : 30 .0 .0 .0

Broadcast Number: 30 .255 .255 .255

Chapter (8): Transmission impairments and Problems

Transmission lines suffer from three major problems:

1. **Attenuation**.
2. **Delay distortion.**
3. **Noise.**

Attenuation:

Loss of energy as signal propagates outward, (measured in DB / km). It also depends on frequency, resulting in different frequency spectrum. Amplifier, are used to reduce the effect of losses.

Delay distortion:

Delay distortion is caused by the different speed for different frequencies.

This is clearer in digital data, as fast component of one bit may catch-up and may overtake slow component from the bit ahead, resulting into mixing and incorrect reception.

Noise:

There are many causes for noise, of which is the following:

- thermal noise caused by random motion of electrons in wires is not avoidable.
- Cross talk caused by inductive coupling between wires dose to each other.
- Spike nose (or impulse noise) from power lines.

Modems

DC signaling (baseband) is not suitable for data communication (only for slow speed for short distances), due to strong attenuation and delay distortion. So, AC signaling is used. This is achieved by many methods of which:

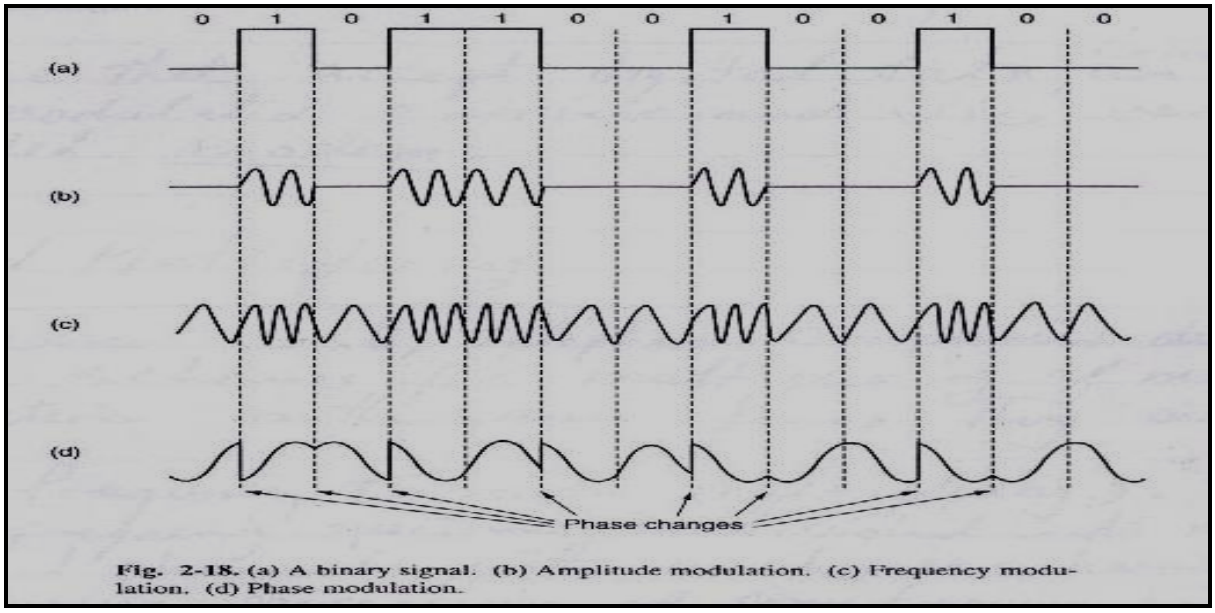


Fig. 2-18. (a) A binary signal. (b) Amplitude modulation. (c) Frequency modulation. (d) Phase modulation.

AM: Amplitude Modulation, carrier signal is modulated by 0 & 1 respectively.

FM: Frequency Modulation (or frequency shift keying, FSK), as two (or more) different tones as used.

PSM: Phase Shift Modulation: as the carrier frequency is systematically shifted 45, 135, 225 or 315 degrees at uniformly spaced intervals, each transmits 2 bits of information.

The device that accepts digital data converts it to modulated carrier and vice versa is called modem.