Table of Contents

# CHAPTER ONE

# INTRODUCTION TO DATA COMMUNICATION

## DATA COMMUNICATION

### DEFINITION OF TERMS

**Computer network**

"A group of computers linked together using a transmission media so that they can communicate with each other, share resources (such as hard disk and printer) and access remote hosts or other network.

**Communication**

This is the transmission and reception of information across a media with a feedback loop between them

**Data communication**

Is the electronic transmission of data from one place to another?

**Communication channel/ media**

This is the path / rout connecting a sending and a receiving end to allow information flow through

**Workstation**

A workstation is a client. More specifically, it is a standalone computer equipped with its own processor and system and application software. It can perform its functions independent of the network. To expand its resources and knowledge, it may get connected to a network

**Server**

A server is a computer that shares its resources across the network, and a client are one that accesses shared resources. Depending on the size and requirements of the network, servers can be classified as below:

- ✓ File Server
- ✓ Database Server
- ✓ Print Server
- ✓ Disk Server

### FORMS OF DATA TRANSMISSION

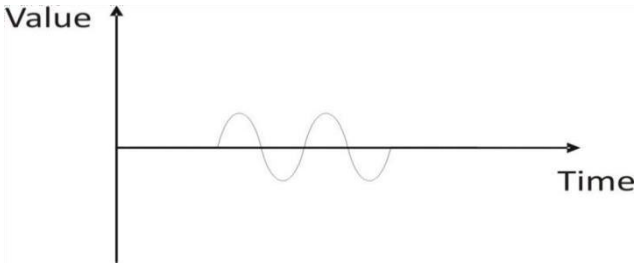
Data can be transmitted across a network in the following two basic terms.

a. Analogue data transmission

b. Digital data transmission

#### Analogue data transmission

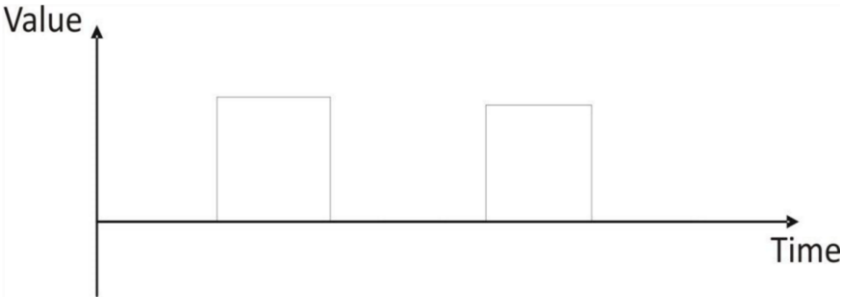
Here data is transmitted as continuous wave form from one terminal to the other. E.g. telephone systems use analogue data transmission where the signals are transmitted in a continuous wave form.




### Digital data transmission

This method of data transmission uses distinct "ON" or "OFF" electricity states. The data is represented as "presence" i.e. "ON" and "absence" i.e. "OFF" of electric pulses.

These are represented using 1 and 0 respectively. Digital transmission is faster when compared to analogue. As most of the communications lines i.e. telephone line work on analog data transmission, we use modem an instrument which converts analog data into digital form.




## DATA COMMUNICATION CRITERIA

The effectiveness of data communications system depends on four fundamental characteristics:

1. Delivery. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. Accuracy. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. Timeliness. The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission and this occurs in a real-time system.
4. Jitter. Jitter refers to the variation in the packet arrival time. It is the uneven delay of delivery of audio or video packets. For example, let us assume that video packets are sent every 20ms. If some of the packets arrive with 20ms delay and others with 30ms delay, an uneven quality in the video is the result.

### Data Communication And Terminal Equipment

Communication facilities have an ancient history, but we tend to think of the advent of the telegraph and later the telephone as the beginning of modern communications. Extensive telegraph and telephone networks were established all over the world, decades before the emergence of computers. Data communication equipment (DCE) is the hardware devices that can be used to establish, maintain and terminate communication between a data source and its destination. Data communications equipment is most used to perform signal exchange, coding and line clocking tasks as part of intermediate equipment or DTE. A typical example of data communication equipment is the modem.

Data terminal equipment (DTE) refers to the interface equipment which is source or destination in communication. The terminal equipment is capable of converting information to signals and

also reconverting received signals. Data terminal equipment does communicate directly with each other. Communication between them is done by data communication equipment. Popular examples of data terminal equipment are computers, printers, routers, servers etc.

Data communication equipment and data terminal equipment are often confused with each other. In fact the confusion is more pronounce when data communication equipment are embedded in some data terminal equipment. The truth is that when the two are separated they are interlinked. Also, data terminal equipment and data communication connectors are wired differently if a single straight cable is employed. Data communication equipment generates internal clock signals, while data terminal equipment works with externally provided signals. Figure 4 shows a typical arrangement of data communication and terminal equipment.

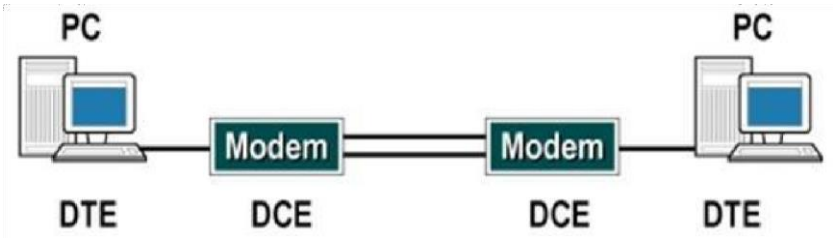



Figure 4: Data communication and terminal equipment

### Data Representation

Data representation is defined as the methods used to represent information in computers. Different types of data can be stored in the computer system. This includes numeric data, text, executable files, images, audio, video, etc. all these will look different to us as human. However, all types of information or data stored in the computer are represented as a sequence of 0s and 1s.

### Decimal Numbers

As human we are used to writing numbers using digits 0 to 9. This is called base 10. This number system has been widely adopted, in large part because we have 10 fingers. However, other number systems still persist in modern society.

### Binary Numbers

Any positive integer (whole number) can be represented by a sequence of 0s and 1s. Numbers in this form are said to be in base two, and are called binary numbers. Computers are based on the binary (base 2) number system because electrical wire can only be of two states (on or off).

### Hexadecimal Numbers

Writing numbers in binary is tedious since this representation uses between 3 to 4 times as many digits as the decimal representation. The hexadecimal (base 16) number system is often used as shorthand for binary. Base 16 is useful because 16 is a power of 2, and numbers have roughly as many digits as in the corresponding decimal representation. Another name for hexadecimal numbers is alphadecimal because the numbers are written from 0 to 9 and A to F. where A is 10, B is 11 up to F that is 15.

### Text

American Standard Code for Information Interchange (ASCII code) defines 128 different symbols. The symbols are all the characters found on a standard keyboard, plus a few extra. Unique numeric code (0 to

127) is assigned to each character. In ASCII, “A” is 65, “B” is 66, “a” is 97, “b” is 98, and so forth. When a file is save as “plain text”, it is stored using ASCII. ASCII format uses 1 byte per character 1 byte gives only 256 (128 standard and 128 non-standard) possible characters. The code value for any character can be converter to base 2, so any written message made up of ASCII characters can be converted to a string of 0s and 1s.

### Graphics

Graphics on computer screen are consists of pixels. The pixels are tiny dots of color that collectively paint a graphic image on a computer screen. It is physical point in a raster image, or the smallest addressable element in an all points addressable display device. Hence it is the smallest controllable element of a picture represented on the screen. The address of a pixel corresponds to its physical coordinates. LCD pixels are manufactured in two-dimensional grid, and are often represented using dots or squares, but CRT pixels correspond to their timing mechanism and sweep rates. The pixels are organized into many rows and columns on the screen.

### Review Questions

1. Define data and Data Communication.
2. Compare analog and digital data
3. Why data communication
4. List and explain components of data communication system.
5. Highlights any 5 examples of resources that can be share on data communication and networks
6. Define and gives example of basic components of data communication network.
7. What are the major criteria that data communication network must meet.
8. Highlights the factors that affect response time as related to performance of data communication network.
9. List various ways of data representation in computer system.
10. Define Data communication equipment and data terminal equipment. Give at least two examples in each case.

## DATA TRANSMISSION TECHNIQUES

### Digital-To-Analog Conversion

Digital-to-analog conversion is the process of changing one of the characteristics of an analog signal based on the information in digital data. Figure 55 shows the relationship between the digital information, the digital-to-analog modulating process, and the resultant analog signal.

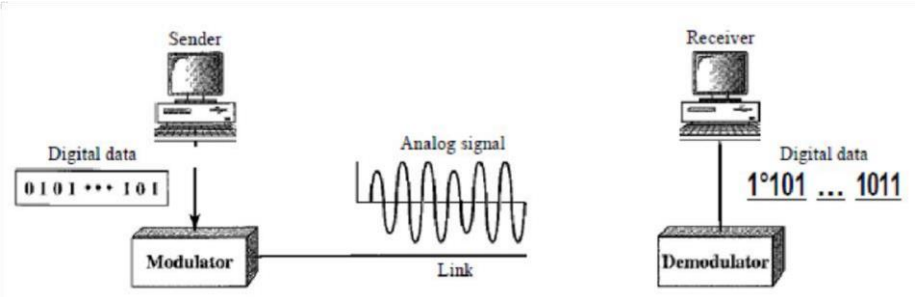



Figure 55: Digital-to-analog conversion

## MODULATION

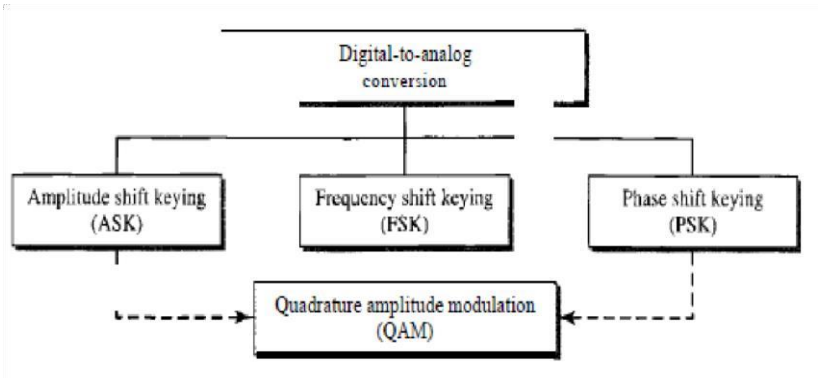
**What is Modulation Techniques?**

Sine wave is defined by three characteristics: amplitude, frequency, and phase. When we vary anyone of these characteristics, we create a different version of that wave. So, by changing one characteristic of a simple electric signal, we can use it to represent digital data. The techniques of varying the characteristics are known as modulation techniques.

Modulation Techniques are methods used to encode digital information in an analog world. Additionally, digital signals usually require an intermediate modulation step for transport across wideband, analogoriented networks. Modulation is the process where a Radio Frequency or Light Wave's amplitude, frequency, or phase is changed in order to transmit intelligence. Digital information changes the carrier signal by modifying one or more of its characteristics (amplitude, frequency, or phase). This kind of modification is called modulation (shift keying).

## Types of Modulation

Any of the three characteristics can be altered in this way, giving us at least three types for modulating digital data into an analog signal: amplitude shift keying (ASK), frequency shift keying (FSK), and phase shift keying (PSK). In addition, there is a fourth (and better) mechanism that combines changing both the amplitude and phase, called quadrature amplitude modulation (QAM). QAM is the most efficient of these options and is the mechanism commonly used today




Types of digital-to-analog conversion

## Amplitude Shift Keying

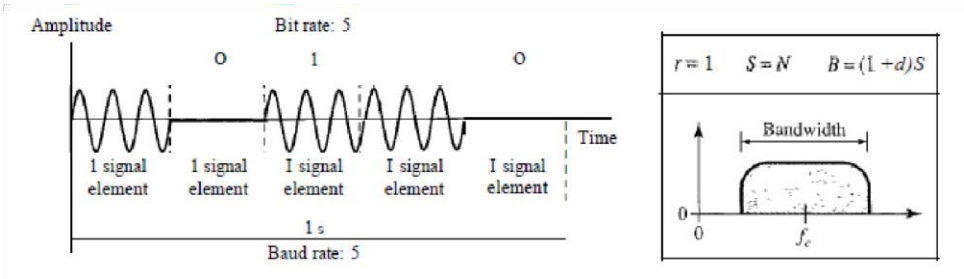
In amplitude shift keying, the amplitude of the carrier signal is varied to create signal elements. Both frequency and phase remain constant while the amplitude changes. Binary ASK (BASK) although we can have several levels (kinds) of signal elements, each with a different amplitude, ASK is normally implemented using only two levels. This is referred to as binary amplitude shift keying or on-off keying (OOK). The peak amplitude of one signal level is 0; the other is the same as the amplitude of the carrier frequency. Figure 57 gives conceptual views of binary ASK.

Bandwidth for ASK Figure 57 also shows the bandwidth for ASK. Although the carrier signal is only one simple sine wave, the process of modulation produces a nonperiodic composite signal. This signal, as was discussed earlier, has a continuous set of frequencies. As we expect, the bandwidth is proportional to the signal rate (baud rate). However, there is normally another factor involved, called d, which depends on the modulation and filtering process. The value of d is between 0 and 1. This means that the bandwidth can be expressed as shown, where 5 is the signal rate and the B is the bandwidth.

$$B = (1 + d) \times S$$

The formula shows that the required bandwidth has a minimum value of 5 and a maximum value of 25. The most important point here is the location of the bandwidth.

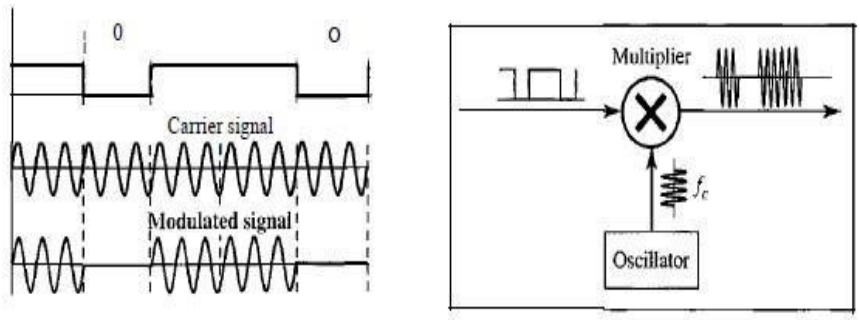
The middle of the bandwidth is where Ie the carrier frequency, is located. This means if we have a bandpass channel available, we can choose our Ie so that the modulated signal occupies that bandwidth. This is in fact the most important advantage of digital-to- analog conversion. We can shift the resulting bandwidth to match what is available.




Binary amplitude shift keying

**Implementation of ASK**

The complete discussion of ASK implementation is beyond the scope of this book. However, the simple ideas behind the implementation may help us to better understand the concept itself. Figure 58 illustrate how we can simply implement binary ASK. If digital data are presented as a unipolar NRZ, digital signal with a high voltage of IV and a low voltage of 0 V, the implementation can achieved by multiplying the NRZ digital signal by the carrier signal coming from an oscillator. When the amplitude of the NRZ signal is 1, the amplitude of the carrier frequency is held; when the amplitude of the NRZ signal is 0, the amplitude of the carrier frequency is zero.




Implementation of binary ASK  Multilevel ASK

The above discussion uses only two amplitude levels. We can have multilevel ASK in which there are more than two levels. We can use 4,8, 16, or more different amplitudes for the signal and modulate the data using 2, 3, 4, or more bits at a time. In these cases, r = 2, r = 3, r =4, and so on. Although this is not implemented with pure ASK, it is implemented with QAM.

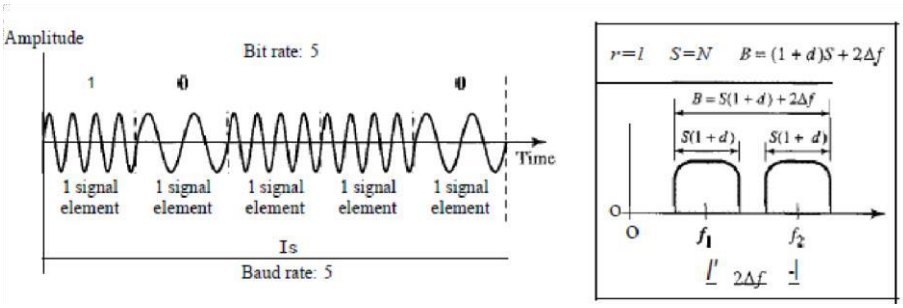
## Frequency Shift Keying

In frequency shift keying, the frequency of the carrier signal is varied to represent data. The frequency of the modulated signal is constant for the duration of one signal element, but changes for the next signal element if the data element changes. Both peak amplitude and phase remain constant for all signal elements.

**Binary FSK (BFSK)**

One way to think about binary FSK (or BFSK) is to consider two carrier frequencies. In Figure 59, we have selected two carrier frequencies, $f_1$ and$f_2$. We use the first carrier if the data element is 0; we use the second if the data element is 1. However, note that this is an unrealistic

example used only for demonstration purposes. Normally the carrier frequencies are very high, and the difference between them is very small.




Binary frequency shift keying

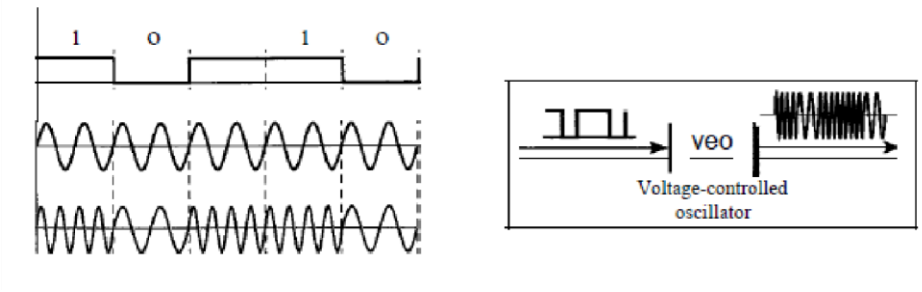
As Figure 59 shows, the middle of one bandwidth is f1 and the middle of the other is f2. Both f1 and f2 are Δf apart from the midpoint between the two bands. The difference between the two frequencies is 2Δf  Bandwidth for BFSK Figure 59 also shows the bandwidth of FSK. Again the carrier signals are only simple sine waves, but the modulation creates a nonperiodic composite signal with continuous frequencies. We can think of FSK as two ASK signals, each with its own carrier frequency. If the difference between the two frequencies is 211j, then the required bandwidth is

$$B=(l+d)xS+2\Delta f$$

What should be the minimum value of 2Δf In Figure 59, we have chosen a value greater than (l + d)S. It can be shown that the minimum value should be at least S for the proper operation of modulation and demodulation.

**Implementation**

There are two implementations of BFSK: noncoherent and coherent. In noncoherent BFSK, there may be discontinuity in the phase when one signal element ends and the next begins. In coherent BFSK, the phase continues through the boundary of two signal elements. Noncoherent BFSK can be implemented by treating BFSK as two ASK modulations and using two carrier frequencies. Coherent BFSK can be implemented by using one voltage-controlled oscillator (VeO) that changes its frequency according to the input voltage. Figure 60 shows the simplified idea behind the second implementation. The input to the oscillator is the unipolar NRZ signal. When the amplitude of NRZ is zero, the oscillator keeps its regular frequency; when the amplitude is positive, the frequency is increased.




Implementation ofBFSK

Multilevel FSK

Multilevel modulation (MFSK) is not uncommon with the FSK method. We can use more than two frequencies. For example, we can use four different frequenciesf1, f2, f3, and f4 to send 2

bits at a time. To send 3 bits at a time, we can use eight frequencies. And so on. However, we need to remember that the frequencies need to be 2Δf apart. For the proper operation of the modulator and demodulator, it can be shown that the minimum value of 2Δf to be S. We can show that the bandwidth with d =0 is

$$B=(l+d) \times S + (L - 1)\, 2\Delta f$$

$$B = L \times S$$

## Phase Shift Keying

In phase shift keying, the phase of the carrier is varied to represent two or more different signal elements. Both peak amplitude and frequency remain constant as the phase changes. Today, PSK is more common than ASK or FSK. However, we will see that QAM, which combines

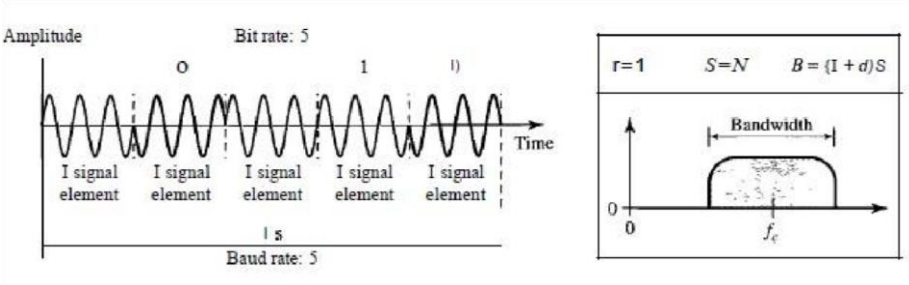
ASK and PSK, is the dominant method of digital-to- analog modulation.

### Binary PSK (BPSK)

The simplest PSK is binary PSK, in which we have only two signal elements, one with a phase of 0°, and the other with a phase of 180°. Figure 5.9 gives a conceptual view of PSK. Binary PSK is as simple as binary ASK with one big advantage-it is less susceptible to noise. In ASK, the criterion for bit detection is the amplitude of the signal; in PSK, it is the phase. Noise can change the amplitude easier than it can change the phase. In other words, PSK is less susceptible to noise than ASK. PSK is superior to FSK because we do not need two carrier signals.

Bandwidth Figure 60 also shows the bandwidth for BPSK. The bandwidth is the same as that for binary ASK, but less than that for BFSK. No bandwidth is wasted for separating two carrier signals.

Implementation The implementation of BPSK is as simple as that for ASK. The reason is that the signal element with phase 180° can be seen as the complement of the signal element with phase 0°. This gives us a clue on how to implement BPSK. We use the same idea we used for ASK but with a polar NRZ signal instead of a unipolar NRZ signal.



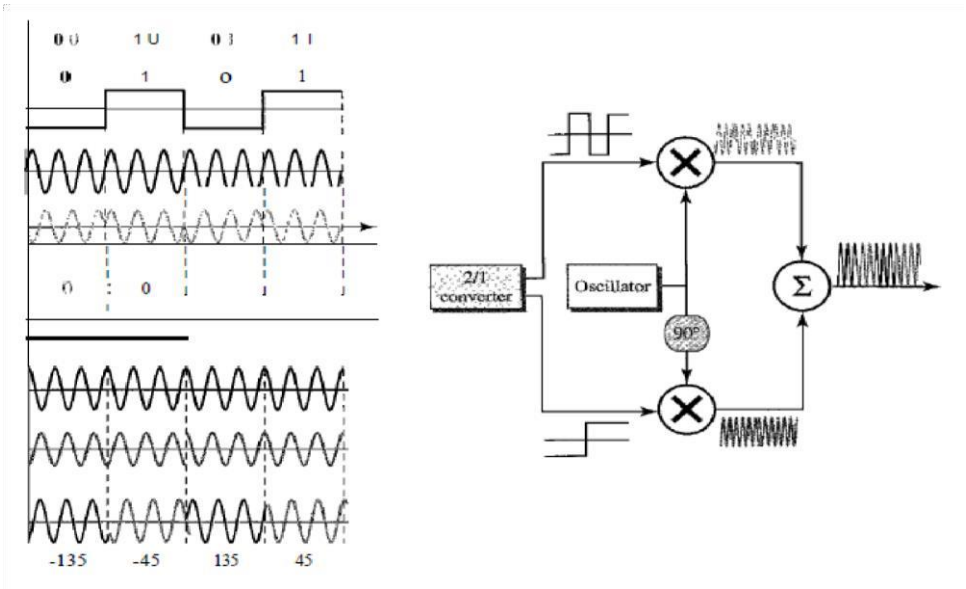

Binary phase shift keying

### Quadrature PSK (QPSK)

The simplicity of BPSK enticed designers to use 2 bits at a time in each signal element, thereby decreasing the baud rate and eventually the required bandwidth. The scheme is called quadrature PSK or QPSK because it uses two separate BPSK modulations; one is in-phase, the other quadrature (out-ofphase). The incoming bits are first passed through a serial-toparallel conversion that sends one bit to one modulator and the next bit to the other modulator. If the duration of each bit in the incoming signal is T, the duration of each bit sent to the

corresponding BPSK signal is 2T. This means that the bit to each BPSK signal has one-half the frequency of the original signal. Figure 62 shows the idea.

The two composite signals created by each multiplier are sine waves with the same frequency, but different phases. When they are added, the result is another sine wave, with one of four possible phases: 45°, 45°, 135°, and -135°. There are four kinds of signal elements in the output signal (L = 4), so we can send 2 bits per signal element (r =2).

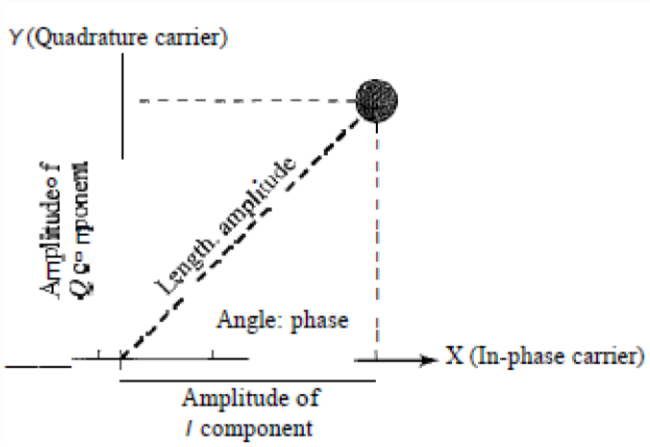



QPSK and its implementation:

**Constellation Diagram**

A constellation diagram can help us define the amplitude and phase of a signal element, particularly when we are using two carriers (one inphase and one quadrature), the diagram is useful when we are dealing with multilevel ASK, PSK, or QAM. In a constellation diagram, a signal element type is represented as a dot. The bit or combination of bits it can carry is often written next to it.

The diagram has two axes. The horizontal X axis is related to the inphase carrier; the vertical Y axis is related to the quadrature carrier. For each point on the diagram, four pieces of information can be deduced. The projection of the point on the X axis defines the peak amplitude of the in-phase component; the projection of the point on the Y axis defines the peak amplitude of the quadrature component. The length of the line (vector) that connects the point to the origin is the peak amplitude of the signal element (combination of the X and Y components); the angle the line makes with the X axis is the phase of the signal element. All the information we need, can easily be found on a constellation diagram. Figure 63 shows a constellation diagram.




Concept of a constellation diagram

## Review Questions

1. Define analog transmission.
2. Define carrier signal and its role in analog transmission.
3. Describe digital-to-analog conversion.
4. Which characteristics of an analog signal are changed to represent the digital signal in each of the following digital-toanalog conversion? a. ASK b. FSK
   **c.** PSK
   **d.** QAM
5. Which of the four digital-to-analog conversion techniques (ASK, FSK, PSK or QAM) is the most susceptible to noise? Juxtapose your answer.
6. Define constellation diagram and its role in analog transmission.
7. What are the two components of a signal when the signal is represented on a constellation diagram? Which component is shown on the horizontal axis?
8. Which is shown on the vertical axis?

## METHODS OF DIGITAL DATA TRANSMISSION

we see that for communication to occur there will be a channel of communication through which the devices are interconnected. In digital data transmission where we have more than one bits to send from sender to receiver. Our primary when we are considering the wiring is the data stream. Do we send 1 bit at a time; or do we group bits into larger groups and, if so, how? The transmission of binary data across a link can be accomplished in either parallel or serial mode. In parallel mode, multiple bits are sent with each clock tick. In serial mode, 1 bit is sent with each clock tick. While there is only one way to send parallel data, there are three subclasses of serial transmission: asynchronous, synchronous, and isochronous. See

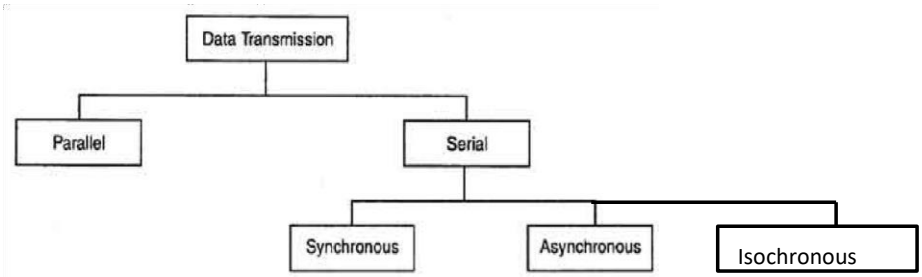
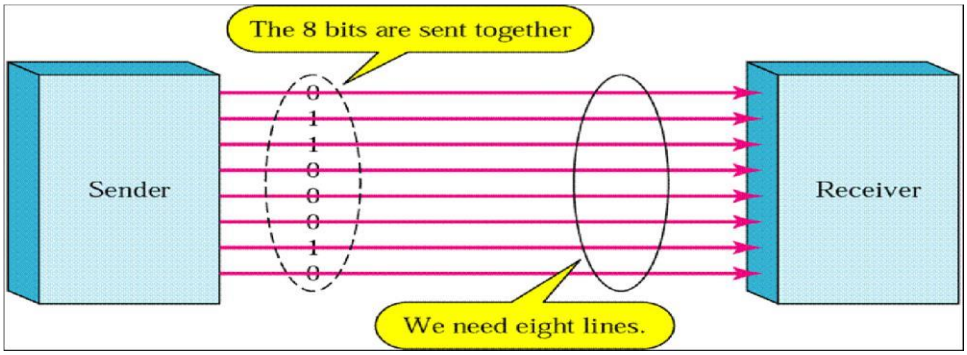



Figure 17 : Data Transmission

## Parallel Transmission

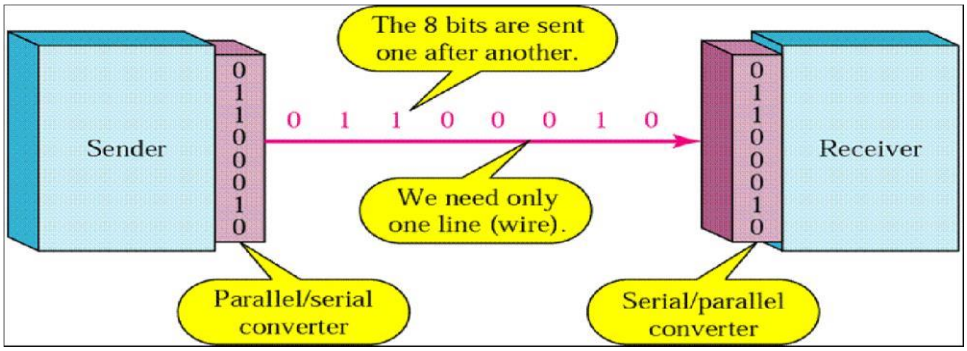
Binary data, consisting of 1s and 0s, will be organized into groups of n bits each. Computers produce and consume data in groups of bits. By grouping, we can send data n bits at a time instead of 1. This is called parallel transmission. The advantage of parallel transmission is speed. All else being equal, parallel transmission can increase the transfer speed by a factor of n over serial transmission. Shortcoming of parallel transmission it requires n communication lines just to transmit the data stream. Hence it is expensive, parallel transmission is usually limited to short distances. See figure 18.




Parallel transmission

## Serial Transmission

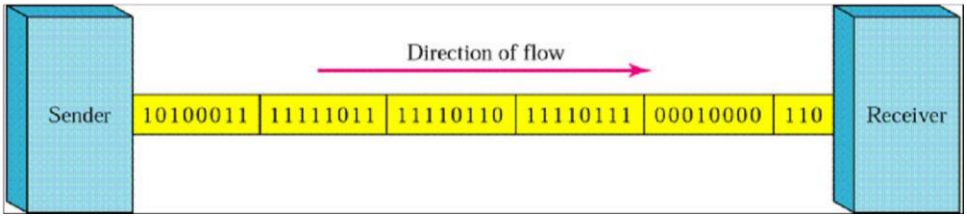
In serial transmission one bit follows another, so we need only one communication channel rather than n to transmit data between two communicating devices. The advantage of serial over parallel transmission is that with only one communication channel, serial transmission reduces the cost of transmission over parallel by roughly a factor of n. Since communication within devices is parallel, conversion devices are required at the interface between the sender and the line (parallel-to-serial) and between the line and the receiver (serial-toparallel). Serial transmission occurs in one of three ways: asynchronous, synchronous, and isochronous.




Serial Transmission

### *Synchronous Transmission*

In synchronous transmission, we send bits one after another without start or stop bits or gaps. It is the responsibility of the receiver to group the bits.




Synchronous Transmission

A sequence of events is isochronous if the events occur regularly, or at equal time intervals. The isochronous transmission guarantees that the data arrive at a fixed rate. In real-time audio and video, in which uneven delays between frames are not acceptable, synchronous transmission fails. For example, TV images are broadcast at the rate of 30 images per second; they must be viewed at the same rate. If each image is sent by using one or more frames, there should be no delays between frames.

### *Asynchronous Transmission*

In asynchronous transmission, we send 1 start bit (0) at the beginning and 1 or more stop bits (1) at the end of each byte. There may be a gap between each byte.

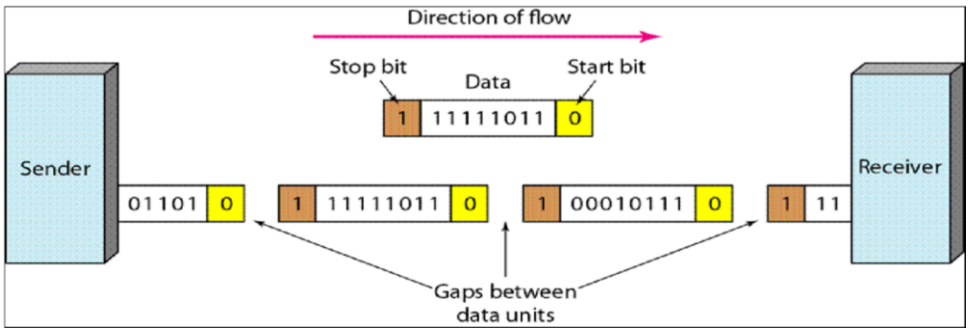


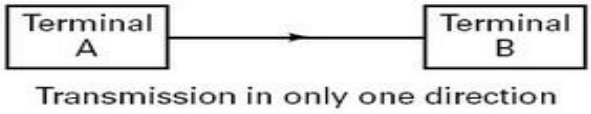

Figure 21: Asynchronous Transmission

## Review Questions

1. Describe with diagram the data transmission type.
2. Compare a 10K Byte data transmission using Asynchronous transmission & Synchronous Transmission. Determine the efficiency (10 Kbytes = 80 kbits)
3. Compare synchronous and asynchronous transmission
4. What is data flow? Hence describe three major types of data flow in data communication network.
5. Describe briefly with diagram and relevant example, three major data flow approaches.
6. If an Ethernet frame has overhead of 64bytes including start and stop frames, and the data size is 2500 bytes. Determine the Ethernet frame efficiency.

# MODES OF DATA TRANSMISSION

## Simplex Connection



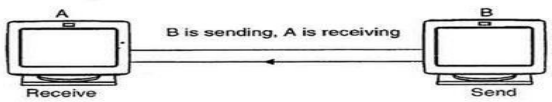

This is a method of transmission whereby data only flows in one direction.

Examples of Simplex mode:

- ✓ Communication between a computer and a keyboard
- ✓ Transmission is loudspeaker system. An announcer speaks into a microphone and his/her voice is sent through an amplifier and then to all the speakers.
- ✓ Many fire alarms work the same way.

## Half duplex

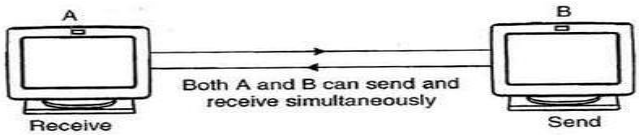
This is an operation model whereby data only flows in the direction at a time at the end of which data can flow in the opposite direction. E.g. walkie-talkie




-

## Full duplex

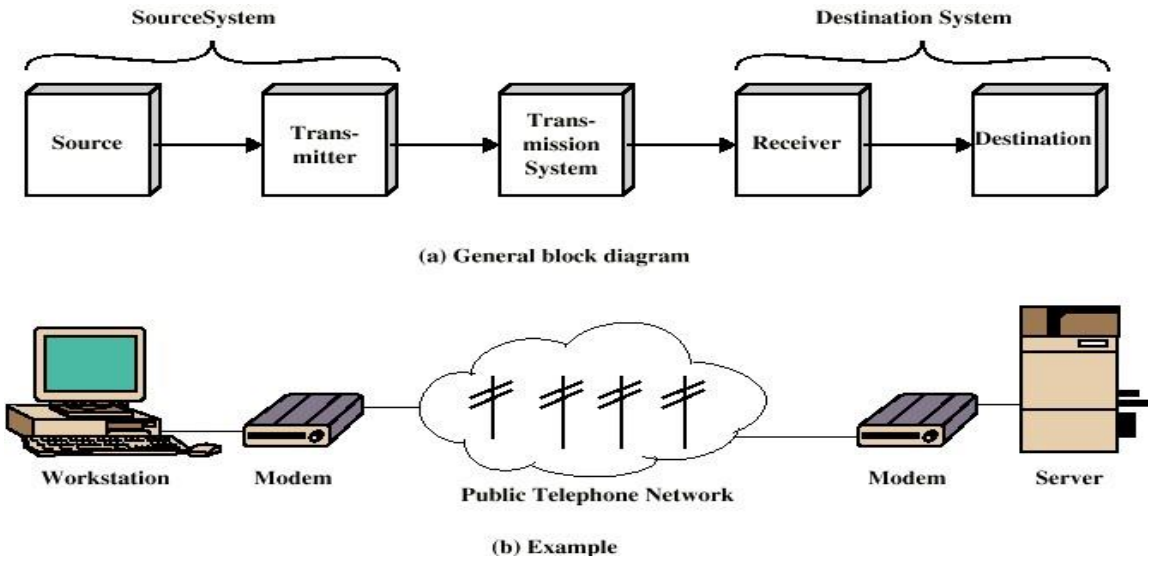
This is a link in which data transmission between the two communicating devices can occur simultaneously. Internet and telephone connections are full-duplex connections




Full duplex mode

## DATA TRANSMISSION

Simplified Communications Model



**Source:** This device generates the data to be transmitted; examples are telephones and personal computers.

**Transmitter:** This is the source of information. It is an electronic device that radiates signals towards a receiving device.

Usually, the data generated by a source system are not transmitted directly in the form in which they were generated. Rather, a transmitter transforms and encodes the information in such a way as to produce electro- magnetic signals that can be transmitted across some sort of transmission system. For example, a modem takes a digital bit stream from an attached device such as a personal computer and transforms that bit stream into an analog signal that can be handled by the telephone network.

**Transmission system:** This can be a single transmission line or a complex net-work connecting source and destination.

**Receiver:** The receiver accepts the signal from the transmission system and converts it into a form that can be handled by the destination device. For example, a modem will accept an analog signal coming from a network or transmission line and convert it into a digital bit stream.

**Destination:** Takes the incoming data from the receiver.

## COMMUNICATION CHANNEL CONFIGURATION

A communication network is basically described as a collection of communicating devices, switches or links which are interconnected and `*autonomous*. Communicating device is any system that transmits or receives data. Interconnections of devices can either be physical e.g. via cables or through the air e.g. satellites and lasers.

An *autonomous* device is a crash-independent device i.e. its failure does not cause the network to fair.

The three main goals of a communication network are:

i. Resource sharing
ii. Improve reliability
iii. Cost saving
iv. Enhance security and data backup

There are two main types of network systems, these are

i. Point –to-point communication system
ii. Multipoint (drop) communication system

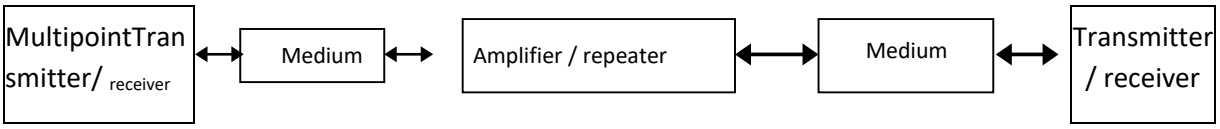
### Point –to-point

When two communication devices are directly linked by a physical media, it forms a pointto-point mode. The main advantages are.

a) Transmissions are direct with minimal delay

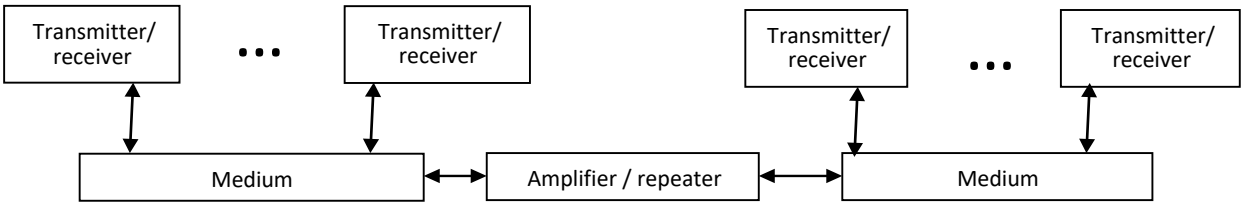
b) Signals do not suffer from corruptions from other transmission

c) Communication is private




## Multipoint

When several devices are directly connected to one or more devices, it constitutes a multipoint communication system .although several devices are interconnected, communication occurs between two devices at a time.




Forms of information:

i. Text - alphabetic characters.
ii. Numeric data - information in form of numbers.
iii. Graphical data - in the form of pictures or diagrams.
iv. Sound - audio/voice data
v. Video - pictures accompanied by sound
vi. Multimedia a mixture of different forms of information.

## MULTIPLEXING

**Definition of Multiplexing**

Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared. Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link. As data and telecommunications use increases, so does traffic. We can accommodate this increase by continuing to add individual links each time a new channel is needed; or we can install higher-bandwidth links and use each to carry multiple signals. In a multiplexed system, n lines share the bandwidth of one link. Figure 6.1 shows the basic format of a multiplexed system. The lines on the left direct their transmission streams to a multiplexer (MUX), which combines them into a single stream (many-toone). At the receiving end, that stream is fed into a demultiplexer (DEMUX), which separates the stream back into its component transmissions (one-to-many) and directs them to their corresponding lines. In the figure, the word link refers to the physical path. The word channel refers to the portion of a link that carries a transmission between a given pair of lines. One link can have many (n) channels. Multiplexing is the transmission of multiple data communication sessions over a common wire or medium. Multiplexing reduces the number of wires or cable required to connect multiple sessions. A session is considered to be data communication between two devices: computer to computer, terminal to computer, etc. There are three basic multiplexing techniques: frequencydivision multiplexing, wavelength-

division multiplexing, and time-division multiplexing. The first two are techniques designed for analog signals, the third, for digital signals (see Figure 6.2).

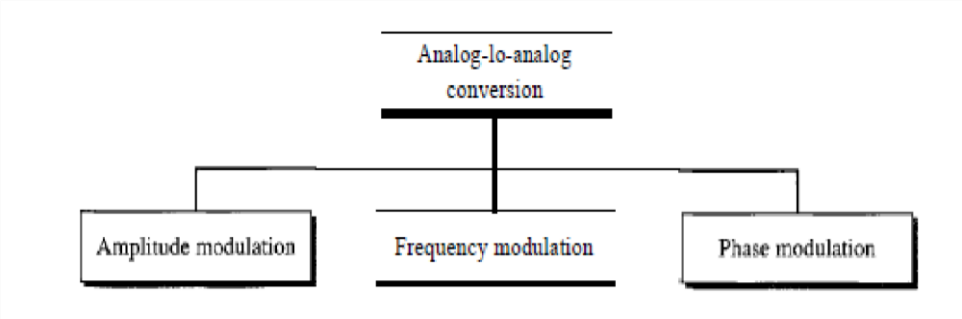



Figure 64: Categories of multiplexing

## Types of Multiplexing Techniques

### Frequency Division Multiplexing

Frequency Division Multiplexing (FDM) is an analog technique where each communications channel is assigned a carrier frequency. To separate the channels, a guard-band would be used. This is to ensure that the channels do not interfere with each other. For example, if we had our 3 terminals each requiring a bandwidth of 3 kHz and a 300 Hz guard-band, Terminal 1 would be assigned the lowest frequency channel 0-3 kHz, Terminal 2 would be assigned the next frequency channel 3.3kHz-6.3kHz and Terminal 3 would be assigned the final frequency channel 6.6kHz-9.6 kHz.

The frequencies are stacked on top of each other and many frequencies can be sent at once. The downside is that the overall line bandwidth increases. Individual terminal requirement were 3 kHz bandwidth each, in the above example: the bandwidth to transmit all 3 terminals is now 9.6 kHz.

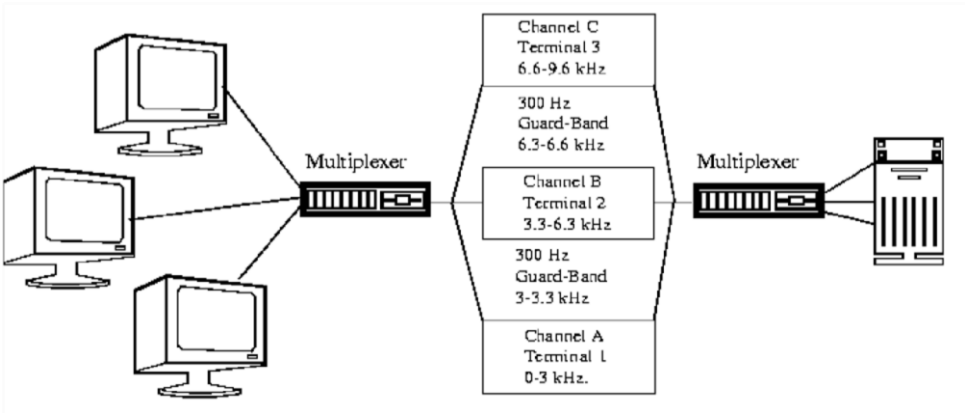



Figure 65: Frequency Division Multiplexing

FDM does not require all channels to terminate at a single location. Channels can be extracted using a multi-drop technique; terminals can be stationed at different locations within a building or a city. FDM is an analog and slightly historical multiplexing technique. It is prone to noise problems and has been overtaken by Time Division Multiplexing which is better suited for digital data.

### Time Division Multiplexing

Time Division Multiplexing is a technique where a short time sample of each channel is inserted into the multiplexed data stream. Each channel is sampled in turn and then the

sequence is repeated. The sample period has to be fast enough to sample each channel according to the Nyquist Theory (2x highest frequency) and to be able to sample all the other channels within that same time period. It can be thought of as a very fast mechanical switch, selecting each channel for a very short time then going on to the next channel. Each channel has a time slice assigned to it whether the terminal is being used or not. Again, to the send and receiving stations, it appears as if there is a single line connecting them. All lines originate in one location and end in one location. TDM is more efficient, easier to operate, less complex and less expensive than FDM.

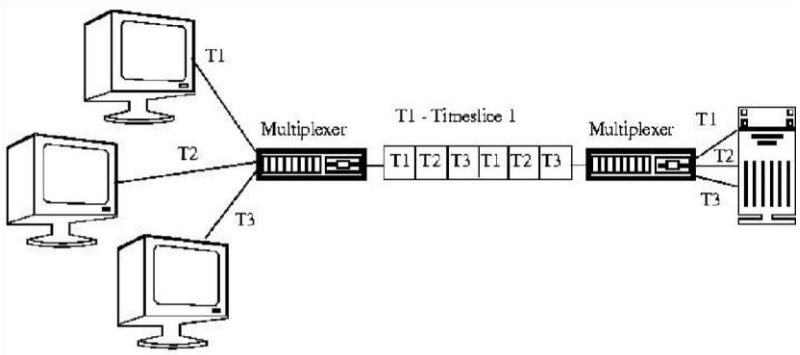



Figure 66: Time Division Multiplexing

## Wavelength Division Multiplexing

This technique is used in optical fiber. It is useful to increase the information carried by single optical fiber WDM can be view as an optical domain version of FDM in which multiple information signal modulate optical signals at different optical wavelength (colors). The resulting signals are combine and transmitted simultaneously over the same optical fiber as in the diagram below.

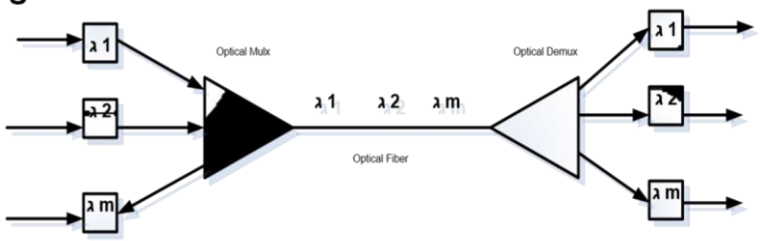



**Figure 67: Wavelength Division Multiplexing**

Various optical devices such as prisms and diffraction grating can be used to combine and split color signal. For instance early WDM systems combine 16 wavelengths at 2.5Gbps to provide an aggregate signal of 16 x 2.5Gbps. WDM systems with 32 wavelengths at 10gbps have a total bit rate of 320Gbps and are widely deployed. Systems that carry 160 wavelengths at 10Gbps are also available and achieved at amazing bit rate of 1.6 terabit/second. The attraction of WDM is that a huge increase in available bandwidth is obtained with less investment associated with deploying additional optical fiber. The additional bandwidth can be used to carry more traffic and can also provide the additional protection bandwidth refined by self-healing network topologies.

## Review Question

1. Explain briefly the term multiplexing
2. With the aid of diagram describe briefly;

i. Wavelength Division multiplexing (WDM) ii. Time Division Multiplexing (TDM) iii. Frequency Division Multiplexing (FDM)

**3.** Suppose that a frequency band W Hz wide into M channels of equal bandwidth.

**a)** What bit rate is achievable in each channel? Assume all channels have the same SNR.

**b)** What bit rate is available to each M user if the entire frequency band is used as a single channel and TDM is applied?

**c)** How does the comparison of (a) and (b) change if we suppose that FDM require a guard band between adjacent channels? Assume the guard band is 10%of channel bandwidth

**4.** Suppose Ray Power FM 100.5, has a large band of available bandwidth, say 1GHz, which is to be used by central office to transmit and receive from large number of users. Describe how the following approach can be use to organizing the system:

**a)** A single TDM

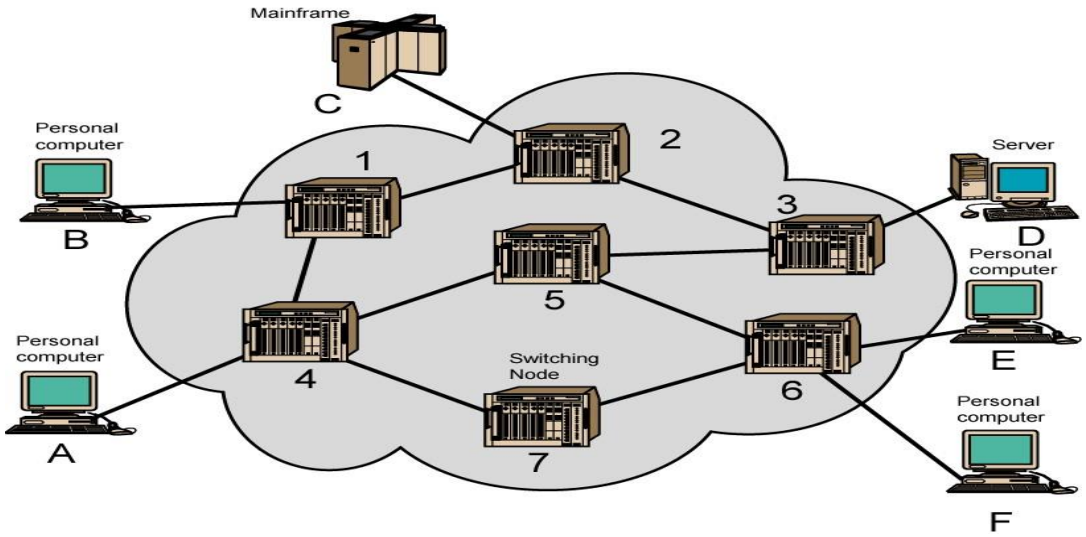
**b)** A hybrid TDM/FDM system in which the frequency band is divided into multiple channel and time division multiplexing is used within each channel

**5.** Compare the operation of multiplexer, an add-drop multiplexer, a switch, and a digital cross-connect.

## SWITCHING COMMUNICATION NETWORKS

Long distance transmission is typically done over a network of switched nodes. The switched nodes are not concerned with content of data rather their purpose is to provide a switching facility that will move data from node to node until they reach the destination.

End devices are stations which may be: Computer, terminal, phone, etc. A collection of nodes and connections is referred to as a ***communications network***. Data is routed by being switched from node to node




**Simple Switching Network**

Data from station A intended for station F are sent to nodes 4. They may then be routed via node 5 and 6 or node 7 and 6 to the destination. Several observations are in order:

i. Some nodes connect only to other nodes

ii. Nods stations links are generally dedicated point to point links. Nodes to nodes are usually multiplex using either frequency division multiplexing (FDM) or time division multiplexing (TDM)

iii. The network is not fully connected i.e. there is no direct link between every possible pair of nodes.

The main objective of networking is to share resources and information efficiently. Whenever we have multiple devices, we have problem of connect them to make one-to-one connection possible. One solution is to install a point to point link between each pair of devices such as in mesh topology or between a central device and every other device as in star topology.

These methods, however, are impractical and wasteful when applied to very large network. The number and length of the links require too many infrastructures to be cost efficient; and majority of those links would be idle most of the time.

A better solution is to uses switching. A switch network consists of a series of inter-linked nodes, called switches. Switches are hardware and/or software capable of creating temporary connection between two or more devices linked to switch but not to each other.

Traditionally, three methods of switching have been important:

- Circuit switching
- Packet switching and
- Message switching

## Circuit Switching

### Explanation of Circuit switching operation

Communication via circuit switching implies that there is a dedicated communication path between two stations. The path is a connected sequence of links between network nodes. On each physical link, a channel is dedicated to the connection. A common example of circuit switching is the telephone network..

Communication via circuit switching involves three phases:

**i. Circuit Establishment**

Before any signals can be transmitted, an end-to-end (station to station) circuit must be established. For example, station A wants to communicate with station E. station A sends a request to node 4 requesting a connection to station E. typically, the link from A to 4 is a dedicated line, so that part of connection already exists. On the basis of routing information and measures availability and perhaps cost, let's assume that node 4,5, and 6 are used to complete the connection. In completing the connection, a test is made to determine if station E is busy or is prepared to accept the connection.

**ii. Information Transfer**

Information now can transmit from A through the network to E the transmission may be analogue voice, or binary data. Generally the connection is ***full duplex***, and signals may be transmitted in both direction simultaneously.

**iii. Circuit Disconnection**

Once the transmission is completed, the connection is terminated, usually by the action of one of the two stations. Signals must be propagated to the nodes 4,5, and 6 to reallocate the dedicated resources.

Circuit switching can be rather inefficient. Channel capacity is dedicated for the duration of a connection, even if no data are being transferred. The connection provides for transmission at a constant data rate. Thus, each of the devices that are connected must transmit and receive at the same data rate as the other.

Circuit switching was designed to handle voice traffic (in analog) but is now used for data traffic (in digital form).

**Examples of circuit switched network**

i. Public telephone network
ii. Private branch exchange (PBX) used to connect telephone within a building or an office.
iii. A data switch similar to PBX but its designed to interconnect digital data processing devices such as terminals and computers.

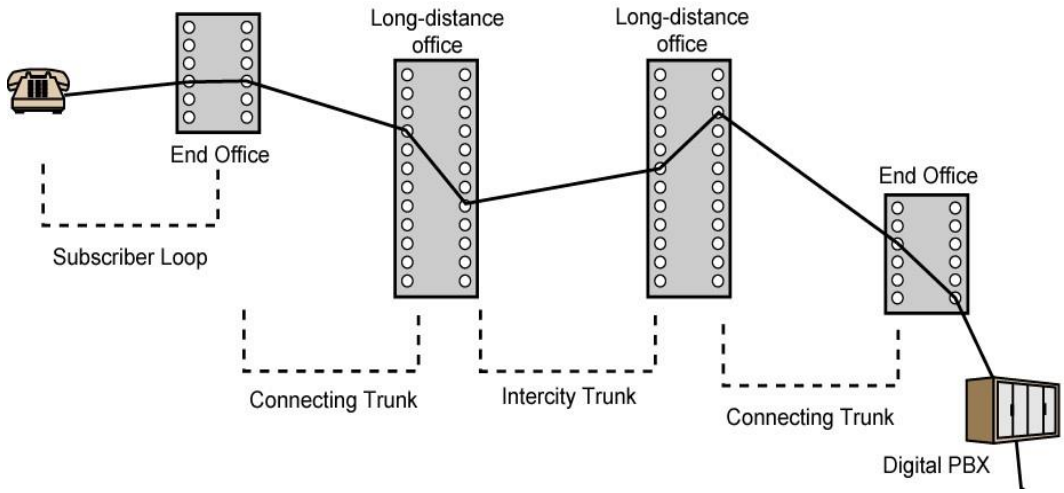
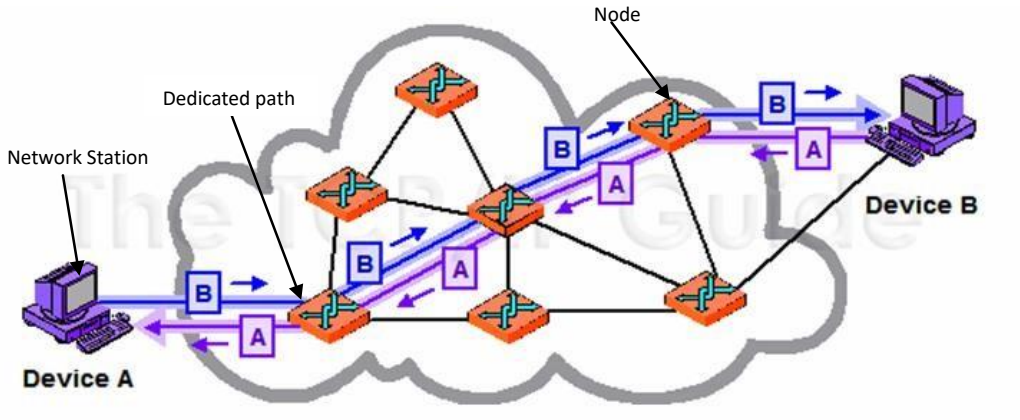



**Figure 1 Public Circuit Switched Network**

**Telecoms Components**

i. Subscriber
Devices attached to network e.g.
telephones ii. Subscriber line.
This is the link between the subscriber and the network usually called ***Local Loop or Subscriber loop*** and can be few km up to few tens of km
iii. Exchange
These are switching centres that supports subscribers also known as
***End office*** iv. Trunks
This are branches between exchanges and are usually multiplexed

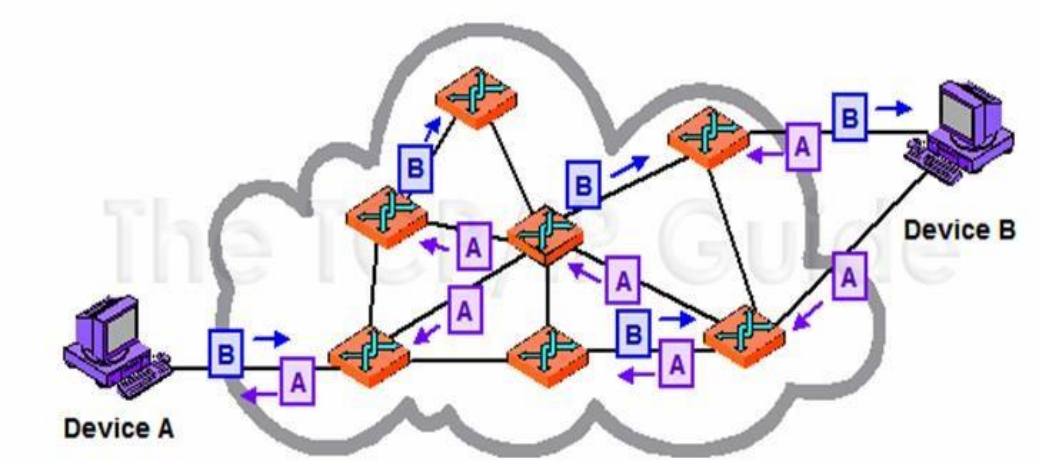
**Sample diagrams of circuit switching**




**Circuit Switching Network**

## Packet Switching

In a packet switching data are transmitted in short packets. A typical packet length is 1000 byte. If a source has longer message to send, the message is broken up into a series of packets. Each packet contains a portion (or the entire short message) of the user's data plus some control information. These packets are routed to the destination via different available nodes.




**Packet Switching Networks**

### Basic operation of Packet Switching

A transmitting computer or other device sends a message as a sequence of packets. Each packet includes control information including the destination station. The packets are initially sent to the node to which the sending station attaches. As each packet arrives at these nodes, the node stores the packet briefly, and determines the next available link. When the link is available, the packet is transmitted to the next node. The entire packet eventually delivered to the intended node.

### Approaches to packet switching

#### a) Datagram Approach

In the datagram approach to packet switching, each packet is treated independently from all others and each packet can be sent via any available path, with no

reference to packet that have gone before. In the datagram approach packets, with the same destination address, do not all follow the same route, and they may arrive out of sequence at the exit point.

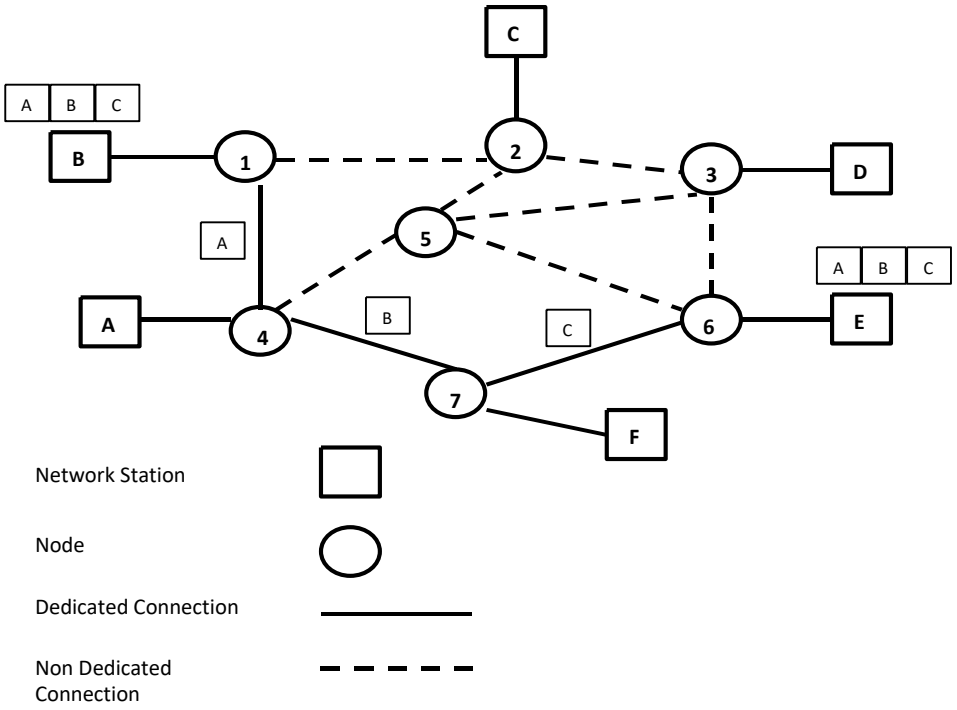
**Advantages of datagram approach**

i. Call setup phase is avoided thus if a station wishes to send only one or a few packets, datagram delivery will be quicker

ii. Its flexible in that in case of congestion packets can be routed away from the congestion

iii. It more reliable since if a node fail the packets can be relayed through alternative routes

**Figure 6 Virtual switching network**




## Virtual Circuit

In this approach, a pre-planned route is established before any packets are sent. Once the route is established, all the packets between a pair of communicating parties follow this same route through the network. Each packet now contains a virtual circuit identifier as well as the data. Each node on the pre-established route knows where to direct such packet. No routing decisions are required. At any time, each station can have more than one virtual circuit to any other station and can have virtual circuits to more than one station.

**Network Communication and Data Packets**

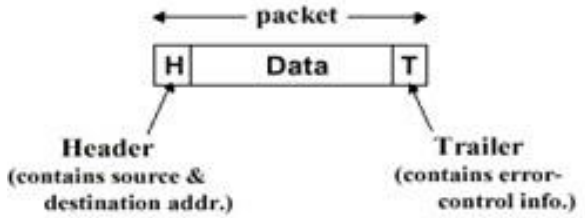
Network communication usually involves long messages. However, networks do not handle large chunks of data well, so they reformat the data into smaller, more manageable pieces, called packets or frames.
Networks split data into small pieces for two reasons:

1. Large units of data sent across a network hamper effective communications by ***saturating the network***. If a sender and receiver are using all possible bandwidth, other computer can not communicate.

2. Network can be unreliable. ***If errors*** occur during transmission of a packet, ***the entire packet must be re-sent***. If data is into many smaller packets, only the packet in which the error occurred must be re-sent. This is more efficient and makes it easier to recover from errors. With data split into packets, individual communications are faster and more efficient, which allows more computers to use network. When the packets reach their destination, the computer collects and reassembles them in their proper order to re-create the original data.

**Packet Structure**

All the packets have three basic parts:

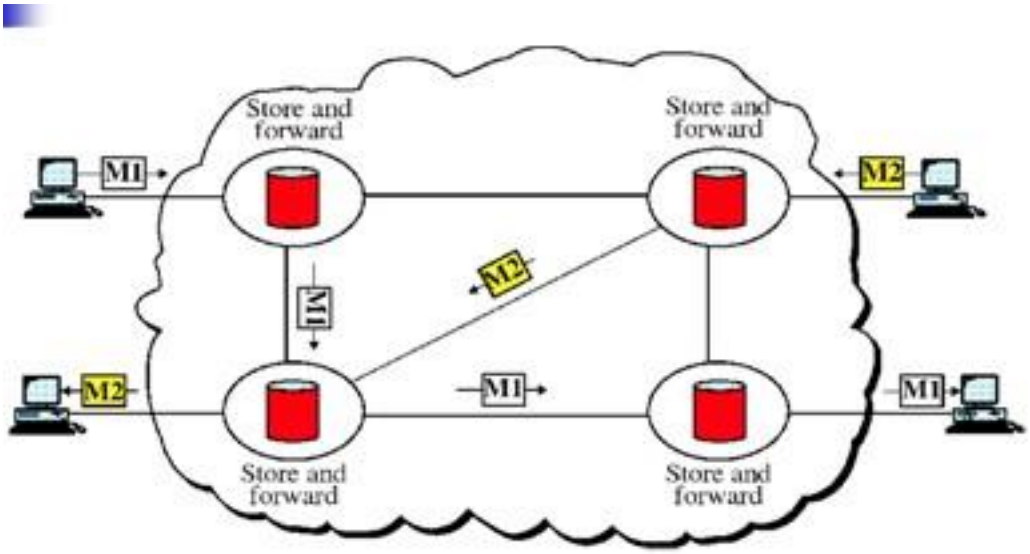



1. ***Packet header:*** The packet header usually contains the source address and destination address of the packet.
2. ***Data section:*** The data section consists of the actual data being sent. The sizes of this section can very depending on the network type, 512 bytes to 4K.
3. ***Packet trailer:*** The packet trailer contains information to verify the validity of the packet. Using a cyclic redundancy check (CRC) usually does this. The CRC is a number on the packet calculated by the sending computer and added to the trailer. When the receiving computer gets the packet, it recalculates the CRC and compares it to the one in the trailer. If the CRCs match, it accepts the packet as undamaged. If CRCs don't match, the receiving computer requests that the packet be re-sent.

## Message Switching

The descriptive term store and forward best know message switching. In this mechanism, a anode (usually a special computer with number of disks) receives a message, stores it until the appropriate route is free, then send it along. Note that in message switching the messages are stored and relayed from the ***secondary storage (disk)***, while in packet switching the packets are stored and forward from primary storage (RAM).

The primary uses of message switching have been to provide high-level network service (e.g. delayed delivery, broadcast) for unintelligent devices. Since such devices have been replaced, message switching has virtually disappeared. Also delays inherent in the process, as well as the requirement for large capacity storage media at each node, make it unpopular for direct communication.




# CHAPTER TWO

# COMMUNICATION AND TRANSMISSION MEDIA

The most common components of a network are:

i. Data communication media
ii. Communication devices
iii. Network software

## Data communication media

A data communication media is a channel through which data is transmitted between computers and other devices.

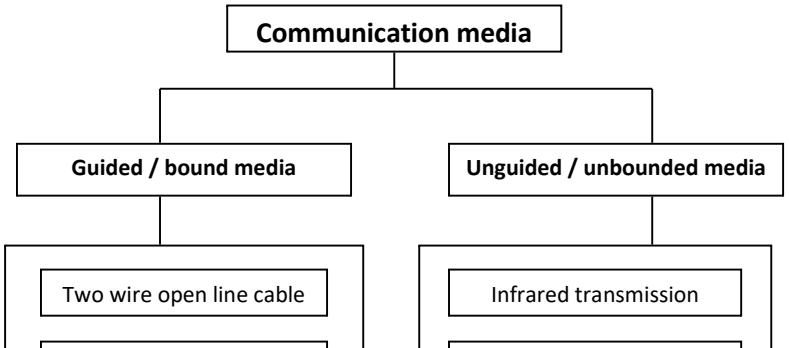
## Transmission Media

The data to be transmitted between two locations is normal in an electrical signal form. The data can either be flowing current or radiated electromagnetic waves. In either case, they need a physical path through` which they can flow. This is called the transmission medium.

Transmission media can be broadly categorized into two types:

i. Terrestrial (land lines) / Guided / Bound
ii. Air media (radio waves) / Unguided

Data communication media can be classified as follows



## Communication using bound / guided media

Guided /physical / non-wireless / bounded media have a physical link between sender and receiver. Mainly there are three categories of guided media: twisted-Pair, coaxial, and fiber-optic.

### *Guided media*

Guided /physical / non-wireless / bounded media have a physical link between sender and receiver. Mainly there are three categories of guided media: twisted-Pair, coaxial, and fiber-optic.

**1. Two-wire cable**

They consist of pairs of bare copper wire conductors that are tired to insulators attached to cross-arms in telephone poles. They are currently being faced out due to limitation of the numbers of pairs that can be carried in a single pole line, they are prone to damage, vandalism and are affected by bad weather. Although this cable was popular in the seventies, it is almost obsolete due to its many limitations, which included: Interferences of the signal resulting from the inductive and capacitive coupling effects of the two parallel wires

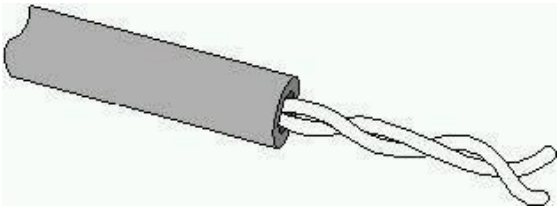
**2. Twisted-Pair Cable**

Consist of two insulated copper wires twisted in a spiral pattern to minimize electromagnetic interference (EMI). It's the cheapest media used for both the analogue and digital signals. They are mainly used in telephone systems They are of two types

*Unshielded Twisted (UTP) cable*

UTP, using the 10BaseT specification, is the most popular type of twisted-pair cable and is fast becoming the most popular LAN cabling. The maximum cable length segment is 100 meters, about 328 feet.

UTP do not have a shield that prevent electromagnetic interference hence they are susceptible to noise and external interference.



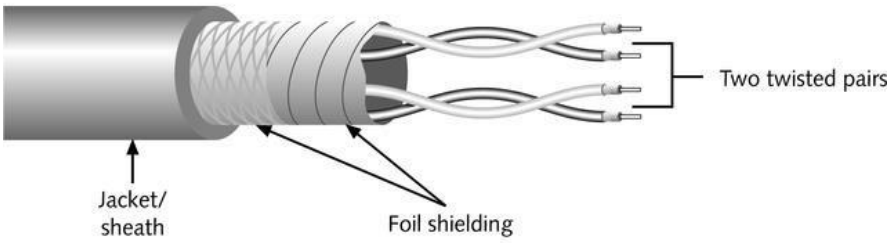
Electronic Industries Association and the Telecommunications Industries Association

(EIA/TIA) specifies the type of UTP cable these include

- **Category 1** This refers to traditional UTP telephone cable that can carry voice but not data transmissions. Most telephone cable prior to 1983 was Category 1 cable.
- **Category 2** This category certifies UTP cable for data transmissions up to 4 megabits per second (Mbps). It consists of four twisted pairs of copper wire.
- **Category 3** This category certifies UTP cable for data transmissions up to 16 Mbps. It consists of four twisted pairs of copper wire with three twists per foot.
- **Category 4** This category certifies UTP cable for data transmissions up to 20 Mbps. It consists of four twisted pairs of copper wire.
- **Category 5** This category certifies UTP cable for data transmissions up to 100 Mbps. It consists of four twisted pairs of copper wire.

*Shielded Twisted (STP)*

STP includes shielding to reduce cross talk as well as to limit the effects of external interference. For most STP cables, this means that the wiring includes a wire braid inside the cladding or sheath material as well as a foil wrap around each individual wire. This shield improves the cable's transmission and interference characteristics, which, in tern, support higher bandwidth over longer distance than UTP.




Advantages of twisted pair cable

i. They are easy to install

ii. They are cheap since they are readily available for telephone use

Disadvantages of twisted pair cable

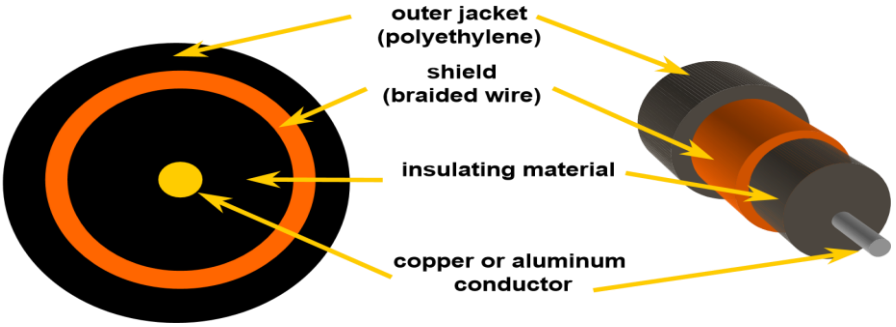
i. Have low data transmission rate

ii. They have high electromagnetic interference

iii. Suffer high attenuation

**3. Coaxial Cable**

Coaxial cable has two conductors that share the same axis. A solid copper wire runs down the center of the cable, and this wire is surrounded by plastic foam dielectric material / insulation. The foam is surrounded by a second conductor, wire mesh tube, metallic foil, or both. The wire mesh protects the wire from EMI. It is often called the shield. A tough plastic jacket forms the cover of the cable, providing protection and insulation.




Where Ethernet is concerned, there are two types of coaxial cable

i. **Thinnet Cable** / Thin Ethernet or thinwire

*Thinnet* cable is a flexible coaxial cable about 0.64 centimeters (0.25 inches) thick. Because this type of coaxial cable is flexible and easy to work with, it can be used in almost any type of network installation. Thinnet cable can be connected directly to a computer's network interface card (NIC).

It can carry a signal for a distance of up to approximately 185 meters (about 607 feet) before the signal starts to suffer from attenuation.

ii. **Thicknet Cable**

*It* is a relatively rigid coaxial cable about 1.27 centimeters (0.5 inches) in diameter.

Thicknet cable can carry a signal for 500 meters (about 1640 feet). Therefore, because of thicknet's ability to support data transfer over longer distances, it is sometimes used as a backbone to connect several smaller thinnet-based networks.

**Coaxial-Cable Grades and Fire Codes**

The type of cable grade that you should use depends on where the cables will be laid in your office. Coaxial cables come in two grades:

i. *Polyvinyl chloride (PVC)* is a type of plastic used to construct the insulation and cable jacket for most types of coaxial cable. PVC coaxial cable is flexible and can be easily routed through the exposed areas of an office. However, when it burns, it gives off poisonous gases.
ii. A *plenum* is the shallow space in many buildings between the false ceiling and the floor above; it is used to circulate warm and cold air through the building.

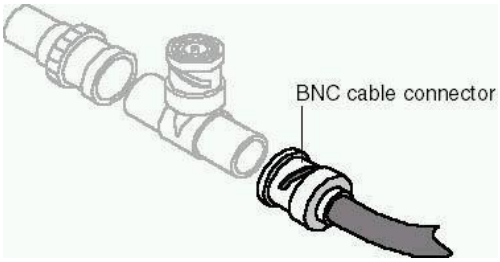
Plenum-grade cabling contains special materials in its insulation and cable jacket. These materials are certified to be fire resistant and produce a minimum amount of smoke; this reduces poisonous chemical fumes. Plenum cable can be used in the plenum area and in vertical runs (for example, in a wall) without conduit. However, plenum cabling is more expensive and less flexible than PVC cable

**Coaxial-Cable Connection Hardware**

i. **The BNC cable connector**

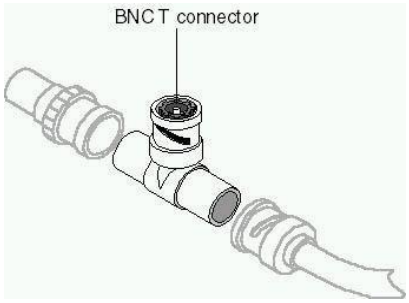
The BNC cable connector is either soldered or crimped to the end of a cable. The basic BNC connector is a male type mounted at each end of a cable. This

connector has a center pin connected to the center cable conductor and a metal tube connected to the outer cable shield. A rotating ring outside the tube locks the cable to any female connector.




ii. **The BNC T connector**

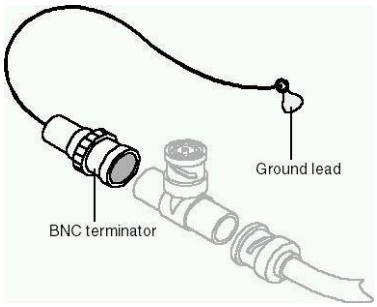
This connector joins the network interface card (NIC) in the computer to the network cable.




iii. **The BNC barrel connector** Figure 2.9 shows a BNC barrel connector. This connector is used to join two lengths of thinnet cable to make one longer length.

iv. **The BNC terminator**

A BNC terminator closes each end of the bus cable to absorb stray signals. Otherwise the signal will bounce and all network activity will stop.




The coaxial cable transmission media is used in two transmission methods

**Baseband**

i. This has the following characteristics
ii. It transmits unmodulated digital signals
iii. Each cable carries a single channel
iv. The propagation of signals is bi-directional
v. Stations are connected via T-connectors.
vi. There is no need for modems.

**Broadband**

i. It has the following characteristics
ii. Digital signal modulated onto Radio Frequency (RF) carrier (analog)
iii. Channel allocation based on Frequency Division Multiplexing (FDM).
iv. Supports bi-directional transmission
v. Stations are connected via RF modems.

**Advantages of coaxial cable**

i. High data transmission rate
ii. They are stable even under high data load
iii. Has capability of carrying more signal
iv. Much less susceptible to interference than twisted pair

**Disadvantages of coaxial cable**

i. They are expensive to buy
ii. They are bulky thus difficult to work with Coaxial-Cabling Considerations

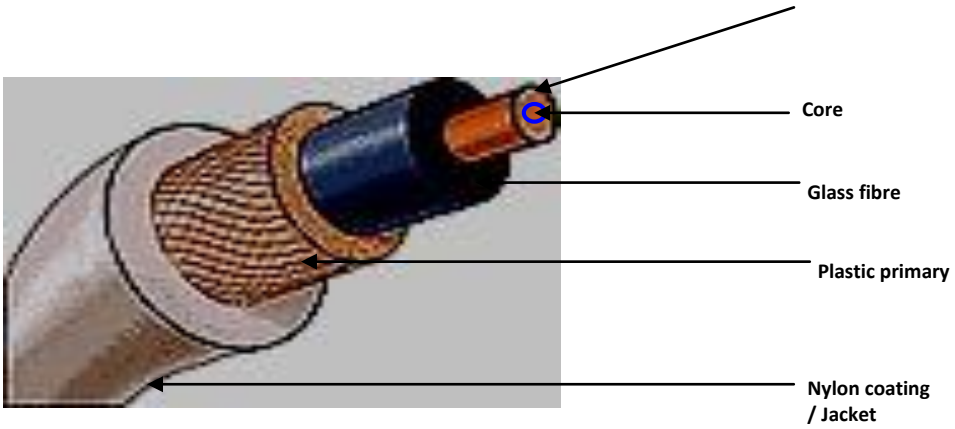
Use coaxial cable if you need a medium that can:

i. Transmit voice, video, and data.
ii. Transmit data for greater distances than is possible with less expensive cabling.
iii. Offer a familiar technology with reasonable data security.

**4. Fiber Optic Cable**

Fiber optic cable transmits light signals rather than electrical signals. In a fibre optic cable light only moves in one direction. For a two way communication to take place, a second connection must be made between the two devices. This is the reason for the cable to contain two strands i.e. the core and the glass fibre

The electric signal from the source are converted to light signal, then propagated along the fibre optic cable. To convert an electric signal to light, you need a light emitting diode (LED) at the transmitter. At the receiving end, a *photosensitive* device can be used to convert the light signal back to electric signal that can be processed by the computer




Cladding

Parts of the fibre optic cable

i. *The Core*

It is a glass strand: a strand is responsible for one direction communication. The core is used to send data in one direction. While the *glass fibre* sends data in the opposite direction. Light from the laser travels through this glass to the other device on the receiving end

ii. *Cladding*

It is a highly reflective material that redirects light back to the core. It has some light bending characteristic that is why even if the cable is bent into coils and a light signal is inserted at one end it will still be seen coming out from the other end.

iii. *Plastic primary*

It's used for insulating between the glass fibre and the nylon; It protects the inner components from the outer components

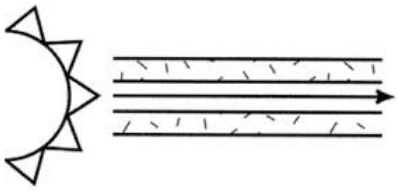
iv. *Nylon coating / jacket*

Protect the cable from the actual physical damage

Fibre optic cables are of two types

i. *Single mode*

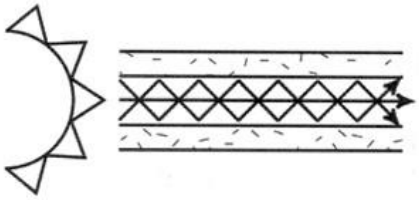
It has a very narrow core. The light in the cable therefore take only one path through it making it to have a low attenuation rate. It allows for faster transmission time and longer distances but costs more



ii. *Multimode*

It has a thicker core and allows several light rays to be fed in the cable. It has a high attenuation rate and it is used for nearby connection especially within a building as it is relatively cheaper.

Multimode fiber gives you high bandwidth at high speeds (10 to 100MBS - Gigabit to 275m to 2km) over medium distances.



Advantages of Fiber Optic

i. Noise resistance: it is immune to EMI
ii. Suffer lower attenuation: signal can run for miles without requiring regeneration
iii. Highest bandwidth: fibre optic cable can support dramatically higher bandwidths (and hence data rate) than all other cables.
iv. Smaller and lighter than copper cable hence space limited situations
v. Can be used in hazardous (highly flammable) places because they do not generate electrical signals
vi. Has greater repeater spacing
vii. Suffers negligible cross-talk
viii. Has high noise immunity

Disadvantages of Fiber Optic

i. Cost : most expensive among all the cables
ii. Installation / maintenance: is high
iii. Fragility : glass fibre is more easily broken than wire
iv. They are complex to configure

**Optical Transmission Modes**

There are 3 primary types of transmission modes using optical fiber.

**i.** Step Index Mode: Step Index has a large core the light rays tend to bounce around, reflecting off the cladding, inside the core. This causes some rays to take a longer or shorted path through the core. Some take the direct path with hardly any reflections while others bounce back and forth taking a longer path. The result is that the light rays arrive at the receiver at different times. The signal becomes longer than the original signal. LED light sources are used. Typical Core: 62.5 microns.

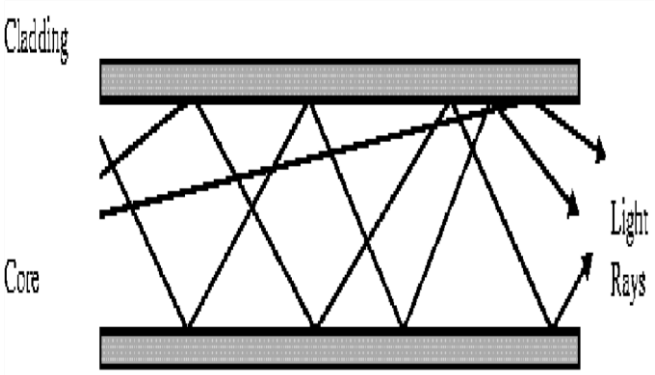



Figure 25: Step Index Mode

**ii.** Grade Index Mode: Grade Index has a gradual change in the Core's Refractive Index. This causes the light rays to be gradually bent back into the core path. This is represented by a curved reflective path in the attached drawing. The result is a better receive signal than Step Index. LED light sources are used. Typical Core: 62.5 microns.

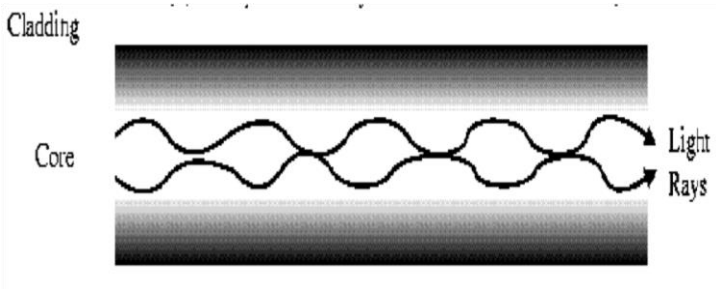



Figure 26: Grade Index Mode

Note: Both Step Index and Graded Index allow more than one light source to be used (different colours simultaneously). Multiple channels of data can be run simultaneously.

**iii.** Single Mode: Single Mode has separate distinct Refractive Indexes for the cladding and core. The light ray passes through the core with relatively few reflections off the cladding. Single Mode is used for a single source of light (one colour) operation. It requires a laser and the core is very small: 9 microns.

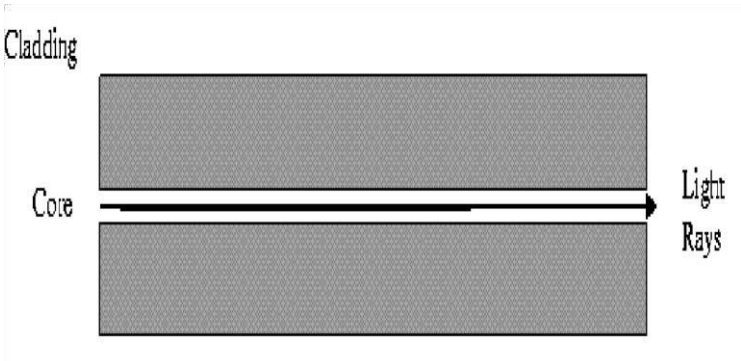



Figure 27: Single Mode

Table 1: Summary Table of the Characteristic of All Cable Type

| Factor | UTP | STP | Coaxial | Fiber Optic |
|---|---|---|---|---|
| Cost | Lowest | Moderate | Moderate | Highest |
| Installation | Easy | Fairly easy | Fairly easy | Difficult |
| Bandwidth Capacity | 10 Mbps | 16 Mbps | 10 Mbps | 100 Mbps – 1 Gbps |
| Node Capacity Per Segment | 2 | 2 | 30 (10Base2) 100 (10Base5) | 2 |
| Attenuation | High | High | Lower | Lowest |
| EMI | Most vulnerable to EMI | Less vulnerable than UTP | Less vulnerable than UTP | No effect by EMI |

Point to point transmission characteristic of guided media

| Transmission media | Total data rate | Bandwidth | Repeater spacing |
|---|---|---|---|
| Twisted pair | 4 Mbps | 3 MHz | 2 to 10 km |
| Coaxial cable | 500 Mbps | 350 MHz | 1 to 10 km |
| Optical fiber | 2 Gps | 2 GHz | 10 to 100 km |

## Unguided Transmission Media

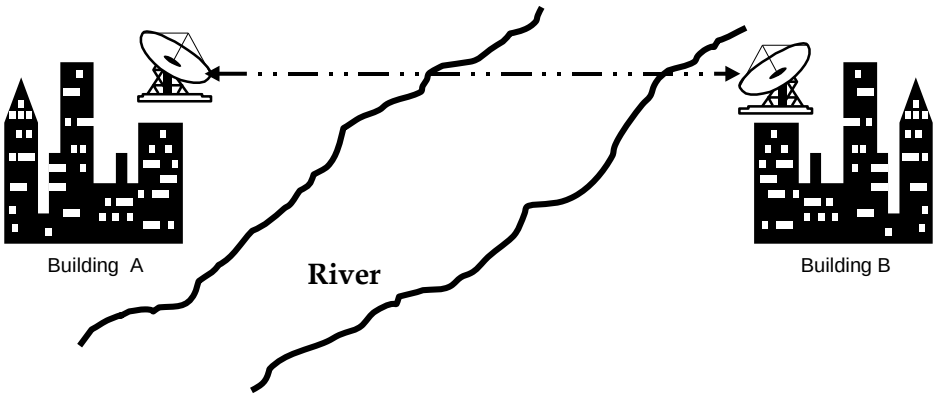
Unguided/non-physical/wireless/unbounded media have no physical link between sender and receiver.

1. **Microwave transmission**

   Microwave transmission is line of sight transmission. The transmit station must be in visible contact with the receive station. This sets a limit on the distance between stations depending on the local geography. Typically the line of sight due to the Earth's curvature is only 50 km to the horizon! Repeater stations must be placed so the data signal can hop, skip and jump across the country.

   Microwaves operate at high operating frequencies of 3 to 10 GHz. This allows them to carry large quantities of data due to their large bandwidth.

   .




Microwave Transmission

Terrestrial microwave systems are typically used when using cabling is very costly and difficult to set.

Advantages of microwave transmission

i. They operate at a high speed

ii. It is less prone to transmission errors unlike twisted pair cable

iii. Are capable of operating in digital or analog data

Disadvantages of microwave transmission

i. Its signals are affected by atmospheric conductors like lightning

ii. Require additional number of repeaters after every few kilometers

iii. If any object come in between the transmission line of sight it affect signal transmission

## 2. Satellite Communication

Satellites are transponders (units that receive on one frequency and retransmit on another) that are set in geostationary orbits directly over the equator. These geostationary orbits are 36,000 km from the Earth's surface. At this point, the gravitational pull of the Earth and the centrifugal force of Earth's rotation are balanced and cancel each other out. Centrifugal force is the rotational force placed on the satellite that wants to fling it out into space.

Satellite stay in a stationary orbit above the earth; Signals are beamed up to the satellite from a station on the ground. This is called *up link*. These signals are relayed down to the earth station. This down transmission is called *down link.*

A satellite transmission system has three main components

i. Transmitter earth station – set up the uplink
ii. A satellite –
iii. Receiving earth station – one receiving the sent signal on the other end

The geographical area where satellite signals can be located or accesses clearly is called a satellite *footprint*. The satellite transmits the signal to many recipients' earth stations to form a *point to multipoint* transmission.

The new trend in microwave transmission have seen the use of very small aperture terminals (VSAT) technology. This VSAT refers to a very small satellite dish used both in data, radio and TV communication. Many business are adopting this new technology because it enable direct access to satellite communication instead of having to go through state owned or licensed satellite gateways

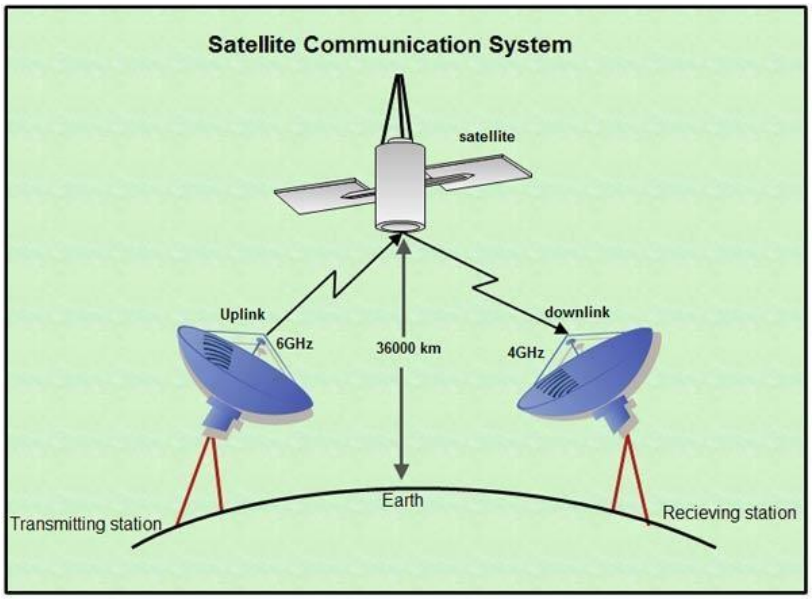



*Fig 5: satellite communication*

*Advantages of satellite communication*

i. Satellite microwave can provide transmission capability to and from any location on earth, n matter how remote

ii. Has the second highest band width after fibre optic

iii. Earth station can be installed on the customer property than layering extensive cables

*Disadvantages of satellite communication*

i. Its extremely expensive to install

ii. Any station can receive the signals

iii. Heavy rains or bad weather will increase loss of signals

### 3. Infrared Transmission

Infrared media uses infrared light to transmit signals. LEDs transmit the signals, and photodiodes receive the signals. The remote control we use for television, VCR and CD player use infrared technology to send and receive signals.

The transmitter and the receiver of the infrared signals must be within the line of sight in the same room. Infrared signals do have a downside; the signals cannot penetrate walls or other objects, and they are diluted by strong light sources.

**4. Radio transmission**

Radio waves are *omnidirectional* meaning that the waves start at a central point and spread outwards to all directions. The waves are radiated into the atmosphere by radio frequency antennae at a constant velocity

The radio wave can be HIGH (HF) high frequency, very high frequency (VHF) or ultra high frequency (UHF). The high frequency radio wave signal is transmitted by directing it to ionosphere of the earth. The ionosphere will reflect it back to the earth surface and the receiver will pick the signal. It was the only way to communicate before the invention of satellite

VHF radio waves are transmitted along the earth surface. UHF radio waves use the line of sight principal thus there should be no barrier between the sending and the receiving devices.

Used in : Radio and television broadcast, walkie-talkies

Disadvantages

i. Signals can be intercepted by a unauthorized parties
ii. VHF require repeaters at strategic points to overcome attenuation
iii. The sender and the receiver must be in line of sight as with UHF

**Transmission Media Problems and Impairment**

Data is transmitted through transmission medium which are not perfect. The imperfection causes signal impairment. Due to the imperfection error is introduced in the transmitted data i.e. the original signal at the beginning of the transmission is not the same as the signal at the Receiver. Some of the transmission media/impairment problems are:

**Attenuation Distortion**

Attenuation results in loss of energy. When a signal travels through a medium, it loses some of its energy in overcoming the resistance of the medium. The electrical energy in the signal may convert to heat. To compensate for this loss, amplifiers are used to amplify the signal. Figure below shows the effect of attenuation and amplification. The loss of signal or attenuation is measured at the receiving end and compared to a standard reference frequency.

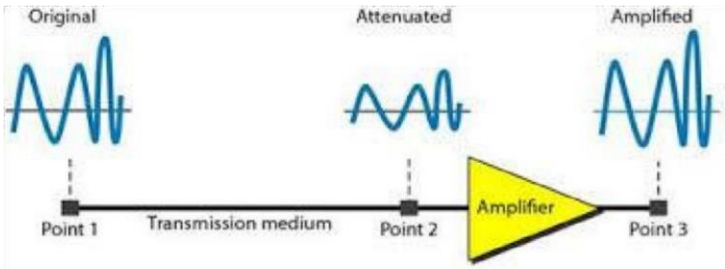



Figure 31: effect of attenuation and amplification.

**Crosstalk**

Crosstalk is when one line induces a signal into another line. In voice communications, we often hear this as another conversation going on in the background. In digital communication, this can cause severe disruption of the data transfer. Cross talk can be caused by overlapping of bands in a multiplexed system or by poor shielding of cables running close to one another. There are no specific communications standards applied to the measurement of crosstalk.

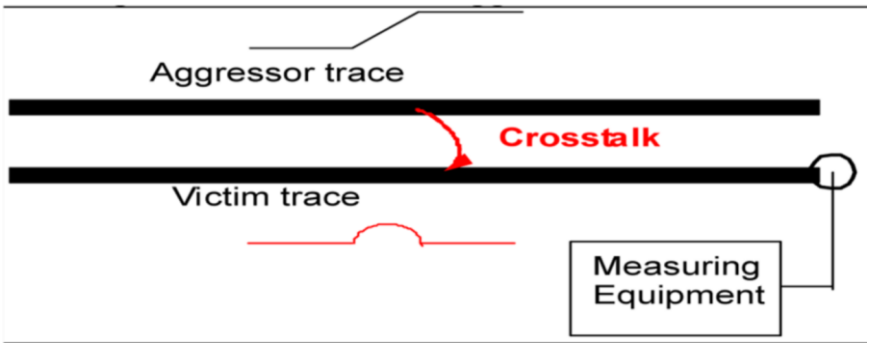



Figure 32: Crosstalk impairment

**Echo or Signal Return**

All media have a preferred termination condition for perfect transfer of signal power. The signal arriving at the end of a transmission line should be fully absorbed otherwise it will be reflected back down the line to the sender and appear as an Echo. Echo Suppressors are often fitted to transmission lines to reduce this effect. Normally during data transmission, these suppressors must be disabled or they will prevent return communication in full duplex mode. Echo suppressors are disabled on the phone line if they hear carrier for 400ms or more. If the carrier is absent for 100 mSec, the echo suppressor is re-enabled. Echo Cancellers are currently used in Modems to replicate the echo path response and then combine the results to eliminate the echo. Thus no signal interruption is necessary.

Noise

Noise is any unwanted signal that is mixed or combined with the original signal during transmission. Due to noise the original signal is altered and signal received is not same as the one sent. Noise is sharp quick spikes on the signal caused from electromagnetic interference, lightning, sudden power switching, electromechanical switching, etc. These appear on the telephone line as clicks and pops which are not a problem for voice communication but can appear as a loss of data or even as wrong data bits during data transfers. Impulse noise has duration of less than 1 mSec and their effect is dissipated within 4mSec.

**Review Questions**

**1.** Explain briefly the following:

i. Attenuation ii. Propagation delay iii. Crosstalk iv. Echo

2. Compare Guided and Unguided transmission with relevant examples

3. Compare coaxial and twisted pair cable transmission based on the following:

a. Attenuation

b. Propagation delay

# CHAPTER THREE

# COMPUTER NETWORKING

**What is Computer Network?**

Computer network is interconnectivity of two or more computer system for purpose of sharing data. A computer network is a communication system much like a telephone system, any connected device can use the network to send and receive information. In essence a computer network consists of two or more computers connected to each other so that they can share resources. Networking arose from the need to share resources in a timely fashion.

## Purpose of networking

***i. Resource sharing***

Different computers are connected to each other hence a user at one site may be able to use the resource available at another site e.g. printer, internet,

***ii. Remote communication***

This involves the transmission of data signals between two communication devices loaded at different geographical locations. Through remote communication people can be able to share ideas and pass messages over the network

***iii. Distributed processing***

If a particular process can be subdivided into several sub-processes then each sub-process can be processed at different sites concurrently hence speeding up the entire process

***iv. Cost effectiveness***

Reduction of resources in a network leads to reduction of cost. In stead of purchasing a printer for each computer you can share one printer thus saving cost

***v. Reliability***

If one site fails in a computer network, the remaining sites can potentially continue operating

## Limitations of networking

***i. Cost***

It's expensive to acquire networking equipments, train network administrators, users and maintain the network

***ii. Data security***

Data and information held on a network is prone to more illegal access, danger of data theft and also tapping of unauthorized people during transmission

***iii. Network failure***

If the network fails there is the danger of paralyzing organization operations besides damaging files and programs

***iv. Moral and cultural effect***

Large networks like internet have chart rooms and messaging services that may enable underage children to meet peers and adults on the net some of whom may have bad intensions. Apparently the access to pornographic and other negative materials is also a problem.

***v. Over reliance on networks***

Most organizations have done away with manual operations. This means that all business process and society depend on computer networks. The disadvantage of over reliance is that if the network fails then many systems will stop operating

## Protocol and Standards In Networking

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol.

A protocol is a set of rules that govern data communications. It defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

- Syntax. The term syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.
- Semantics. The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be takenor the final destination of the message?
- Timing. The term timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload thereceiver and some data will be lost.

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes. Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications. Data communication standards fall into two categories: de facto (meaning "by fact" or "by convention") and de jure (meaning "by law" or "by regulation").

- De facto. Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.
- De jure. Those standards that have been legislated by an officially recognized body are de jure standards

Standards Organizations

Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

Standards Creation Committees

While many organizations are dedicated to the establishment of standards, data telecommunications in North America rely primarily on those published by the following:

- International Organization for Standardization (ISO). The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.
- International Telecommunication Union-
  Telecommunication Standards Sector (ITU-T). By the early 1970s, a number of countries were defining national standards for telecommunications, but there was still little international compatibility. The United Nations responded by forming, as part of its International Telecommunication Union (ITU), a committee, the Consultative Committee for

  International Telegraphy and Telephony (CCITT). This committee was devoted to the research and establishment of standards for telecommunications in general and for phone and data systems in particular. On March 1, 1993, the name of this committee was changed to the International Telecommunication Union Telecommunication Standards Sector (ITU-T).

- American National Standards Institute (ANSI). Despite its name, the American National Standards Institute is a completely private, nonprofit corporation not affiliated with the U.S. federal government. However, all ANSI activities are undertaken with the welfare of the United States and its citizens occupying primary importance.
- Institute of Electrical and Electronics Engineers (IEEE). The Institute of Electrical and Electronics Engineers is the largest professional engineering society in the world. International in scope, it aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well as in all related branches

of engineering. As one of its goals, the IEEE oversees the development and adoption of international standards for computing and communications.

- Electronic Industries Association (EIA). Aligned with ANSI, the Electronic Industries Association is a nonprofit organization devoted to the promotion of electronics manufacturing concerns. Its activities include public awareness education and lobbying efforts in addition to standards development. In the field of information technology, the EIA has made significant contributions by defining physical connection interfaces and electronic signalling specifications for data communication.

## TYPES OF NETWORKS

### Server based

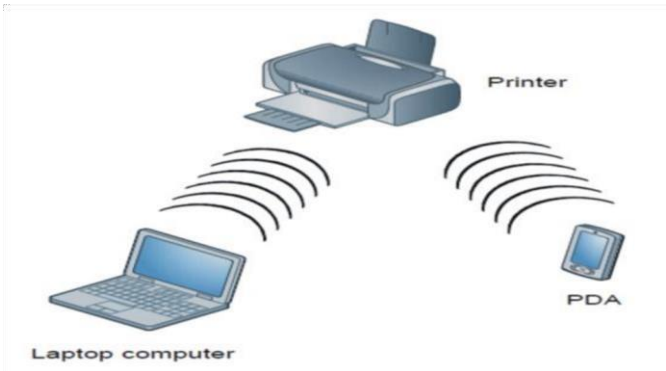
### Peer to peer based

## NETWORK CATEGORIES

There are several different types of computer networks. Computer networks can be characterized by their size as well as their purpose. The size of a network can be expressed by the geographic area they occupy and number of computers that are part of the network. Networks can cover anything from a handful of devices within a single room to millions of devices spread across the entire globe.

### Personal Area Network

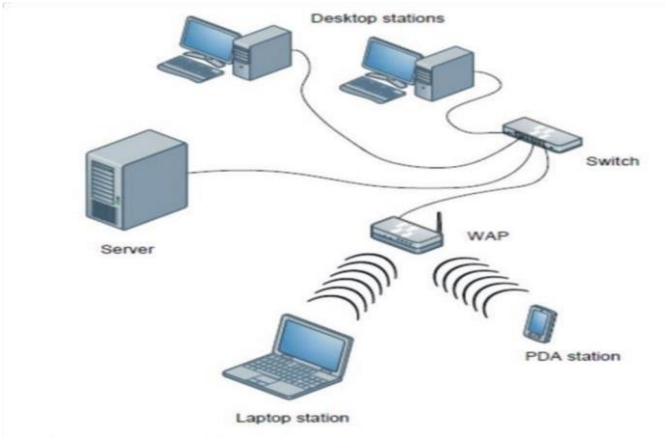
A personal area network (PAN) is the interconnection of information technology devices within the range of an individual person, typically within a range of 10 meters. For example, a person traveling with a laptop, a personal digital assistant (PDA), and a portable printer could interconnect them without having to plug anything in, using some form of wireless technology. Typically, this kind of personal area network could also be interconnected without wires to the Internet or other networks. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink). However, it is possible to have multiple individuals using this same network within a residence. If this is the case we can refer to the network as Home Area network (HAN). In this type of setup, all the devices are connected together using both wired and/or wireless. All networked devices can be connected to a single modem as a gateway to the Internet. See figure 5.




Personal Area Network

## Local Area Network

A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and type of technology used, a LAN can be as simple as two desktops and a printer in someone‟s home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers. In addition to the size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. LANs are designed to allow resources to be shared between personal computers or workstations. Early LANs had data rates in the 4 to 16 mega-bits-per-seconds (Mbps). Today, however, speeds are normally 100Mbps or 1000Mbps. Wireless LANs (WLAN) are the newest evolution in LAN technology. See figure 6.



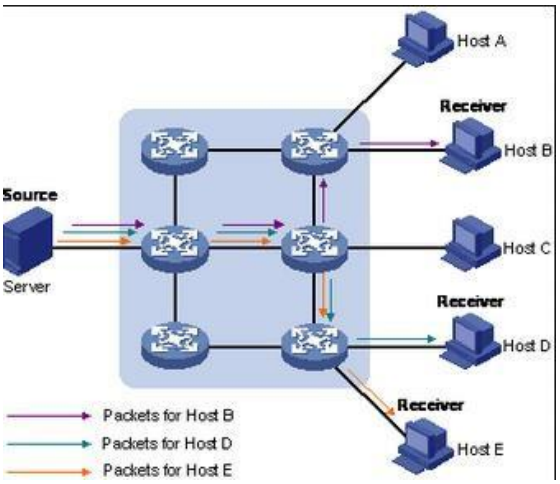

Local Area Network

**LAN Transmission Methods**

LAN data transmissions at Layer 2 fall into three classifications: unicast, multicast, and broadcast. In each type of transmission, a single frame is sent to one node on the network. If the frame is to be sent to more than one node on the network, the sender must send individual unicast data streams to each node.

*i. Unicast*

In a unicast transmission, a single frame or packet is sent from a single source to a single destination on a network. Unicast is a one-to-one transmission method in which the network carries a message to one receiver, such as from a server to a LAN workstation. In a unicast environment, even though multiple users might ask for the same information from the same server at the same time, such as a video clip, duplicate data streams are sent. One stream is sent to each user, as illustrated in the Figure 6-3.

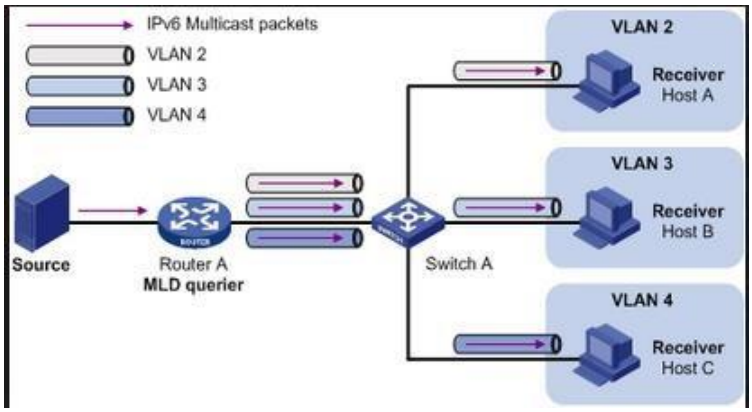



Unicast sends separate data streams to each computer requesting the data, in turn flooding the network with traffic. Unicast might be compared to an after-work gathering. You and several of your co-workers might be going to the same destination, but each taking his own vehicle, flooding the streets with cars. (So the next time you go to an after-work gathering, and each person drives his own car, tell them you're "unicasting.")

*ii. Multicast*

In a multicast transmission environment, a single data frame or a single source to multiple destinations packet is copied and sent to a specific subset of nodes on the network.

Multicast is a one-to-many transmission method in which the network carries a message to multiple receivers at the same time. Multicast is similar to broadcasting, except that multicasting means sending to a specific group, whereas broadcasting implies sending to everybody, whether they want the traffic or not. When sending large amounts of data, multicast saves considerable network bandwidth because the bulk of the data is sent only once. The data travels from its source through major backbones and is then multiplied, or distributed out, at switching points closer to the end users (see Figure 6-4). This is more efficient than a unicast system, in which the data is copied and forwarded to each recipient.



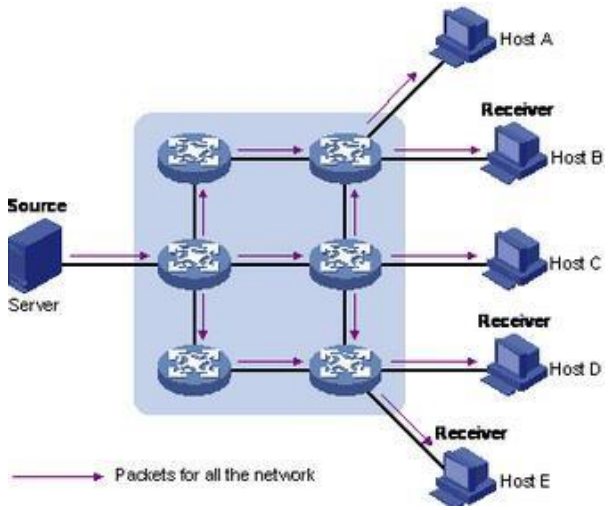

Multicast conserves network bandwidth by sending a single data stream across the network, much as you and others might carpool to and from work, thereby reducing the traffic on the roads. For example, a few of you might ride together to some point, such as a drop-off point in the city, and then disperse from there. Multicasting works in the same way by using the concept of shared transmission

across a network. Multicasting sends the data to a predetermined endpoint, such as a switch, where the traffic is sent to each intended recipient, instead of each traffic stream being sent from start to finish across the network, independent of others.

*iii. Broadcast*

In a broadcast transmission environment from a single source to all nodes, a single data frame or packet is copied and sent to all nodes on the network.

Broadcast is a one-to-all transmission method in which the network carries a message to all devices at the same time, as illustrated in Figure 6-5.




Broadcast message traffic is sent out to every node on the network where the broadcast is not filtered or blocked by a router. Broadcasts are issued by the Address Resolution Protocol (ARP) for address resolution when the location of a user or server is not known. For example, the location could be unknown when a network client or server first joins the network and identifies itself. Sometimes broadcasts are a result of network devices continually announcing their presence in the network, so that other devices don't forget who is still a part of the network. Regardless of the reason for a broadcast, the broadcast must reach all possible stations that might potentially respond.

***Media Access Methods***

Currently, there are four approaches that are the most popular. They are contained in the following list.

I. Carrier Sense Multiple Access With Collision Detection (CSMA/CD)

Is a media access control method used most notably in LAN using early Ethernet technology. It uses a carrier sensing scheme in which a transmitting data station detects other signals while transmitting a frame, and stops transmitting that frame, transmits a jam signal, and then waits for a random time interval before trying to resend the frame.

II. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

CSMA/CA in computer networking is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by transmitting only when the channel is sensed to be "idle". When they do transmit, nodes transmit their packet data in its entirety. It is particularly important for wireless networks, where the collision detection of the alternative CSMA/CD is unreliable due to the hidden node problem.

CSMA/CA is a protocol that operates in the Data Link Layer (Layer 2) of the OSI model.

Carrier Sense: prior to transmitting, a node first listens to the shared medium (such as listening for wireless signals in a wireless network) to determine whether another node is transmitting or not. Note that the hidden node problem means another node may be transmitting which goes undetected at this stage.

Collision Avoidance: if another node was heard, we wait for a period of time for the node to stop transmitting before listening again for a free communications channel.

Request to Send/Clear to Send (RTS/CTS) may optionally be used at this point to mediate access to the shared medium. This goes some way to alleviating the problem of hidden nodes because, for instance, in a wireless network, the Access Point only issues a Clear to Send to one node at a time. However, wireless 802.11 implementations do not typically implement RTS/CTS for all transmissions; they may turn it off completely, or at least not use it for small packets (the overhead of RTS, CTS and transmission is too great for small data transfers).

Transmission: if the medium was identified as being clear or the node received a CTS to explicitly indicate it can send, it sends the frame in its entirety. Unlike CSMA/CD, it is very challenging for a wireless node to listen at the same time as it transmits (its transmission will dwarf any attempt to listen). Continuing the wireless example, the node awaits receipt of an acknowledgement packet from the Access Point to indicate the packet was received and checksummed correctly. If such acknowledgement does not arrive after a timely manner, it assumes the packet collided with some other transmission, causing the node to enter a period of binary exponential backoff prior to attempting to re-transmit.

III. Token Passing.

Token Passing is a non-contention method in that two devices cannot transmit signals at the same time. Each device needs to wait to get the token before it can transmit. The token circulates on the network until it reaches a device with data to send.

The most common token passing approach is called Token Ring. When the token gets to a computer that is waiting to send, the device takes control of the token. It appends its data to the token signal and puts it back out on the network. The data has the destination address and the token moves around the network in its established order until it reaches the device with the appropriate address.

When the appropriate receiving device gets the token it takes the data and appends a successful reception message to the token and sends it back around. The sending computer

regains control of the token and then sends more data or puts it back out on the network as free to receive data and direction.

Some authors estimate that Token Rings can make use of about 75% of the network bandwidth. While considerably more efficient than Ethernet, it is more expensive and slightly more difficult to configure.

Some token passing architecture actually make use of multiple tokens. One example of this is called FDDI - Fiber Distributed Data Interface. This will be described in later web pages.

IV. Demand Priority.

Was developed by Hewlett Packard to be used with VG AnyLAN. This was designed to be a flexible, high speed and efficient replacement to Ethernet.

The demand priority method makes use of multiport hubs that conduct round robin searches of the connected devices looking for requests to transmit. The underlying topology is a star wired tree. The hubs can be cascaded off a root hub for centralized control.

The administrator is able to set priorities on certain types of data. For example, you might choose to give e-media transmissions priority.

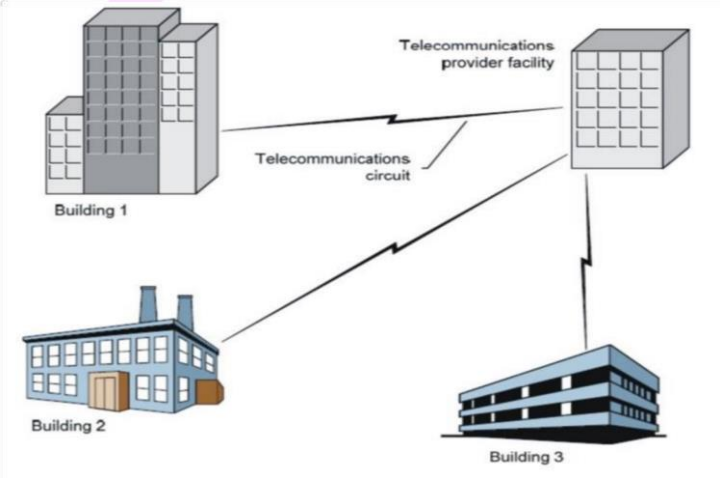
It also usually makes use of a cabling with four pairs of wires that enables simultaneous transmission and reception. Though it can use of two pair STP, two or four pair UTP or fiber optic cabling. The hubs are also configured to limit where the original message is broadcast. It is restricted to devices connected to the same hub.

Each hub interacts with other hubs and is unaware of specific devices attached to another hub. Each hub is only aware of devices to which it is attached.

Because not all data goes through all stations it is inherently more secure than Ethernet or Token Ring

## Metropolitan Area Network

A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a highspeed connectivity, normally to the internet, and have endpoints spread over a city or part of city. A good example of a MAN is part of the telephone company network that can provide a high-speed DSL line to the customer.

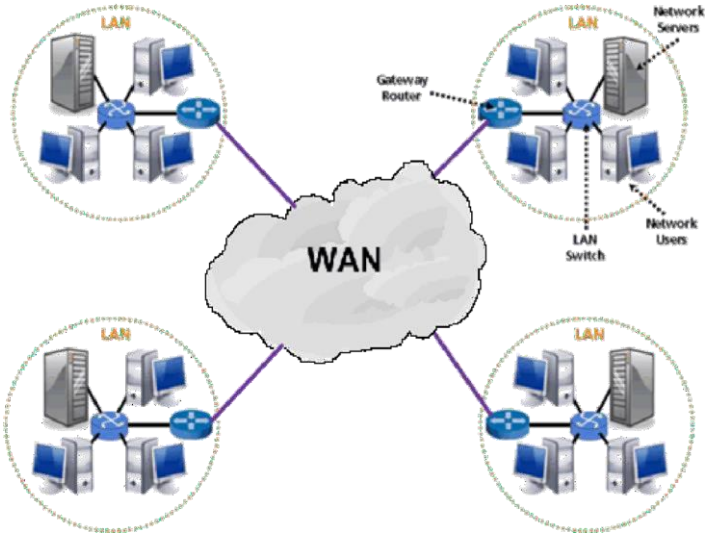



Metropolitan area Network

## Wide Area Network

A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the internet. We normally refer to the first one as a switched WAN and to the second as a point-to-point WAN.

The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN. The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an internet service provider (ISP). A good example of a switched WAN is X.25, the asynchronous transfer mode (ATM) network. See figure 8.




Wide Area Network

***WAN Connection Types:***

*i. Leased Lines*

Typically referred to as a point-to-point connection or dedicated connection. Is is a preestablished WAN communications path from the CPE, through the DCE switch, to the CPE of the remote site, allowing DTE networks to communicate at any time with no setup procedures before transmitting date. It uses synchronous serial lines up to 45 Mbps

*ii. Circuit Switching*

Sets up like a phone call. No data can transfer before the end-to-end connection is established. Uses dial-up modems and ISDN. It is used for low-bandwidth data transfers.

*iii. Packet Switching*

WAN switching method that allows you to share bandwidth with other companies to save money. As long as you are not constantly transmitting data and are instead using bursty data transfers, packet switching can save you a lot of money. However, if you have a constant data transfers, you will need to use a leased line. Frame Relay and X.25 are packet switching technologies. Speeds can vary from 56 Kbps to 2.048 Mbps.

***WAN Protocols:***

*i. Frame Relay*

Frame Relay is a Date Link and Physical Layer specification that provides high performance. Frame Relay assumes that the facilities used are less error prone than when X.25 was being implemented and that they use less overhead. Frame Relay is more cost-effective than point-topoint links and can run at speeds of 64Kbps to 45Mbps. Frame Relay provides features for dynamic-bandwidth allocation and congestion control.

*ii. X.25*

International Telecommunication Union (ITU-T) standard that defines how connections between DTE and DCE are maintained for remote terminal access and computer communications in PDNs(Public Data Networks). X.25 specifies LAPB, a data link layer protocol, and PLP, a network layer protocol. Frame Relay has to some degree superseded X.25.

*iii. ISDN*

Integrated Services Digital Network is a set of digital services that transmit voice and data over existing phone lines. ISDN can offer a cost-effective solution for remote users who need a higher-speed connection than an analog dial-up link offers. ISDN is also a good choice as a backup link for other types of links such as Frame Relay or a T-1 connection.

It is indented to be worldwide public telecommunication network to replace existing public service telephone network and thereby have variety of services to provide. The concept of ISDN is best described by considering it from several view points;

- Principles of ISDN
- User interface
- Its objectives

**Principles of ISDN**

The following principles and evolution of ISDN are based on the CCITT Recommendation I.120 (1988) for Integrated Services Digital Networks. CCITT defines the standards for ISDN. There are six key points.

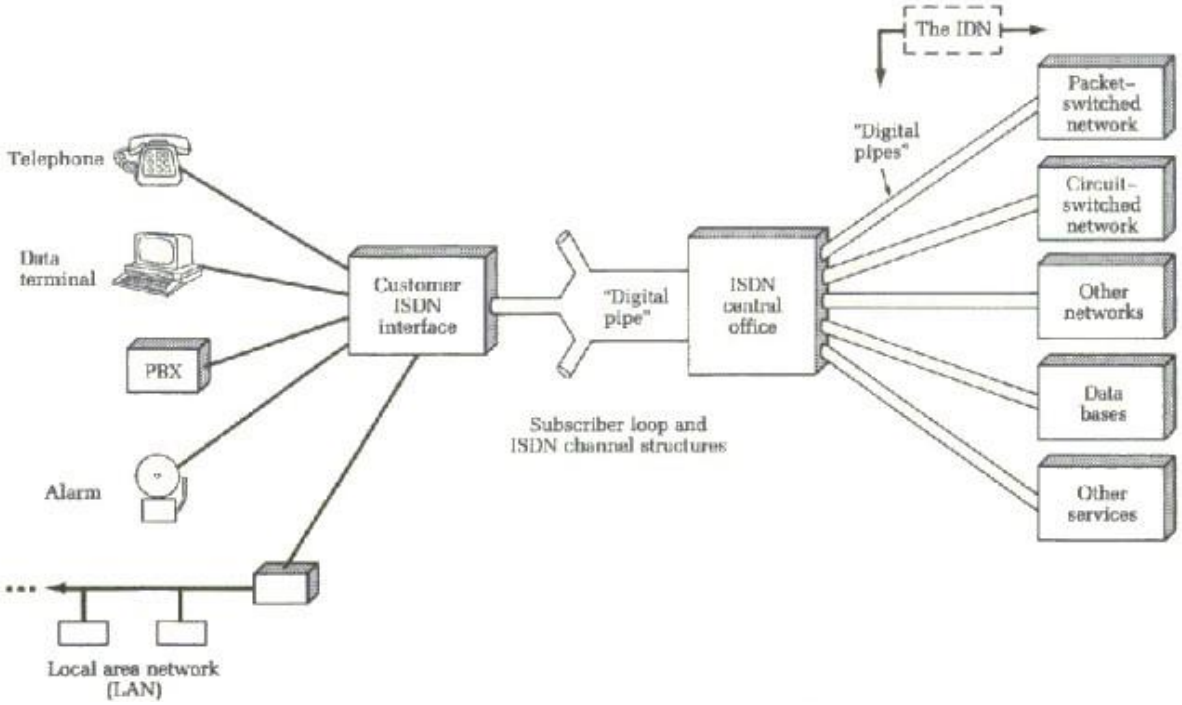
i. To support voice and non voice applications using a limited set of standardized facilities. This means that ISDN will carry telephone calls and the exchange of digital data in conformance with CCITT recommendations specifying a small number of interfaces and transmission facilities.

ii. Support for switched and non-switched applications. This means that ISDN will support packet switching, circuit switching and dedicated non-switched lines (leased lines). iii. Reliance on 64kbps connections (B channels). The intention of ISDN is to provide circuit and packet-switched connections at 64kbps, the fundamental building block of ISDN. The reasoning for the use of this rate was to support digitised voice and was the standard or evolving digital networks. This data rate is now being seen as restrictive and future developments of ISDN will permit higher rates. A data channel (D channel) handles signaling at 16 kbps or 64 kbps, depending on the service type.

iv. Intelligence in the network. ISDN should provide more sophisticated services than that of purely setting up circuit switched calls.

v. Layered protocol architecture. The protocols for user access to ISDN can be mapped into the OSI model. This allows standards developed for OSI to be used over ISDN e.g. x.25 level 3 for access to ISDN packet switching services. Also new ISDN standards can be based on existing standards, thus reducing implementation cost. One example here is LAPD, based on LAPB. Standards can be developed and implemented independently for each layer. New paths may be provided through a layer, allowing customers to implement ISDN at their own pace.

vi. Variety of configurations. This allows ISDN to be implemented using more than one physical implementation permitting differences in national policy, competition between network providers, types of technology and types of customer equipment. **User interface**




***Conceptual view of ISDN Connection***

The diagram above shows a conceptual view of ISDN from the user or customer point of view. The user has access to ISDN by means of a local interface to the digital pipe of a certain bit rate of various sizes that are available depending on different needs.

**Objectives of the ISDN**

Activists currently are leading to a development of World Wide ISDN. This requires combination of governments, telecommunication companies and standard organization e.g. IEEE.

1. Standardization

ISDN standards should be provided to permit universal access and provide cost effective equipment.

2. Transparency

The most important service provided is transparency transmission of service thereby permitting users to develop applications and protocols with confidence that they will not be affected by the underlying ISDN architecture. Separation of competitive functions

It must be possible to separate functions that could be provided competitively as opposed to those that are permanently part of ISDN. 3. Leased and switched service

ISDN should provide dedicated point to point services as well as switched services thereby allowing user to optimize implementation of switching techniques. 4. Cost related tariffs

The price of ISDN services should be related to cost and should be independent of the type of data being carried.

5. Smooth migration

The conversion of ISDN should be gradual and evolving network should coexist with existing equipment and services.

6. Multiplexed support

In addition to providing low capacity support to individual users, multiplexed support must be provided to accommodate user owned Pbx and local network equipment.

**Services (user access)**
To define the requirement for ISDN user access an understanding of anticipated configuration of user premises equipment and the necessary standard interfaces is important. The first step is to group functions that may exist on the user premises.

Functional groupings

Certain finite arrangement of physical equipment or combinations of equipment must be done.

Reference points

To conceptual points should be used to separate the groups of functions that have been done in number one. The architecture of subscriber's premises is broken up functionally into groupings separated by reference points. This separation permits interface standards to be developed at each reference point. This is used to give guidance to the equipment providers. Once a stable interface standard exist technical important on the other side of interface can be made without affecting the groupings. Finally with stable interfaces some subscriber is free to procedure equipment from different suppliers for the various functional groupings so long as the equipment conforms to the relevant interface standards.

*LAPB*
Link Access Procedure Balanced was created to be used as a connection-oriented protocol at the Data Link layer for use with X.25. It can also be used as a simple Data Link transport. LAPB has a tremendous amount of overhead because of its strict timeout and windowing techniques. You can use LAPB instead of the lower-overhead HDLC if your links are very error prone. However, that typically is not a problem anymore.

*iv.* High-Level Data Link Control (*HDLC)*

Was derived from SDLC, which was created by IBM as a Data Link connection protocol. HDLC is a connection-oriented protocol at the Data Link layer, but it has very little overhead compared to LAPB. HDLC was not intended to encapsulate multiple Network layer protocols across the same link. The HDLC header carries no identification of the type of protocol being carried inside the HDLC encapsulation. Because of this, each vendor that uses HDLC has their own way of identifying the Network layer protocol, which means that each vendor's HDLC is proprietary for their equipment.

*v.* Synchronous Data Link Control *(SDLC)*

SDLC is a bit-oriented, full-duplex serial protocol that has spawned numerous protocols,

including HDLC and LAPB *vii.* Point-to-Point protocol (*PPP)*

Is an industry standard protocol because many versions of HDLC are proprietary, PPP can be used to create point-to-point links between different vendor's equipment. It uses a Network Control Protocol field in the Data Link header to identify the Network layer protocol. It allows authentication and multilink connections and can be run over asynchronous and synchronous links.

*Other Types of Area Networks*

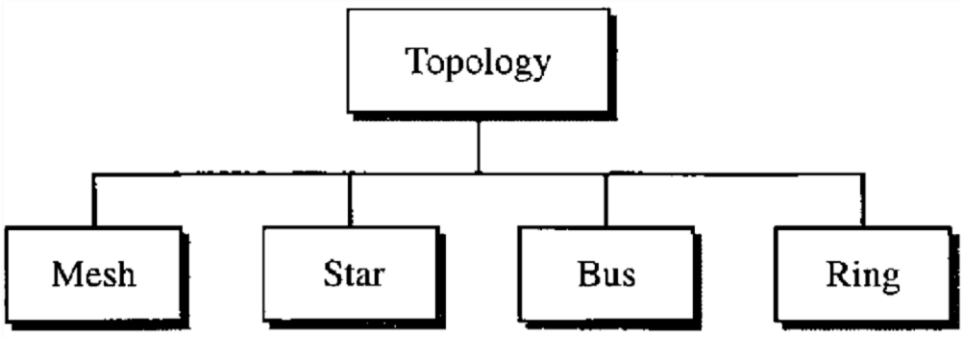
While LAN and WAN are by far the most popular network types mentioned, you may also commonly see references to these others:

*i.* *Wireless Local Area Network*

A LAN based on WiFi wireless network technology *ii.*

## NETWORK TOPOLOGIES

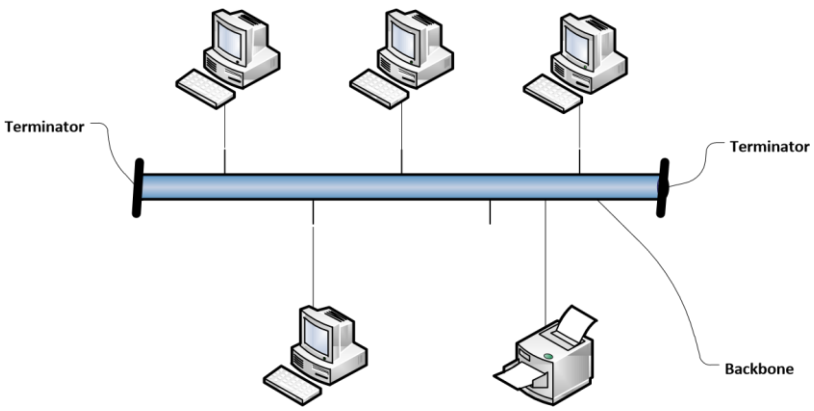
The term topology in computer networking refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all links and linking devices (usually called nodes) to one another. The cost and flexibility of a network installation are partly affected by as is system reliability. Many network topologies are commonly used, but they all have certain similarities. Information is carried either through space (wireless) or cable. The cable must control the movement of information on the network so that data can be transmitted in a reliable manner. There are four basic topologies possible: mesh, star, bus, and ring. See Figure 9.




Network Topology categories

### Bus Topology

The Bus topology consists of a single cable that runs to every workstation. See figure 10. The bus topology is also known as linear bus. In other words, all the nodes (computers and servers) are connected to the single cable (called bus), by the help of interface connectors. This central cable is the back bone of the network and every workstation communicates with the other device through this bus.




Bus Topology

Computers on a bus topology network communicate by addressing data to a particular computer and putting that data on the cable in the form of electronic signals. To understand how computers communicate on a bus you need to be familiar with three concepts:

i. **Sending the signal:** Network data in the form of electronic signals is sent to all of the computers on the network; however, the information is accepted only by the computer whose address matches the address encoded in the original signal. Only one computer at a time can send messages.

Because only one computer at a time can send data on a bus network, network performance is affected by the number of computers attached to the bus. The more computers on a bus, the more computers there will be waiting to put data on the bus, and the slower the network.

There is no standard measure for the impact of numbers of computers on any given network. The amount the network slows down is not solely related to the number of computers on the network. It depends on numerous factors including:

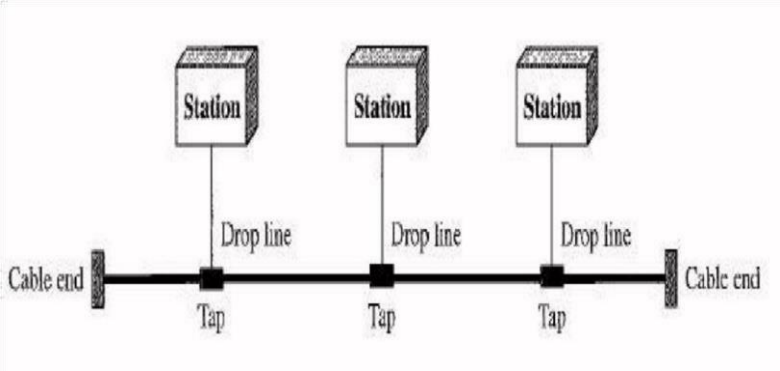
- Hardware capacities of computers on the network
- Number of times computers on the network transmit data
- Type of applications being run on the network
- Types of cable used on the network
- Distance between computers on the network

The bus is a passive topology. Computers on a bus only listen for data being sent on the network. They are not responsible for moving data from one computer to the next. If one computer fails, it does not affect the rest of the network. In active topology computers regenerate signals and move data along the network.

ii. **Signal Bounce:** Because the data, or electronic signal, is sent to the entire network, it will travel from one end of the cable to the other. If the signal were allowed to continue uninterrupted, it would keep bouncing back and forth along the cable and prevent other computers from sending signals. Therefore, the signal must be stopped.

The Terminator: To stop the signal from bouncing, a component called a terminator is placed at each end of the cable to absorb free signals. Absorbing the signal clears the cable so that other computers can send data. Every cable end on the network must be plugged into something. For example, a cable end could be plugged into a computer or a connector to extend the cable length. Any open cable ends-ends not plugged into something – must be terminated to prevent signal bounce.

In bus topology nodes are connected to the bus cable by drop lines and taps. See figure 11. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.




Bus Topology with three stations

Advantages of Linear Bus Topology

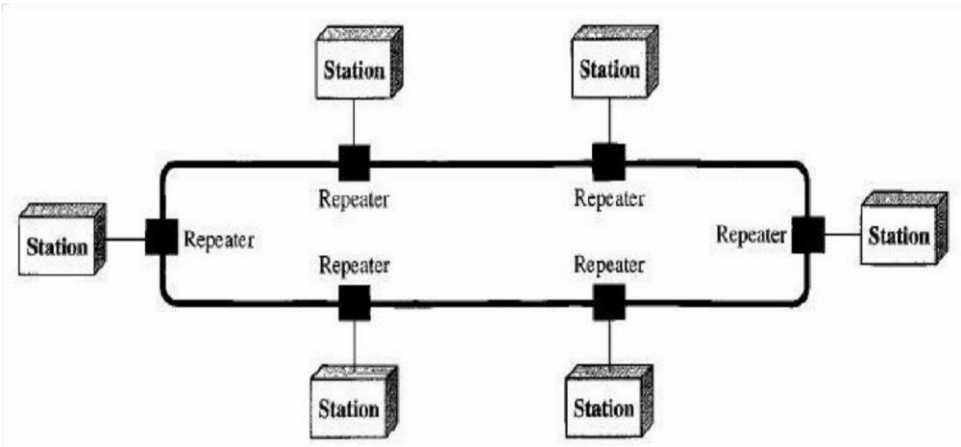
1) It is easy to set-up and extend bus network.
2) Cable length required for this topology is the least compared to other networks.
3) Bus topology very cheap.
4) Linear Bus network is mostly used in small networks.

Disadvantages of Linear Bus Topology

1) There is a limit on central cable length and number of nodes that can be connected.
2) Dependency on central cable in this topology has its disadvantages. If the main cable (i.e. bus) encounters some problem, whole network breaks down.
3) Proper termination is required to dump signals. Use of terminators is must.
4) It is difficult to detect and troubleshoot fault at individual station.
5) Maintenance costs can get higher with time.
6) Efficiency of Bus network reduces, as the number of devices connected to it increases.
7) It is not suitable for networks with heavy traffic.
8) Security is very low because all the computers receive the sent signal from the source.

## Ring Topology

The ring topology connects computers on a single circle of cable. There are no terminated ends. A ring topology connects one host to the next and the last host to the first. The signal travels around the loop in one direction and pass through each computer. Unlike the passive bus topology, each computer acts like a repeater to boost the signal and send it on to the next computer. Because the signal passes through each computer, the failure of one computer can impact the entire network.




Ring Topology

One method of transmitting data around a ring is called token passing. The token is passed from computer to computer until it gets to a computer that has data to send. The sending computer modifies the token, puts an electronic address on the data, and sends it around the ring.

Advantages of Ring Topology

1) This type of network topology is very organized. Each node gets to send the data when it receives an empty token. This helps to reduces chances of collision. Also in ring topology all the traffic flows in only one direction at very high speed.
2) Even when the load on the network increases, its performance is better than that of Bus topology.
3) There is no need for network server to control the connectivity between workstations.
4) Additional components do not affect the performance of network.
5) Each computer has equal access to resources.

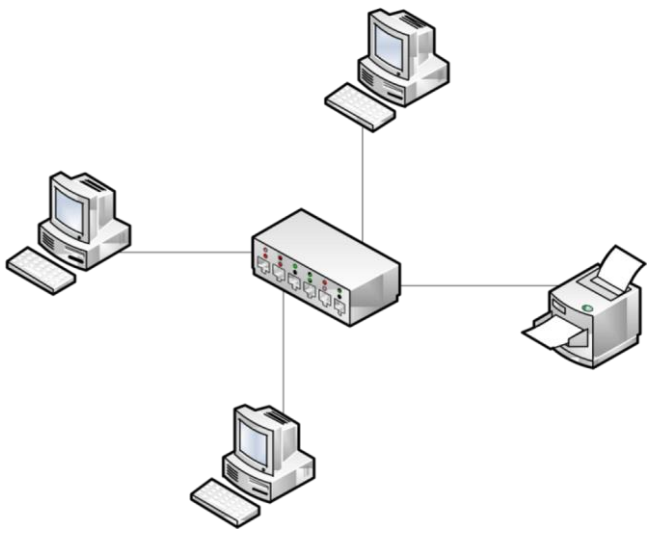
Disadvantages of Ring Topology

1) Each packet of data must pass through all the computers between source and destination. This makes it slower than Star topology.
2) If one workstation or port goes down, the entire network gets affected.
3) Network is highly dependent on the wire which connects different components.
4) MAU‟s and network cards are expensive as compared to Ethernet cards and hubs.

## Star Topology

In the star topology, computers are connected by cable segments to centralized component, called a hub or switch.

Signals are transmitted from the sending computer through the hub or switch to all computers on the network. This topology originated in the early days of computing with computers connected to a centralized mainframe computer. It is now a common topology in microcomputer networking. Each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device



Star Topology

The star network offers centralized resources and management. However, because each computer is connected to a central point, this topology requires a great deal of cable in a large network installation. Also, if the central point fails, the entire network goes down.

**Advantages of Star Topology**

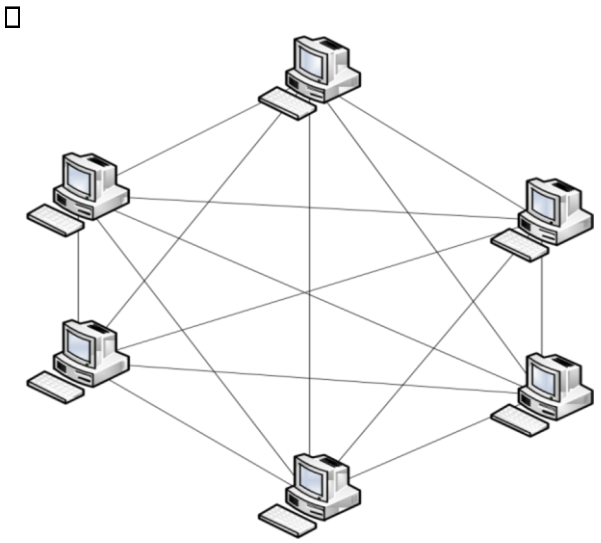
1) As compared to Bus topology it gives far much better performance, signals don‟t necessarily get transmitted to all the workstations. A sent signal reaches the intended destination after passing through no more than 3-4 devices and 2-3 links. Performance of the network is dependent on the capacity of central hub.
2) Easy to connect new nodes or devices. In star topology new nodes can be added easily without affecting rest of the network. Similarly components can also be removed easily.
3) Centralized management. It helps in monitoring the network.
4) Failure of one node or link doesn‟t affect the rest of network. At the same time it is easy to detect the failure and troubleshoot it.

**Disadvantages of Star Topology**

1) Too much dependency on central device has its own drawbacks. If it fails whole network goes down.
2) The use of hub, a router or a switch as central device increases the overall cost of the network.
3) Performance and as well number of nodes which can be added in such topology is depended on capacity of central device.

## Mesh Topology

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. In a mesh topology, Node1 must be connected to n1 nodes, node2 must be connected to (n – 1) nodes, and finally node n must be connected to (n – 1) nodes. We need n (n - 1) physical links. In other words, we can say that in a mesh topology, we need $n(n\ 1) / 2$ .



Mesh topology

To accommodate many links, every device on the network must have (n – 1) input/output (I/O) ports to be connected to the (n – 1) stations as shown in Figure above. For these reasons a mesh topology is usually implemented in a limited fashion, as a backbone connecting the main computers of a hybrid network that can include several other topologies. One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Advantages of Mesh topology

**1)** Data can be transmitted from different devices simultaneously. This topology can withstand high traffic.
**2)** Even if one of the components fails there is always an alternative present. So data transfer doesn‟t get affected.
**3)** Expansion and modification in topology can be done without disrupting other nodes.

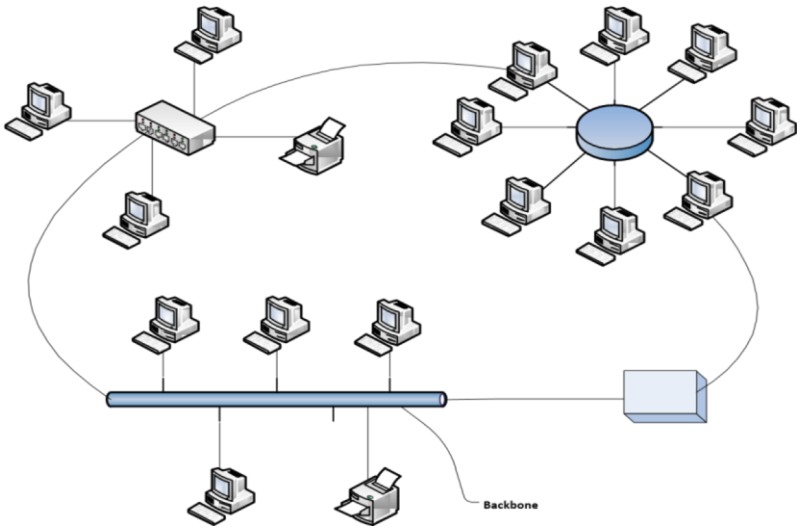
Disadvantages of Mesh topology

**1)** There are high chances of redundancy in many of the network connections.
**2)** Overall cost of this network is way too high as compared to other network topologies.
**3)** Set-up and maintenance of this topology is very difficult. Even administration of the network is tough.

## Hybrid Topology

Before starting about Hybrid topology, we saw that a network topology is a connection of various links and nodes, communicating with each other for transfer of data. We also saw various advantages and disadvantages of Star, Bus, Ring, Mesh. Hybrid, as the name suggests, is mixture of two different things. Similarly in this type of topology we integrate two or more different topologies to form a resultant topology which has good points (as well as weaknesses) of all the constituent basic topologies rather than having characteristics of one specific topology. This combination of topologies is done according to the requirements of the organization.

For example, if there is an existing ring topology in one office department while a bus topology in another department, connecting these two will result in Hybrid topology. Remember connecting two similar topologies cannot be termed as Hybrid topology. Star-Ring and Star-Bus networks are most common examples of hybrid network.




Hybrid Network

Advantages of Hybrid Network Topology

1) Reliable: Unlike other networks, fault detection and troubleshooting is easy in this type of topology. The part in which fault is detected can be isolated from the rest of network and required corrective measures can be taken, WITHOUT affecting the functioning of rest of the network.
2) Scalable: It‟s easy to increase the size of network by adding new components, without disturbing existing architecture.
3) Flexible: Hybrid Network can be designed according to the requirements of the organization and by optimizing the available resources. Special care can be given to nodes where traffic is high as well as where chances of fault are high.
4) Effective: Hybrid topology is the combination of two or more topologies, so we can design it in such a way that strengths of constituent topologies are maximized while there weaknesses are neutralized. For example we saw Ring Topology has good data reliability (achieved by use of tokens) and Star topology has high tolerance capability (as each node is not directly connected to other but through central device), so these two can be used effectively in hybrid star-ring topology.

Disadvantages of Hybrid Topology

1) Complexity of Design: One of the biggest drawbacks of hybrid topology is its design. It is not easy to design this type of architecture and it‟s a tough job for designers. Configuration and installation process needs to be very efficient.
2) Costly Hub: The hubs used to connect two distinct networks, are very expensive. These hubs are different from usual hubs as they need to be intelligent enough to work with different architectures and should be function even if a part of network is down.
3) Costly Infrastructure: As hybrid architectures are usually larger in scale, they require a lot of cables; cooling systems, sophisticate network devices, etc.

## Review Questions

1. Enumerates five components of a data communications system.
2. Define key element of protocol.
3. Define two types of standards.
4. Describe the role of the following standards creation committee.

**i.** International Organization for Standardization (ISO).

**ii.** International Telecommunication Union

**iii.** American National Standards Institute (ANSI).

**iv.** Institute of Electrical and Electronics Engineers (IEEE).

**1)** What are the three criteria necessary for an effective and efficient network?

**2)** Categorize the four basic topologies in terms of line configuration.

**3)** Name the four basic network topologies, and cite an advantage of each type.

**4)** For n devices in a network, what is the number of cable links required for a mesh, ring, bus, and star topology?

**5)** What are some of the factors that determine whether a communication system is a LAN or WAN?

**6)** Assuming you get a job as a network engineer in a multinational company that has five (5) regional station that must be interconnected with others for smooth operation of the organization. The company is about to network the regional offices together. Each physical link must allow communication in both directions. Use the knowledge acquired in this course to advice the management of the company based on the following:

**a)** Recommend the most suitable Network topology for the organization.

**b)** Give detail explanation of the recommended Topology.

**c)** Illustrate the explanation in (b) with a diagram to show the interconnectivity of the five (5) regional offices.

**d)** Explain four (4) major advantages of the topology named in (a) over other network topology.

# CHAPTER FOUR

# NETWORKING COMPONENTS AND MODELS

Networking means connecting two or more devices for the purpose of sharing data and resources. When two or more separate networks are connected for exchanging data or resources, they become an internetwork (or internet). The devices required to link number of LANs into an Internet are known as internetworking devices.

Factors to consider when purchasing communication devices

i. Cost
ii. Warrant
iii. Reputation of company and brand
iv. Compatibility with your other devices

## Networking Devices

Expansion within a single network, called network connectivity and to expand a single network the following networking devices can be used.

i. Hub
ii. Network interface card
iii. Repeaters
iv. Bridges

## Internetworking Devices

Expansion that involves and joins two separate networks called internetworking connectivity. Following devices can be used for internetworking.

i. Routers
ii. Brouters
iii. Gateways
iv. Switches

### Hub

It's a component that connects computers with the same network architecture / communication protocol to enable rely of signals from one computer to another. A hub organizes the cables and relays signals to the other media segments. Hubs usually broadcast the data signals to all the computers in the network but only the one whose address is on the message will receive.

Intelligent hubs are able to monitors the way computers are communicating on a network and keep this information in their small database called management information database (MIB). Intelligent hubs can isolate non-functioning computers in a network

Broadcast storm is a condition where a network is overwhelmed with messages broadcasted due to malfunctioning of the NIC or the hub related problem especially when several hubs are joined together to expand the network

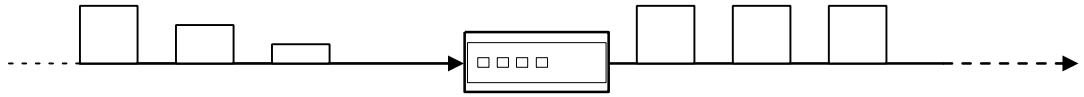
### Network Interface Card (NIC)

It is a circuit board that can be inbuilt with the motherboard or fitted in the expansion slot of the workstation and creates a physical interface / link between computer and the networking media.

**Repeater**

It receives a signal from one segment of the network, cleans it to remove any distortion, boots it and then sends it to another segment

A repeater installed on a link receive the signal before it becomes too week or corrupted, regenerates the original bit pattern, and puts the refreshed signals back onto the link.



Incoming weak signals Repeater Regenerated signals

Repeater

**Bridge**

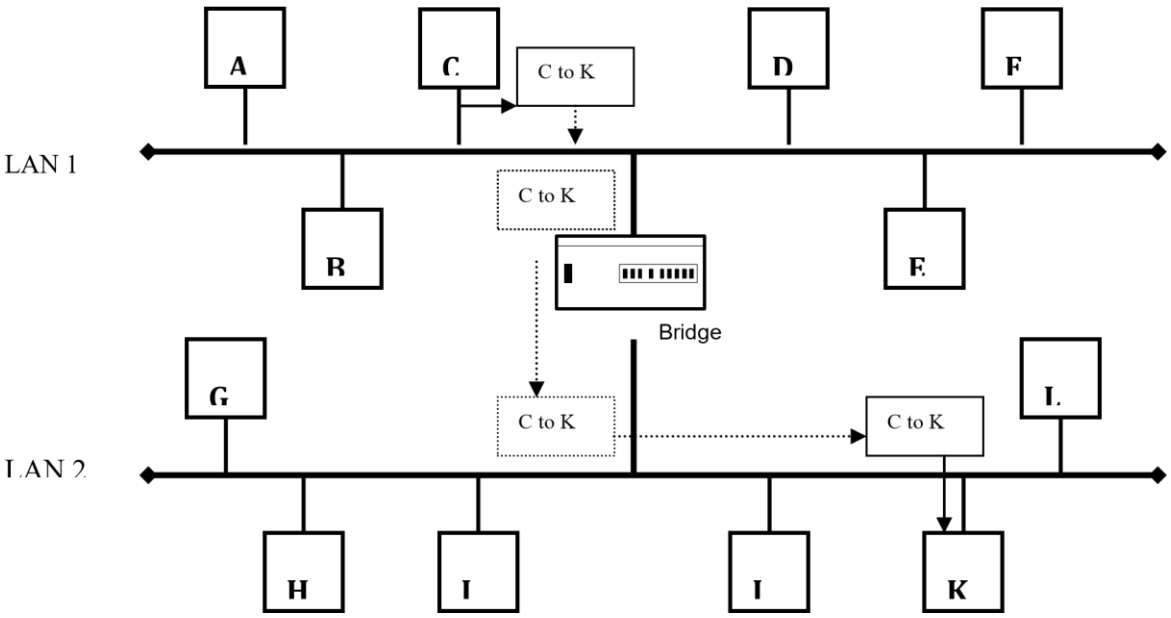
It's a functional unit that interconnect two LANs that use the same logical link control protocol but may use different medium access control protocol

It's a network device that selectively determines the appropriate network segment for which a message is meant for delivery through address filtering

**Purpose**

i. Extend the number of stations a segment can support

ii. Reduce the overall traffic flow by allowing broadcasting only in the destination segment of the network




*Bridge*

In above figure, the packet generated by computer C is intended for computer K. The bridge allows the packet to cross and relay it to the entire lower segment where it is

received by computer K. IF a packet is destined on a same segment (for example from computer A to computer F) the bridge will block the packet from crossing into lower segment to reduce the traffic.

**Internetworking**

**Router**

Routers are used to connect separate networks. It makes the use of an internet protocol and assumes that all the attached devices on the network use the same communication architecture and protocol.

Modern router can be used like bridges to connect multiple network segments and filter traffic. Also, unlike bridges, routers can be used to connect two or more independent networks.

For example a network X and Y with different internet protocol address (IP Address) can interconnected so that users on each network can share resources on the other network and still both network continue to function separately.

**Brouters**

Brouters combines the best of both bridges and routers. When brouters receive packets that are routable, they will operate as a router by choosing the best path for the packet and forwarding it to its destination. However, when a non-routable packet is received, the brouter functions as a bridge, forwarding the packet based on hardware address. To do this brouters maintain both bridging table, which contains hardware address, and a routing table, which contains network address.

**Gateway**

It's a device that can be configured to provide access to wide area network or Internet. Gateways operate in all seven layers of OSI model. A gateway is a protocol converter. A gateway can accept a packet formatted for one protocol (e.g. AppleTalk) and convert it to a packet formatted for another protocol (e.g. TCP/IP) before forwarding it. It may be a computer configured to access the Internet

**Switches**

Switches unlike the hub, they forward a packet of data directly on the address node without broadcasting. It transmits the packet using the point to point transmission as if they were linked by a direct cable between them. They are more expensive than the hubs. Switching hubs are those hubs that incorporate the switching mechanism.

## TYPES OF NETWORK MODELS

### THE OSI 7 LAYER MODEL

Introduction to open system connections

Networks are complicated structures with many interrelated parts. To better understand how the various parts fit together, it is useful to have a network model. A network model is like a generic car. Every car has wheels, a steering, an engine, headlights, and breaks. Similar to a car, every network has a physical layer, a data link layer, and a network layer, and so on.

One car can be automatic and another can be manual; one car may have engine in front and another can have engine in back. Likewise on network may implement the physical or data link layer differently than another, but they both are networks, and they both have layers in one form or another.

WHY OSI: OSI was created to standardize the rules of networking in order for all systems to be able to communicate. In order for communication to occur on a networking using different device drivers and protocol stacks, the rules for communication must be explicitly defined. Why OSI was developed:

i. Reduce Network communication complexity: one big problem to seven smaller ones

ii. Standardizes interfaces

iii. Facilitate modular engineering

iv. Assures interoperable technology

v. Accelerated evolution by making it easy to replace a single layer with a different version

vi. Simplifies teaching and learning

vii. Testing and maintenance is simplified

The OSI model deals with the following issues;

i. How a device on a network sends its data, and how it knows when and where to send it

ii. How a device on a network receives its data, and how to know where to look for it. iii. How devices using different languages communicate with each other. iv. How devices on a network are physically connected to each other.

v. How protocols work with devices on a network to arrange data.

The OSI model is broken down into 7 layers. For now, remember this little trick; *Please Do Not Tell Secret Passwords Anytime.*

OSI Reference Model

OSI (Open System Interconnection) is the most widely accepted model for understanding the network communication. It is developed by ISO (International Standards Organization) in 1977. ISO is a multinational body dedicated to worldwide agreement on international standards. It covers all aspects of network communications in OSI reference model. An open system is a set of protocols that allows any two different systems to communicate regardless of the underlying architecture. Vendor-specific protocol close off communication between unrelated systems.

The purpose of OSI model is to open communication between different system without requiring changes to the logic of the underlying hardware and software. The OSI is not a protocol; it is model for understanding and designing a network architecture that is flexible, robust and open for communication with other systems.

Layered Architecture of OSI

The OSI model has seven layers. Number of layers in any model is derived on following principles.

1. A layer should be created where a different level of abstraction is needed.
2. Each layer should perform a well define function.

3. The function of each layer should be chosen with an eye towards defining internationally standardized protocol
4. The layer boundaries should be chosen to minimize the information flow across the interface.
5. The number of layers should be large enough that distinct function need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy

Advantages of Layered Network Architecture

i. Provide modular approach for any network architecture
ii. A new layer can be introduced any time (if required) without interfering other layers.
iii. A layer can be removed easily if its functions become obsolete.
iv. Modification to a particular layer can be done without interfering other layers.

Disadvantages of Layered Network Architecture

i. Increases the address overhead in data packet as it travels from bottom layer to the top layer.

***Interconnection and Internetworking Services***

The 7 layers of the OSI model can be split into 2 halves, those which provide *interconnection* services and those which provide *internetworking* services. Each layer within the model provides a set of services to the layer above and enhances the service provided by the layer below.

| | | |
|---|---|---|
| 7 | Application Layer | Internetworking Layers |
| 6 | Presentation Layer | |
| 5 | Session Layer | |
| 4 | Transport Layer | Interconnection Layers |
| 3 | Network Layer | |
| 2 | Data Link Layer | |
| 1 | Physical Layer | |

a) The Interconnection Layers

Interconnection group of standards makes up the bottom 4 layers of the OSI model, which are known as the *physical, data link, and network and transport layers.*

The *physical layer* defines the functional, procedural and physical interfaces of communication links between equipment. For example, plug specifications, and pin allocations.

The *data link* layer adds error-checking information and formats data for physical transmission.

The *network layer* provides routing and multiplexing services.

The *transport layer* includes error detection and correction as well as multiplexing. Its basic function is to enhance the quality provided by the network layer below, if this is necessary.

b) The Internetworking Layers

The internetworking group includes the top 3 layers of the OSI model and basically provides the support services for the user applications. They are known as the *session, presentation, and application* layers.

The *session layer* provides the organization, synchronization and timing of the exchange of the data between end systems.

The *presentation layer* is concerned with now the information to be exchanged. This includes resolving character set differences, such as ASCII to EBCDIC, providing text compression and encryption/decryption services.

The *application layer* provides support for the user applications, which wish to exchange information. (I.e. file transfer)

Function Each Layer

1. Physical Layer (repeater, hub, transciever)

The physical layer co-ordinates the functions required to transmit a bit streams over a physical medium. It deals with the mechanical and electrical specifications of the primary connections, such as cables and connectors.

The physical layer is responsible for sending the bits across the network media. It does not define what a bit is or how it is used merely how it's sent. The physical layer is responsible for transmitting and receiving the data. It defines pin assignments for serial connections, determines data synchronization, and defines the entire network's timing base.

Items defined by the physical layer include hubs, simple active hubs, terminators, couplers, cables and cabling, connectors, repeaters, multiplexers, transmitters, receivers, and transceivers. Any item that does not process information but is required for the sending and receiving of data is defined by this layer.

There are several items/ issues addresses by this layer. They are;

i. Network connections types, including multi-point and point-to-point networks.

ii. Network Topologies: How are the networking devices arranged? Including ring, star, bus, and mesh networks.

iii. Analog or Digital signaling.

iv. Bit Synchronization deals with synchronization between sender and receiver (When to send data and when to listen for it).

v. Baseband vs. Broadband transmissions.

vi. Multiplexing (Combining multiple streams of data into one channel). vii. Which modulation technique (bits to pulse)? viii. How long will a bit last?

ix. Bit-serial or parallel transmission?

x. Half- or Full-duplex transmission?

xi. How many pins does the network connector have? xii. How is a connection set up or torn down?

2. Data Link Layer (bridge, switch, NIC)

The main purpose of the data link layer is to deliver data units (group of bits) from one station to the next station (node-to-node) without error. It accepts packets from the network layer and packages the information into data units called frames to be presented to the physical layer for transmission. The data link layer adds header (contains sender's and receiver's address) and trailer (contains control information, such as routing, segmentation, CRC etc.) to the data being sent.

The Data link Layer is also involved in error detection and avoidance using a Cyclic Redundancy Check (CRC) added to the frame that the receiving computer analyses. This second also checks for lost frames and sends requests for re-transmissions of frames that are missing or corrupted at this level.

The most important aspect of the Data Link Layer is in Broadcast networks, where this layer establishes which computer on a network receives the information and which computers relay or ignore the information. It does so by using a Media Access Control (MAC) address, which uniquely identifies each Network Interface Card (NIC). Bridges, Intelligent Hubs, And NICs are all associated with the Data Link Layer.

The Data Link Layer is sub-divided into two layers. This is done because of the two distinct functions that each sub-division provides.

i. Logical Link Control - Generates and maintains links between network devices

ii. Media Access Control - Defines how multiple devices share a media channel

The Logical Link Control provides Service Access Points (Saps) for other computers to make reference to when transporting data to upper layers of the OSI Model.

Media Access Control gives every NIC a unique 12 digit hexadecimal address. These addresses are used by the Logical Link Control to set up connections between NICs. Every MAC address must be unique or they will cause identity crashes on the network. The MAC address is normally set at the factory, and conflicts are rare. But in the case of a conflict, the MAC address is user set-able.

Data link layer is responsible for following:

i. Node to node delivery: Provides reliable transfer of information between two adjacent nodes

ii. Creates frames, or packets, from bits and vice versa

iii. Flow control: It regulates the amount of data that can be transmitted at one time.

iv. Error handling: Provides frame-level error control. Data link layer protocols provide for data recovery, usually by having the entire frame retransmitted.

3. Network Layer (router )

The network layer is responsible for the source to destination delivery of packet across multiple network links. Whereas the data link layer oversees station to station (node to node) delivery. The network layer ensures that each packet gets from its point of origin to its destination successfully and efficiently. For this purpose the network layer provides two reliable services switching and routing.

Switching refers to temporary connection between physical links, resulting in longer links for network transmission; i.e. long distance telephone services.

Routing means selecting the best path for sending a packet from one point to another when more than one path is available. In this case, each packet may take a different route to the destination. Where the packets are collected and resembled into their original order.

In order to provide its services to the data link layer, it must convert the logical network address into physical machine addresses, and vice versa on the receiving computer. This is done so that no relaying, routing, or networking information must be processed by a level higher in the model then this level. Essentially, any function that doesn't provide an environment for executing user programs falls under this layer or lower.

Network layer is responsible for following:

i. Source to destination delivery: moving the packet from its point of origin to its intended destination across multiple network links.

ii. Responsible for Routing and message priority: Deciding which of the multiple paths a packet should take. Routing considerations include speed and cost.

iii. Multiplexing: using a single physical line to carry data between many devices at the same time.

iv. Breaking large packets into smaller chucks when the original packet is bigger than the Data Link is set. Similarly, it re-assembles the packet on the receiving computer into the original-sized packet

v. routing decisions

- Dynamicrouting
- Fixedrouting

vi. Performs congestion control

4. Transport Layer

The transport layer is responsible for source to destination (end to end) delivery of the entire message. Whereas the network layer oversees end to end delivery of individual packets, it does not recognize any relationship between those packets.

Transport layer is responsible for following:

i. Provides reliable end-to-end communication: Confirms the transmission and arrival of all packets of a message at the destination point.

ii. Segmentation and reassembling: The transport layer Header contains sequence, or segmentation number. These numbers enable the transport layer to reassemble the message correctly at the destination and to identify and replace packet lost in transmission.

iii. Hide the details of the network from the session layer

– Example: If we want replace a point-to-point link with a satellite link, this change should not affect the behaviour of the upper layers

5. Session Layer

   The session layer is the network *dialog controller*. It establishes, maintains, and synchronizes the link between communicating devices. It also ensures that each session close appropriately rather than shutting down abruptly and leaving the user hanging.

   Session layer is responsible for following:

   i. Session management: Dividing a session into sub-sessions by the introduction of checkpoint ad separating *long messages* into shorter units, called dialog units appropriate for transmission.

   ii. Synchronization: Deciding in what order to pass the dialog units to the transport layer, and where in the transmission to require conformation from the receiver. iii. Dialog control: Deciding who sends, and when.

   iv. Graceful close: Ensuring that the exchange has been completed appropriately before the session close.

6. Presentation Layer

   The presentation layer ensures interoperability among communicating devices. It is responsible for code conversion (e.g. from ASCII to EBCDIC and vice versa), if required.

   The presentation layer is also responsible for the encryption and decryption of data for security purposes. It also handles the compression and expansion of data when necessary for transmission efficiency.

   Presentation layer is responsible for following:

   i. Translation: changing the format of message (e.g. from ASCII to EBCDIC and vice versa). ii. Encryption/Decryption: handles encryption and decryption of data for security purposes.

   iii. Compression: It also handles the compression and expansion of data when necessary for transmission efficiency.

   iv. Security: validates passwords and log-in codes.

7. Application Layer (PC)

   The application layer enables the user, whether human or software, to access the network. It provides user interface and support for services such as electronic mail, remote file access and transfer.

   Presentation layer is responsible for following:

   i. Mail services: provides the basis for electronic mail forwarding and storage.

   ii. Directory services: Provides distributed database sources and access for global information about various object and services.

   iii. File access, transfer, and management: Allows a user at a remote computer to access files in another host (to make changes or read data); to retrieve files from a remote computer for use in the local computer.

**The OSI Network Layer Service Primitives**

The network layer service is defined by a set of primitives - these primitives look very like programming language procedures. Because the network layer must provide two

types of service, namely connection-oriented and connectionless, there are two sets of primitives.

**Primitives for the Connection-Oriented service**
With this service the primitives can be divided into 4 groups, depending on their function:

i. Making the connection - CONNECT
ii. Closing the connection - DISCONNECT
iii. Sending information (ie using the connection) - DATA, DATA-ACKNOWLEDGE, EXPEDITED-DATA. iv. Resetting the connection - RESET.

Basically, you make a connection and close a connection by using the CONNECT and

DISCONNECT calls. Data is sent using DATA, DATA-ACKNOWLEDGE, and EXPEDITED-

DATA (for those special expedited data transmissions}. If something goes wrong, then the connection can be reset, using the RESET call.

**Primitives for the Connectionless service**
These primitives are divided into two groups:

i. Send a packet of data - UNITDATA
ii. Enquire into the performance of the network - FACILITY, REPORT.

Packets are sent using UNITDATA. FACILITY lets you inquire to the network about things like average delivery statistics and the like. REPORT is used by the network to tell the host if there is a problem with the network, for example, if a machine has gone down.

| | layer | Function | Protocol | Services |
|---|---|---|---|---|
| 7 | Application Layer | The application layer enables the user, whether human or software, to access the network. It provides user interface and support for services such as electronic mail, remote file access and transfer. | Simple mail transfer protocol(SMTP)File transfer protocol (FTP) | The Internetworking Layers |
| 6 | Presentation Layer | Is concerned with now the information to be exchanged. The presentation layer ensures interoperability among communicating devices. It is responsible for code conversion (e.g. from ASCII to EBCDIC and vice versa), if required. The presentation layer is also responsible for the encryption and decryption of data for security purposes. It also handles the compression and expansion of data when necessary for transmission efficiency. | | |
| 5 | Session Layer | The session layer is the network *dialog controller.* It establishes, maintains, and synchronizes the link between communicating devices. It also ensures that each session close appropriately rather than shutting down abruptly and leaving the user hanging. It | | |

| | | | | |
|---|---|---|---|---|
| | | provides organization, synchronization and timing of the exchange of the data between end systems. | | |
| 4 | Transport Layer | The transport layer is responsible for source to destination (end to end) delivery of the entire message to ensure reliability (Manages data transfer over a network to ensure reliability) | Transmission control protocol (TCP), Sequential packet exchange (SPX), NetBEUI, Apple transaction protocol (ATP) | The Interconnection Layers |
| 3 | Network Layer | The network layer provides addressing, routing and multiplexing services. It ensures that each packet gets from its point of origin to its destination successfully and efficiently | Internet protocol (IP) Internet-work packets exchange | |
| 2 | Data Link Layer | Data link layer adds error-checking information and formats data for physical transmission. | | |
| 1 | Physical Layer | The physical layer co-ordinates the functions required to transmit a bit streams over a physical medium. It deals with the mechanical and electrical specifications of the primary connections, such as cables and connectors. | | |

## TCP/IP MODEL

The TCP/IP protocol suite refers to several separate protocols that computers use to transfer data across the Internet.

TCP/IP is a two-layer program.

- ✓ The ***higher layer,*** Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message.
- ✓ The ***lower layer***, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination. Listed below are four of the most commonly used TCP/IP protocols,

The TCP/IP suite of protocols is the set of protocols used to communicate across the internet.

Components of TCP/IP

- IP - The Internet Protocol is a network layer protocol that moves data between host computers.
- TCP - The Transport Control Protocol is a transport layer protocol that moves multiple packet data between applications.
- UDP - The User Datagram Protocol is a transport layer protocol like TCP but is less complex and reliable than TCP.
- ICMP - The Internet Control Message Protocol carries network error messages and other network software requirements.

**OSI comparision with TCP/IP Protocol Stack**

| OSI # | OSI Layer Name | TCP/IP # | TCP/IP Layer Name | Encapsulation Units | TCP/IP Protocols |
|---|---|---|---|---|---|
| 7 | Application | 4 | Application | data | FTP, HTTP, POP3, IMAP, telnet, SMTP, DNS, TFTP |
| 6 | Presentation | | | data | |
| 5 | Session | | | data | |
| 4 | Transport | 3 | Transport | segments | TCP, UDP |
| 3 | Network | 2 | Internet | packets | IP |
| 2 | Data Link | 1 | Network Access | frames | |
| 1 | Physical | | | bits | |

The TCP/IP model, similar to the OSI model, is comprised of layers. The OSI has seven layers and the TCP/IP model has four or five layers depending on different preferences. Some people use the Application, Transport, Internet and Network Access layers. Others split the Network Access layer into the Physical and Data Link components.

LAYER 4 – APPLICATION

This layer is comparable to the application, presentation, and session layers of the OSI model all combined into one. It provides a way for applications to have ***access to network services***. This layer also contains the high level protocols. The main issue with this layer is the ability to use both TCP and UDP protocols. For example TFTP uses UDP because usually on a LAN the physical links are short enough to ensure quick and reliable packet delivery without many errors. SMTP instead uses TCP because of the error checking capabilities. Since we consider our email important information we would like to ensure a safe delivery.

LAYER 3 - TRANSPORT

This layer acts as the delivery service used by the application layer. Again the two protocols used are TCP and UDP. The choice is made based on the application's transmission reliability requirements. The transport layer also ***handles all error detection and recovery.*** It uses checksums, acknowledgements, and timeouts to control transmissions and end to end

verification. Unlike the OSI model, TCP/IP treats reliability as an end-to-end problem.

LAYER 2 – INTERNET

The routing and delivery of data is the responsibility of this layer and is the key component of this architecture. It allows communication across networks of the same and different types and carries out translations to deal with dissimilar data addressing schemes. It inject packets into any network and deliver them to the destination independently to one another. Because the path through the network is not predetermined, the packets may be received out of order. The upper layers are responsible for the reordering of the data. This layer can be compared to the network layer of the OSI model. IP and ARP are the major protocols used at this layer.

LAYER 1 - NETWORK ACCESS

This a combination of the Data Link and Physical layers of the OSI model which consists of the actual hardware. This includes wires, network interface cards, etc. Other related details within this layer are connectors, signal strength, and wavelength along with various others. It will use the required LAN operating algorithms, such as Carrier Sense Multiple Access with Collision Detect (CMSA/CD) or IBM Token Passing etc. and is responsible for placing the data within a frame. The frame format is dependent on the system being used, for example Ethernet LAN, Frame relay, etc. The frame is the package that holds the data, in the same way as an envelope holds a letter. The frame holds the hardware address of the host and checking algorithms for data integrity. This layer has actually not been specified in details because it depends on which technology is being used such as Ethernet. So freedom is given to this layer as far as implementation is concerned.

***Five major features that have led to the popularity of TCP/IP in networking***

There are numerous reasons for the increased popularity of TCP/IP; some of these include:

- TCP/IP is an industry standard protocol
- It is a routable protocol suite
- It is provided on almost all network operating systems, and therefore allows connectivity between dissimilar systems (for instance, from a UNIX computer to a Windows NT computer)
- It provides connectivity with the Internet
- The protocols are in the public domain and are freely available, which makes it a popular choice for software companies. There are no restrictions on its use and no royalties to pay
- It is a well-designed protocol
- It is an open standard where no single vendor has any control over the protocol and anyone is allowed to use it and develop applications based on it

**The function of each protocol in the TCP/IP protocol stack**

The TCP/IP suite of protocols is the set of protocols used to communicate across the internet. It is also widely used on many organizational networks due to its flexiblity and wide array of functionality provided. The following are the protocols provided by TCP/IP

i. The Internet Protocol (IP) is a routable protocol that handles IP addressing, routing, and the fragmentation and reassembly of packets.

ii. The Address Resolution Protocol (ARP) used to convert an IP address to a physical address. Handles resolution of an Internet layer address to a Network Interface layer address, such as a hardware address.

iii. The Internet Control Message Protocol (ICMP) handles providing diagnostic functions and reporting errors due to the unsuccessful delivery of IP packets.

iv. The Internet Group Management Protocol (IGMP) handles management of IP multicast group membership.

v. HTTP (Hypertext Transfer Protocol) HTTP is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a Uniform Resource Locator (URL) in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

HTTP is called a *stateless* protocol because each command is executed independently, without any knowledge of the commands that came before it. This is the main reason that it is difficult to implement Web sites that react intelligently to user input. This shortcoming of HTTP is being addressed in a number of new technologies, including ActiveX, Java, JavaScript and cookies.

HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet).

vi. TCP (Transmission Control Protocol)

Enables two to establish a connection and exchange streams of data. TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

For example, when an HTML file is sent to you from a Web server, the Transmission Control Protocol (TCP) program layer in that server divides the file into one or more packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end (the client program in your computer), TCP reassembles the

individual packets and waits until they have arrived to forward them to you as a single file.

TCP is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. In the Open Systems Interconnection (OSI) communication model, TCP is in layer 4, the Transport Layer.

vii. TFTP (Trivial File Transfer Protocol) - Simplified version of the FTP protocol which has no security features.

viii. SMTP (Simple Mail Transfer Protocol) - Protocol used to send email messages between servers.

*Differences between TCP and UDP*

The following table is a summary of the differences between TCP and UDP

| | Transmission Control Protocol (TCP) | User Datagram Protocol (UDP) |
|---|---|---|
| 1 | Transmission Control Protocol (TCP) is a connection oriented protocol, which means the devices should open a connection before transmitting data and should close the connection gracefully after transmitting the data. | User Datagram Protocol (UDP) is *Datagram oriented protocol* with no overhead for opening, maintaining, and closing a connection |
| 2 | It assure reliable delivery of data to the destination | May *not be very reliable* It is efficient for broadcast/multicast transmission |
| 3 | It provides *extensive error checking* mechanisms such as flow control and acknowledgment of data. | It has only the *basic error checking* mechanism using checksums. |
| 4 | *Sequencing of data* is a feature of Transmission Control Protocol (TCP). | There is *no sequencing of data* in User Datagram protocol (UDP) |
| 5 | *Delivery* of data is *guaranteed* | The *delivery* of data can*not* be *guaranteed* |
| 6 | It is comparatively *slow* because of these extensive error checking mechanisms | It is *faster*, simpler and more efficient than TCP. However, User Datagram protocol (UDP) it is less robust than TCP |
| 7 | Multiplexing and Demultiplexing is possible in Transmission Control Protocol (TCP) using TCP port numbers. | Multiplexing and Demultiplexing is possible in User Datagram Protcol (UDP) using UDP port numbers |
| 8 | *Retransmission* of lost packets is *possible* in Transmission Control Protocol (TCP). | There is *no retransmission* of lost packets in User Datagram Protcol (UDP |

Similarities include:

i. Both have layers.
ii. Both have application layers, though they include very different services.
iii. Both have comparable transport and network layers.
iv. Both models need to be known by networking professionals.
v. Both assume packets are switched.
This means that individual packets may take different paths to reach the same destination. This is contrasted with circuit-switched networks where all the packets take the same path.

Differences between TCP/IP with OSI include:

i. TCP/IP combines the presentation and session layer issues into its application layer. ii. TCP/IP combines the OSI data link and physical layers into the network access layer. iii. TCP/IP appears simpler because it has fewer layers.

Testing a TCP/IP configuration by using the ping command

i. To quickly obtain the TCP/IP configuration of a computer, open Command Prompt, and then type ipconfig. From the display of the ipconfig command, ensure that the network adapter for the TCP/IP configuration you are testing is not in a Media disconnected state.

ii. At the command prompt, ping the loopback address by typing ping 127.0.0.1.

iii. Ping the IP address of the computer.

iv. Ping the IP address of the default gateway.

v. If the ping command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.

vi. Ping the IP address of a remote host (a host that is on a different subnet).

If the ping command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all of the gateways (routers) between this computer and the remote host are operational.

vii. Ping the IP address of the DNS server.

If the ping command fails, verify that the DNS server IP address is correct, that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

Notes

- To open a command prompt, click Start, point to All programs, point to Accessories, and then click Command prompt.

- The **ipconfig** command is the command-line equivalent to the winipcfg command, which is available in Windows 95, Windows 98, Windows 98 Second Edition, and Windows Millennium Edition. Computers running Windows XP or Windows Server 2003 operating systems do not include a graphical equivalent of the winipcfg command, however, you can get equivalent functionality for viewing and renewing an IP address by opening Network Connections, right-clicking a network connection, clicking Status, and then clicking the Support tab.

  If the **ipconfig** command displays Media disconnected, the network cable is not plugged in to the network adapter.

- If the **ping** command is not found or the command fails, you can use Event Viewer to check the system log and look for problems reported by Setup or the Internet Protocol (TCP/IP) service.

- The ping command uses Internet Control Message Protocol (ICMP) Echo Request and Echo Reply messages. Packet filtering policies on routers, firewalls, or other types of security gateways might prevent the forwarding of this traffic.

**Testing TCP/IP connectivity by using the net view command**

Open Command Prompt, and then type net view \\ComputerName. The net view command lists the file and print shares by establishing a temporary connection. If there are no file or print shares on the specified computer, the net view command displays a "There are no entries in the list" message.

If the net view command fails with a "System error 53 has occurred" message, verify that Computer Name is correct, that the computer is operational, and that all of the gateways (routers) between this computer and the computer are operational.

If the net view command fails with a "System error 5 has occurred. Access is denied." message, verify that you are logged on using an account that has permission to view the shares on the remote computer.

To further troubleshoot this connectivity problem, do the following:

- Use the ping command to ping Computer Name.

  If the ping command fails with an "Unable to resolve target system name" message, then ComputerName cannot be resolved to its IP address.

- Use the net view command and the IP address of the computer, as follows:

  net view \\IPAddress

  If the net view command succeeds, then ComputerName is being resolved to the wrong IP address.

If the net view command fails with a "System error 53 has occurred" message, the remote computer might not be running the File and Printer Sharing for Microsoft Networks service.

Standards Making Organizations

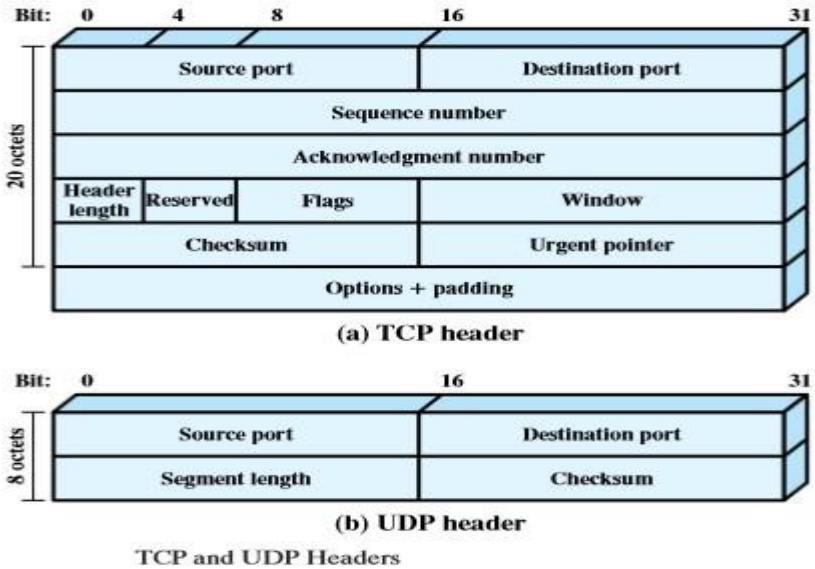
i. ISO = International Standards Organization
ii. ITU = International Teletraffic Union (formerly CCITT)
iii. ANSI = American National Standards Institute
iv. IEEE = Institute of Electrical and Electronic Engineers
v. IETF = Internet Engineering Task Force
vi. ATM Forum = ATM standards-making body

**TCP Header**

The Transmission Control Protocol (TCP) header is the first 24 bytes of a TCP segment that contains the parameters and state of an end-to-end TCP socket. The TCP header is used to track the state of communication between two TCP endpoints. Since TCP segments are inserted (encapsulated) in the payload of the IP packet the TCP header immediately follows the IP header during transmission. TCP does not need to keep track of which systems are communicating, it only needs to track which end to end sockets are currently open. Internet Protocol handles the logical addressing, routing and host-to-host connectivity.

TCP uses port numbers on each side of the connection to track the connection endpoints, state bits such as SYN, ACK, RST, FIN, sequence numbers and acknowledgement numbers to track the communication at each step in transmission.

An example of a TCP header is shown below.




TCP and UDP Headers

**Source port:** 16 Bit number which identifies the Source Port number (Sending Computer's TCP Port).

**Destination port:** 16 Bit number which identifies the Destination Port number (Receiving Port).

**Sequence number:** 32 Bit number used for byte level numbering of TCP segments. If you are using TCP, each byte of data is assigned a sequence number. If SYN flag is set (during the initial three way handshake connection initiation), then this is the initial sequence number. The sequence number of the actual first data byte will then be this sequence number plus 1. For example, let the first byte of data by a device in a particular TCP header will have its sequence number in this field 50000. If this packet has 500 bytes of data in it, then the next packet sent by this device will have the sequence number of 50000 + 500 + 1 = 50501.

**Acknowledgment Number:** 32 Bit number field which indicates the next sequence number that the sending device is expecting from the other device.

**Header Length:** 4 Bit field which shows the number of 32 Bit words in the header. Also known as the Data Offset field. The minimum size header is 5 words (binary pattern is 0101).

**Reserved:** Always set to 0 (Size 6 bits).

**Control Bit Flags:** We have seen before that TCP is a Connection Oriented Protocol. The meaning of Connection Oriented Protocol is that, before any data can be transmitted, a reliable connection must be obtained and acknowledged. Control Bits govern the entire process of connection establishment, data transmissions and connection termination. The control bits are listed as follows: They are:

URG: Urgent Pointer.

ACK: Acknowledgement.

PSH: This flag means Push function. Using this flag, TCP allows a sending application to specify that the data must be pushed immediately. When an application requests the TCP to push data, the TCP should send the data that has accumulated without waiting to fill the segment.

RST: Reset the connection. The RST bit is used to RESET the TCP connection due to unrecoverable errors. When an RST is received in a TCP segment, the receiver must respond by immediately terminating the connection. A RESET causes both sides immediately to release the connection and all its resources. As a result, transfer of data ceases in both directions, which can result in loss of data that is in transit. A TCP RST indicates an abnormal termination of the connection.

SYN: This flag means synchronize sequence numbers. Source is beginning a new counting sequence. In other words, the TCP segment contains the sequence number of the first sent byte (ISN).

FIN: No more data from the sender. Receiving a TCP segment with the FIN flag does not mean that transferring data in the opposite direction is not possible. Because TCP is a fully duplex connection, the FIN flag will

cause the closing of connection only in one direction. To close a TCP connection gracefully, applications use the FIN flag.

**Window:** indicates the size of the receive window, which specifies the number of bytes beyond the sequence number in the acknowledgment field that the receiver is currently willing to receive.

**Checksum:** The 16-bit checksum field is used for error-checking of the header and data.

**Urgent Pointer:** Shows the end of the urgent data so that interrupted data streams can continue. When the URG bit is set, the data is given priority over other data streams (Size 16 bits).

In this lesson, you have learned different fields in Transmission Control Protocol (TCP) Segment Header and the use of these fields. The fields in Transmission Control Protocol (TCP) Segment Header are Source Port, Destination Port, Sequence Number, Acknowledgement Number, Header Length, Flags, Window Size, TCP Checksum and Urgent Pointer. Click "Next" to continue.

# CHAPTER FIVE

# DATA COMMUNICATION SOFTWARE

Data Communication Software

Description of Communication Software

The basic concept behind data communication and network is for the two or more computer or electronic devices to see each other and share resources. For that to be archived there must be a program or software responsible for the communication to take place. The software in this case is refers to as data communication software. Data communication Software is basically a computer program that.

1. It is a computer program required on DTE (PC) to bridge the gap and interpret the bits/bytes that are transmitted via the communication media through the interface.
2. The Core of Data Communication is Communication Software without software, Data communication is incomplete.
3. Communication Software is responsible for controlling data formatting, data transmission, and total communication control.
4. It May completely resides on central PC or part of it may be located on the front end communication PC, a concentrator, remote concentrator or in intelligent terminals.

## 4.1.2. Significance of Data Communication Software

Major significance of data Communication software are:

- **i.** Defines the communication parameters like communication speed, error rate, bandwidth, protocols, etc.
- **ii.** Controls the user accessibility to information. It means how a user can access the information and how information shall be presented to user.
- **iii.** It controls the optimal configuration of communication hardware and makes the effective utilization of network resources.

## 4.1.3. Function of Communication software

General functions of communication software are:

- **i.** Establish logical data paths.
- **ii.** Check accuracy of each transmission, and arrange retransmission if necessary (e.g. TCP/IP).
- **iii.** Exercise flow control to avoid congestion and loss of data.
- **iv.** Maintaining the statistics on traffic volumes over all links, and on network reliability
- **v.** Transmission initiation and termination is done by communication software when user prompts it. In case of modem, modem initialization and making it ready function come under this category. vi. Establishment of logical connections over physical line like dialing the number on phone lines.
- **vii.** Message Assembly and De-assembly.
- **viii.** Data Transmission & receipt. It means Modulation of digital data into analog and vice versa by modem).
- **ix.** Code conversion is done by communication software where it format the data

**x.** Error Detection is also done by it. It checks for lost bits and other error introduced while transmitting.

**xi.** Data Editing xii. Control Character Recognition xiii. Data Delivery and output. Communication software control the output and delivery of data at the destination)

xiv. Transmission monitoring and maintenance

4.1.4. Categories of Communication Software

Data communication software can be categories into two:

1. Application Software: These are the software that enables end users to perform one task or the other on data communication and network system. For example Email Software - all types for email software‟s which include the following, Broadcast Software - including MP3s, audio recording and call recording software, and Wireless Software - all types of wireless related software‟s
2. System Software: Software that allows you to connect with other computers or mobile devices via text, video or audio formats in either a synchronous or asynchronous manner. They are set of software that enable data communication system to function and meet the require objective of resources sharing and other functionability. Data communication system software can be classified in into development software, and management software e.g. networks traffic analyzer, a ping/traceroute program, firewall etc.

## Communication Protocol

**Description of Communication Protocol**

A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking Igbo cannot be understood by a person who speaks only Yoruba. A communication protocol is a description of the rules that communication devices must follow to communicate with each other. A Protocol is one of the components of a data communications system. Without protocol communication cannot occur. The sending device cannot just send the data and expect the receiving device to receive and further interpret it correctly. Protocol was mentioned briefly in chapter two of this book but discussed fully in this chapter.

Elements of a Protocol

There are three key elements of a protocol:

**a.** Syntax is the structure or format of the data. It is the arrangement of data in a particular order.

**b.** Semantics gives the meaning of each section of bits and indicates the interpretation of each section. It also tells what action/decision is to be taken based on the interpretation.

**c.** Timing tells the sender about the readiness of the receiver to receive the data It tells the sender at what rate the data should be sent to the receiver to avoid overwhelming the receiver.

Transmission Control Protocol (TCP)

TCP/IP is the basic communication protocol for two or more computers or electronic devices (e.g mobile phone) to communicate with one another on a network setup. TCP/IP stands for

Transmission Control Protocol/Internet Protocol. TCP/IP defines how electronic devices (like computers) should be connected to the Internet, and how data should be transmitted between them. TCP/IP is the major protocol in communication network that communication can do without. Inside the TCP/IP standard there are several protocols for handling data communication these are: TCP (Transmission Control Protocol) communication between applications; UDP (User Datagram Protocol) simple communication between applications; IP (Internet Protocol) communication between computers; ICMP (Internet Control Message Protocol) for errors and statistics; DHCP (Dynamic Host Configuration Protocol) for dynamic addressing; and TCP Uses a Fixed Connection.

Transmission Control Protocol: Transmission Control Protocol takes care of the communication between your application software (i.e. your browser) and your network software. TCP is responsible for breaking data down into IP packets before they are sent, and for assembling the packets when they arrive. TCP is for communication between applications. If one application wants to communicate with another via TCP, it sends a communication request. This request must be sent to an exact address. After a "handshake" between the two applications, TCP will set up a "full-duplex" communication between the two applications. The "full-duplex" communication will occupy the communication line between the two computers until it is closed by one of the two applications.

Internet Protocol: Internet Protocol is Connection-Less i.e, it does not occupy the communication line between two computers. The Network Layer protocol for TCP/IP is the Internet Protocol (IP). It uses IP addresses and the subnet mask to determine whether the datagram is on the local or a remote network. If it is on the remote network, the datagram is forwarded to the default gateway which is a router that links to another network. IP keeps track of the number of transverses through each router that the datagram goes through to reach its destination. Each transvers is called a hop. If the hop count exceeds 255 hops, the datagram is removed and the destination considered unreachable. IP reduces the need for network lines. Each line can be used for communication between many different computers at the same time. With IP, messages (or other data) are broken up into small independent "packets" and sent between computers via the Internet. IP is responsible for "routing" each packet to the correct destination.

Special Purpose Protocol

The special purpose protocols are the set of protocols design to perform a single task on communication network system. Some of these protocols and their function are listed below:

i. HTTP - Hyper Text Transfer Protocol: HTTP takes care of the communication between a web server and a web browser. HTTP is used for sending requests from a web client (a browser) to a web server, returning web content (web pages) from the server back to the client. ii. HTTPS - Secure HTTP: HTTPS takes care of secure communication between a web server and a web browser. HTTPS typically handles credit card transactions and other sensitive data. iii. SSL - Secure Sockets Layer: The SSL protocol is used for encryption of data for secure data transmission. iv. MIME - Multi-purpose Internet Mail Extensions: The MIME protocol lets SMTP transmit multimedia files including voice, audio, and binary data across TCP/IP networks.

v. IMAP - Internet Message Access Protocol: IMAP is used for storing and retrieving e-mails. vi. FTP - File Transfer Protocol: FTP takes care of transmission of files between computers. vii. NTP - Network Time Protocol: NTP is used to synchronize the time (the clock) between computers. viii. DHCP - Dynamic Host Configuration Protocol: DHCP is used for allocation of dynamic IP addresses to computers in a network. ix. SNMP - Simple Network Management Protocol: SNMP is used for administration of computer networks.

x. LDAP - Lightweight Directory Access Protocol: LDAP is used for collecting information about users and e-mail addresses from the internet. xi. ICMP - Internet Control Message Protocol: ICMP takes care of error-handling in the network. xii. ARP - Address Resolution Protocol: ARP is used by IP to find the hardware address of a computer network card based on the IP address. xiii. RARP - Reverse Address Resolution Protocol: RARP is used by IP to find the IP address based on the hardware address of a computer network card.

## Review Questions

1. Define communication software
2. What are general functions of communication Software
3. Give examples and function of the following communication Software. i. Broadcast software ii. Messaging software iii. Instant communication Software
4. TCP/IP Protocol is communication software. Yes or NO discuss your answer.
5. What are the elements of communication protocol
6. Compare TCP and IP, hence highlights and gives function of basic protocol for handling data communication
7. Describe the communication between one application and other via TCP/IP
8. What happen when a new domain name is registered together with TCP/IP address
9. Give the full meaning and function of the following protocols i. HTTP ii. SSL iii. MIME iv. BOOTP v. SMTP vi. LDAP

# CHAPTER SIX

# NETWORK SECURITY

## DATA SECURITY

Computer security – involves the safeguards required to control access to information and protect computer hardware and software, personnel and data against hazards to which computer systems are exposed to.

Security control help to ensure high systems standards and performance by protecting against adversities. Some of these hazards include;

- Viruses
- Fire
- Natural disaster
- Sabotage and other environmental problems

Computer and network security addresses four requirements;

i. Confidentiality: Requires that data only be accessible by authorized parties. This type of access includes printing, displaying, and other forms of disclosure, including simply revealing the existence of an object.
ii. Integrity: Requires that only authorized parties can modify data. Modification includes writing, changing, changing status, deleting, and creating.
iii. Availability: Requires that data are available to authorized parties. iv. Authenticity: Requires that a host or service be able to verify the identity of a user.

Computer systems/networks are vulnerable to the following attacks;

i. Interruption

An asset of the system is destroyed or it becomes unavailable. This is an attack on availability such as destruction of hardware, cutting on communication lines, disabling file management system etc.

ii. Interception

An authorized party/person gains access to an asset. This is an attack on confidentiality e.g. wire tapping

iii. Modification

Unauthorized party not only gains access but also tampers with an asset. This is an attack is on integrity e.g. changing values in data files, altering with a program so that it performs differently.

iv. Fabricator

Unauthorized party inserts count fates objects into the system. This is an attack on authenticity e.g. insertion of messages in the network or addition of records to a file.

Attacks can also be classified as either passive or active.

***Passive attacks***

Means monitoring transmissions. The goal of the opponent is to obtain information that is being transmitted.

There are two main types of passive attacks;

- Release of message contents
- Traffic analysis

*Release message content* is easily understood in the following narrative.

A telephone conversation, an electric main message, transferred file conversation may contain sensitive or confidential information. We would like to prevent from learning the contents of these transmissions.

*Traffic analysis* is in the form that, suppose that one need away masking the contents of the message they cannot extract the information from it. The common technique for masking contents is encrypt cal. If we had encryption in place opponent may still be able to observe the pattern of the message. The opponent would determine the location and identify of the communicating hosts and could observe the frequency and length of message being exchanged. This information may be useful in guessing the nature of communication that was taking place. Passive attacks are difficult to detect because they do not involve any alteration of the data. However, it's important to prevent the success of their attacks. Passive attacks deals with prevention rather than detection.

***Active attacks***

These attacks involve some modification of the data stream or the creation of false streams. It is subdivided into four categories;

i. Masquerade

Takes place when one entity pretends to be different entity. It's usually one of the other forms of active attacks. E.g. authentication – authentication sequences can be captured and displayed after a valid authentication sequence has taken place thus enabling an authorized with few privileges to obtain extra privileges by impersonating an entity with those privileges

ii. Relay

Involves passive capture of the data unity and its subsequent transmission to produce unauthorized effect. E.g. ―allow Jane to read confidential file account ― is modified to mean ―allow John read confidential file accounts‖.

iii. The denial of service

It prevents or inhibits the normal use or management of communication facilities. This attack may have specific target e.g. an entity may suppress all messages directed to a particular destination. Another form is disruption of entire network either by disabling the network or by overloading it with messages so as to degrade/reduce its performance.

Measures to prevent attacks

i. Encryption

A technique which involves changing data which is difficult to understand before transmitting. As the receiving end, the encrypted data is decrypted to convert it to its normal form.

ii. Digital signature

It is a security code added to the message. It provides an electronic means of guaranteeing authenticity of the sending party and assurance that the encrypted documents have not been altered during transmissions hence it ensures message integrity.

iii. Authentication

It is a process that ensures that users are who they claim to be. The overall aim is to ensure that users attempting to gain access to computer system are actually the people authorized to do so.

iv. Firewalls

Used to prevent viruses from entering into your system or into your computer Some internet business concerned are:

- Fraud
- Hacking
- Interception of information
- Privacy violation

## COMPUTER SECURITY

### Threats To Data Security

There are many different threats to computer systems and the data stored on them. These threats increased considerably when computers started to be networked but with the Internet, they have become one of the most important considerations in managing a computer system.

**i. Hackers**

Unless they are protected, computer systems are vulnerable to anyone who wants to edit, copy or delete files without the owner's permission. Such individuals are usually called hackers.

### ii. Malware

Malware, short for malicious software, is software designed to gain access to a computer system without the owner's consent. The expression is a general term used by the computer industry to mean a variety of forms of hostile, intrusive, or annoying software. These things are sometimes, incorrectly, referred to as a computer virus. Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware is not the same as defective software, that is, software that has a legitimate purpose but contains harmful bugs.

### iii. Virus

A computer virus is a piece of software that is designed to disrupt or stop the normal working of a computer. They are called viruses because like a biological virus, they are passed on from one infected machine to another. Downloading software from the Internet, attachments to emails or using USB memory sticks are the most common ways of a virus infecting your computer.

### iv. Worms

A computer worm is a self-replicating program. It uses a computer network to send copies of itself to computers on the network and it may do so without any user intervention. It is able to do this because of security weaknesses on the target computer. Unlike a virus it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, if only by consuming bandwidth whereas viruses almost always corrupt or modify files on a targeted computer.

### v. Trojan Horses

Trojan horses are designed to allow a hacker remote access to a target computer system. Once a Trojan horse has been installed on a target computer system, it is possible for a hacker to access it remotely and perform various operations. The operations that a hacker can perform are limited by user privileges on the target computer system and the design of the Trojan horse.

### vi. Spyware

Spyware is a type of malware that is installed on computer and collects little bits of information at a time about users without their knowledge. It can be very difficult for a user to tell if spyware is present on a computer. Sometimes, however, spywares such as key loggers are installed by a company, or on a public computer such as in a library in order to secretly monitor other users.

While the term spyware suggests that software that secretly monitors the user's computing, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, such as Internet surfing habits and sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software and redirecting Web browser activity. Spyware is known to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet or functionality of other programs. Spyware is also known more formally as privacy-invasive software.

### vii. Crimeware

Crimeware is a class of malware designed specifically to automate cybercrime. Its purpose is to carry out identity theft. It is most often targeted at financial services companies such as banks online retailers etc. for the purpose of taking funds from those accounts or making unauthorized transactions to benefit the thief controlling the crimeware.

### viii. SPAM

Spam is the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam web search engine spam and social networking spam for example.


### ix. Phishing

Phishing is an e-mail fraud method in which the criminal sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy Web sites. Web sites that are frequently spoofed by phishers include PayPal, eBay, MSN and Yahoo. A phishing

expedition, like the fishing expedition it's named after, is a speculative venture: the phisher puts the lure hoping to fool at least a few of the prey that encounter it, take the bait.
The criminal could then use the information to take money from the persons account for example.

**x. Adware**

Adware, or advertising-supported software, is any software package that automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Common forms of this type of malware are on websites where popup windows appear when you land on the website. Some types of adware are also spyware.

**User Precautions That Can Be Taken**

As a user, there are a number of solutions that can be taken to make your data more secure from the threats outlined in the previous section.

Some of these require software to be installed and used. Others are a feature of the design of the computers themselves and the buildings where they are kept.

Users should be very careful when using the Internet and email. In particular:

i. Never open an email attachment unless you are certain what the file contains. This is especially true for emails received from someone you do not know.

ii. Be careful when visiting websites especially if they are going to download a file to your computer.

iii. Never give out your personal details unless you are absolutely certain that the request is from a reliable source.

iv. Always make sure that antivirus and other protection software is up to date and turned on.

v. If you must leave your computer unattended whilst you are logged on make sure that the screen is ―locked‖ so that no one can use it.

vi. When shopping on the Internet make sure that you use sites where the data is encrypted when you send personal or financial details. You can tell this from the lock that appears in the bottom of the browser window.

## How to deal with security challenges

### 1. Physical Security

The software restrictions outlined on other pages in this site are necessary and relevant but an equally important are the physical security measures taken to prevent unauthorized users from gaining access to the computer.

**Examples of physical security include:**

i. Locating computers away from public use. In a doctors surgery for example behind a screen or in an office where patients cannot have access to the machine.
ii. In an office limiting the number of computers on the ground floor to minimize the risk of theft.
iii. Securing the files servers and network systems in a locked room where few people are likely to know of its existence. These systems also need to protection from environmental issues that could cause the system to fail e.g. extreme heat or cold, flooding and excessive humidity.
iv. Fitting door locks and window grills to prevent theft.

### 2. Usernames and Passwords

A username is a computer identity given to people in an organisation so that they can use the computer system. It uniquely identifies the user to the computer system so that only their files and other shared resources that the systems administrator has permitted, can be seen.

Passwords are used to make the system secure and prevent access from unauthorised users.

Passwords should only be known to the account holder and changed regularly. This helps to keep them secret. Once someone other than the account holder knows a password, it can be changed and the genuine user of the account can be denied access.

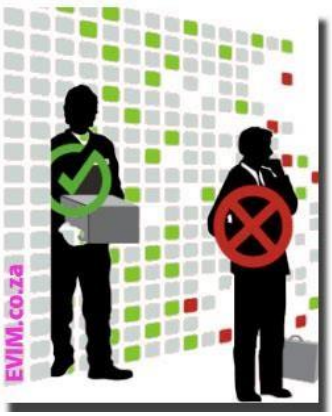
**Basic rules for keeping a password secure are:**

i. Always use a password that is hard to guess.
ii. Longer passwords are more secure than shorter ones.
iii. Strong passwords have random characters and include numbers and non-alphabetic characters

iv. Do not use the same password for all the computer systems and websites that you use
v. Never write your passwords down
vi. Change them regularly

### 3. Access Rights

When a user logs on to a computer system, they will only be allowed have access to certain files and perform certain actions.

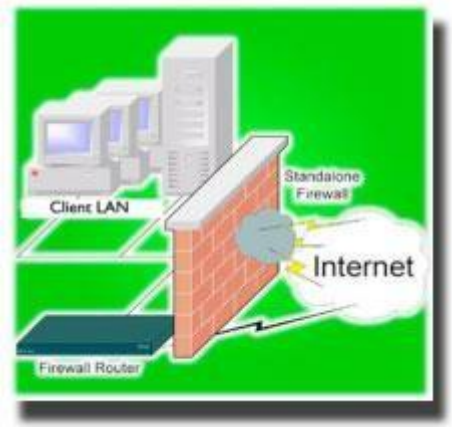



For example, at school you are not permitted to use Google images. Your access rights manage this restriction.

In business, similar restrictions will apply general users in the sales department will not be allowed to see staff details maintained by the personnel department.

In this way the security of the computer system is improved by only allowing them access to the data and resources that they need. **4.**

**Firewalls**




A firewall is a part of a computer network that is designed to block unauthorized access from people outside the organization while permitting authorized communications inside the organization to the outside world Firewalls can be implemented in either hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

### 5. Anti-Virus Software

Anti Malware is a more general term given to this type of software. However, viruses are the biggest threat and these days, anti-virus software will include protection from adware, spyware, viruses, anti-spam and also include a firewall.

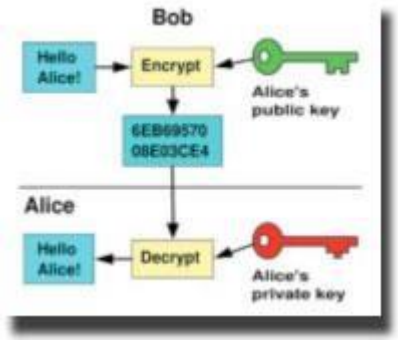
**How does Anti-Virus software work?**

There are two ways protection is provided:

When the software is installed, the administrator will decide what events are to be monitored. For example downloading files from the Internet opening a memory stick etc. The software then scans the files to see if any of the contents match signatures of viruses stored in its database. If they do, they will be blocked from use or the virus element deleted. The user will also be alerted that a virus has been found As new viruses are found, updates will be made available to the anti-virus program so it is important that is kept up to date, otherwise known viruses could get through and infect the computer.

The second method of protection is when unusual activity is detected. For example a program that would not normally download a file from the Internet begins to do so. If this activity matches a rule in the database about a known virus, the transfer will be blocked.
Anti-spyware works in a similar way. Details of the spyware program are stored in a database and this is used to check all incoming files to see if they contain spyware. If they do the file is blocked.
Anti-spam software works on storing known spam addresses and matching these to incoming emails. When a match is found, the email is diverted to a special inbox where the messages get deleted after a certain period.

### 6. Encryption




This is used to protect data whilst it is being transmitted over the Internet or used to protect important data stored on a computer. Un-encrypted data is very easy for people to read especially when it is being transmitted over telephones lines that are used by most people to connect to the Internet.

Encryption works like this:

- Each character is scrambled according to a secret code
- The coded character is then stored or transmitted in place of the original character
- When the data is needed it is converted back using the same encryption key used to create it.

When encrypted data is transmitted the receiving computer has to know what the encryption key is so that it can be converted back.

If data is stored in an encrypted form, the user has to enter a password before the computer will de-crypt the data. This is a good way of protecting data on portable devices such as PDAs and smartphones.

Encryption is used as a way of protecting personal information and payment data on many websites these days. Websites using secure (encrypted) data transmission have web addresses that begin with HTTPS and show a padlock in the browser window

Encryption Method

The universal technique for providing confidentiality for transmitted data is symmetric encryption. A symmetric encryption scheme has five components.

**a.** Plaintext: This is the original message or data that is fed into the algorithm as input.
**b.** Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.
**c.** Secret key: The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
**d.** Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.
**e.** Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Cryptographic Algorithms

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are (Figure 33):

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information

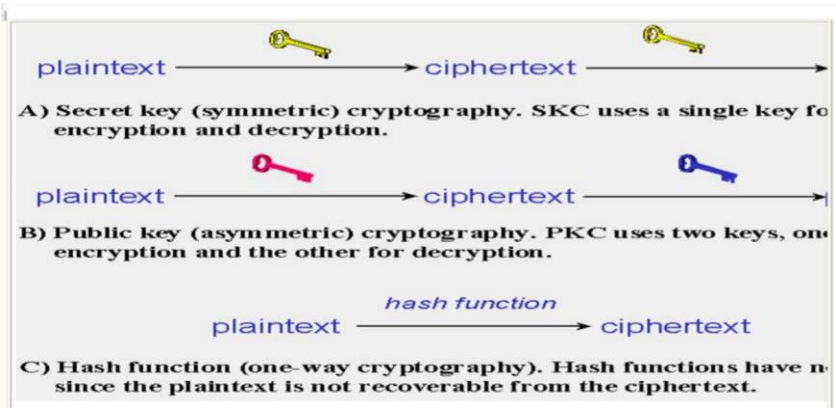



Figure 33: Cryptographic Algorithms

Secret Key Cryptography

With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 33A, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or ruleset) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is socalled because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher.

Stream ciphers come in several flavors but two are worth mentioning here. Self-synchronizing stream ciphers calculate each bit in the keystream as a function of the previous n bits in the keystream. It is termed "self-synchronizing" because the decryption process can stay synchronized with the encryption process merely by knowing how far into the n-bit keystream it is. One problem is error propagation; a garbled bit in transmission will result in n garbled bits at the receiving side. Synchronous stream ciphers generate the keystream in a fashion independent of the message stream but by using the same keystream generation function at sender and receiver. While stream ciphers do not propagate transmission errors, they are, by their nature, periodic so that the keystream will eventually repeat.

Block ciphers can operate in one of several modes; the following four are the most important:

- Electronic Codebook (ECB) mode is the simplest, most obvious application: the secret key is used to encrypt the plaintext block to form a ciphertext block. Two identical plaintext blocks, then, will always generate the same ciphertext block. Although this is the most common mode of block ciphers, it is susceptible to a variety of bruteforce attacks.
- Cipher Block Chaining (CBC) mode adds a feedback mechanism to the encryption scheme. In CBC, the plaintext is exclusivelyORed (XORed) with the previous ciphertext block prior to encryption. In this mode, two identical blocks of plaintext never encrypt to the same ciphertext.
- Cipher Feedback (CFB) mode is a block cipher implementation as a self-synchronizing stream cipher. CFB mode allows data to be encrypted in units smaller than the block size, which might be useful in some applications such as encrypting interactive terminal input. If we were using 1-byte CFB mode, for example, each incoming character is placed into a shift register the same size as the block, encrypted, and the block transmitted. At the receiving side, the ciphertext is decrypted and the extra bits in the block (i.e., everything above and beyond the one byte) are discarded.
- Output Feedback (OFB) mode is a block cipher implementation conceptually similar to a synchronous stream cipher. OFB prevents the same plaintext block from generating the same ciphertext block by using an internal feedback mechanism that is independent of both the plaintext and ciphertext bitstreams.

Public-Key Cryptography

PKC depends upon the existence of so-called one-way functions, or mathematical functions that are easy to computer whereas their inverse function is relatively difficult to compute. In PKC, one of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party. It is straight forward to send messages under this scheme. Suppose Yekini wants to send Adebari a message. Yekini encrypts some information using Adebari‟s ublic key; Adebari decrypts the ciphertext using his private key. This method could be also used to prove who sent a message; Yekini, for example, could encrypt some plaintext with his private key; when Adebari decrypts using Yekini‟s public key, he knows that Yekini sent the message and Yekini cannot deny having sent the message (non-repudiation).

Hash Functions

Hash functions, also called message digests and one-way encryption, and are algorithms that, in some sense, use no key Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

**Why Three Encryption Techniques?**

So, why are there so many different types of cryptographic schemes? Why can't we do everything we need with just one? The answer is that each scheme is optimized for some specific application(s).

- Hash functions, for example, are well-suited for ensuring data integrity because any change made to the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender. Since it is highly unlikely that two different messages will yield the same hash value, data integrity is ensured to a high degree of confidence. o Secret key cryptography, on the other hand, is ideally suited to encrypting messages, thus providing privacy and confidentiality. The sender can generate a session key on a per-message basis to encrypt the message; the receiver, of course, needs the same session key to decrypt the message.
- Public-key cryptography asymmetric schemes can also be used for non-repudiation and user authentication; if the receiver can obtain the session key encrypted with the sender's private key, then only this sender could have sent the message. Public-key cryptography could, theoretically, also be used to encrypt messages although this is rarely done because secret-key cryptography operates about 1000 times faster than public-key cryptography.

Figure 34 puts all of this together and shows how a hybrid cryptographic scheme combines all of these functions to form a secure transmission comprising digital signature and digital envelope. In this example, the sender of the message is Yekini and the receiver is Bello.

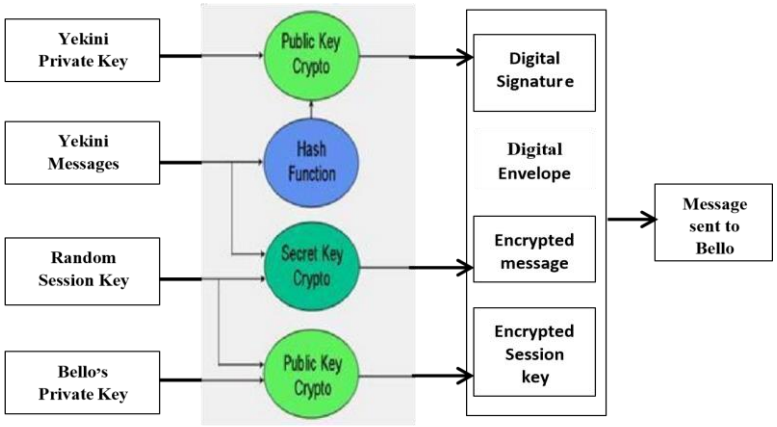



**Figure 34 : hybrid cryptographic scheme**

A digital envelope comprises an encrypted message and an encrypted session key. Yekini uses secret key cryptography to encrypt his message using the session key, which he generates at random with each session. Yekini then encrypts the session key using Bello's public key. The

encrypted message and encrypted session key together form the digital envelope. Upon receipt, Bello recovers the session secret key using his private key and then decrypts the encrypted message.

The digital signature is formed in two steps. First, Yekini computes the hash value of her message; next, he encrypts the hash value with his private key. Upon receipt of the digital signature, Bello recovers the hash value calculated by Yekini by decrypting the digital signature with Yekini's public key. Bello can then apply the hash function to Yekini's original message, which he has already decrypted. If the resultant hash value is not the same as the value supplied by Yekini, then Bello knows that the message has been altered; if the hash values are the same, Bello should believe that the message he received is identical to the one that Yekini sent. This scheme also provides nonrepudiation since it proves that Yekini sent the message; if the hash value recovered by Bello using Yekini's public key proves that the message has not been altered, then only Yekini could have created the digital signature. Bello also has proof that he is the intended receiver; if he can correctly decrypt the message, then he must have correctly decrypted the session key meaning that his is the correct private key.

### 7. Backing up Data

Why Backup?

Despite their appearance, computers are incredibly sensitive pieces of equipment. Dropping a laptop or hitting a desktop computer can easily make them unusable. This is because the hard disk drive is a very delicate: the part that reads the information is closer than the width of a hair to the surface of the disk, yet it must never touch it. This gives you an idea of how well made disks are to prevent it happening.

It is all too easy to accidentally delete important files. Often these are not recoverable. Another scenario is that changes and deletions can be made to a document, it is saved but the modifications have been made in error and the original file is required. Files can also become corrupt as re result of programs crashing, power failures or malware.

It is important then that computer users and business computer users in particular, have protection against these situations by having adequate backup copies of all files.

A backup is a copy of a file that can be used to replace the original in the case of the original being lost or corrupted.

**What should be backed up?**

The simple answer to this question is everything! The aim of a backup is to be able to carry on using a computer system whatever has happened to files, programs, computer system or the buildings or any combination of them. It should be obvious that in business taking a backup is not simply a matter of copying an odd file when you remember to do it. Backups must be done systematically, copying all the user files, programs and the operating system.

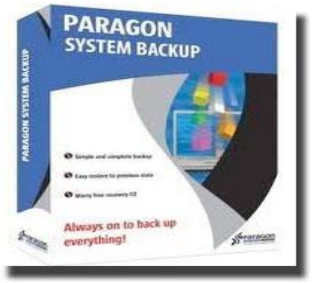
**How should data be backed up?**

**Backups can be made in two ways:**

i. **Manually**

Each of the files to be backed up is manually copied over to the backup medium. This is time consuming and error prone. The operative may miss out a file. The files cannot be is use when the backup takes place so it can also be disruptive to users.

**ii. Automatic**




There are various programs that can be used to make backups. The files to be backup us and the location of the backup can be set in the program. Start times can also be set. Automatic systems give much greater security that the backup will be completed because it doesn´t rely on people´s memory. However they can fail for technical reasons: the backup medium may not be available, it could be full or the file to be backed up could be in use.

For these reasons, it is important to check the backup log to ensure that the backup has been made as expected.

How often should backups be made?

**There are a number of factors to take into account when deciding how often to make a backup**

- How important is the file?
- How much would it cost to re-create?
- How often does the file change?

**How many copies to keep?**

This isn´t as easy a decision as it might first appear. Sometime problems with a file such as corruption or missing data might not be apparent for a few days. To get back to a good copy, the user calls for the last backup version. This too is found to have the same problem. To overcome this situation, companies will normally keep a number of backup copies in the anticipation that one of the ancestral copies will have a good version of the file. The actual number of copies will vary depending on the importance of the data and the frequency of backup. Files that are backed on a daily basis will be kept for one or two weeks before being overwritten. Files that are backed up on a weekly or less frequent basis may be kept for several weeks or months.

**Choice of Backup Medium**

Almost any form of storage medium can be used as storage for a backup. However, there are a number of factors that need to be taken into account especially when it is being used for important data that the company relies on.

Amount of data to be stored – large amounts of data will require magnetic tape or possibly DVD

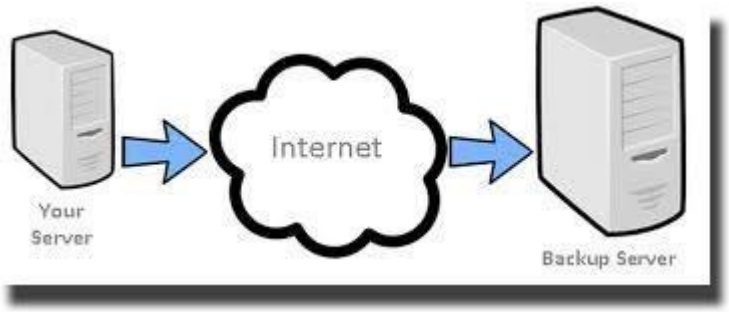
- Length of time backup is required – Space and cost of the storage medium will be a factor as well as the reliability of the medium.
- Speed of writing – hard drives are faster than tape but are more expensive

- Reliability of the backup medium – USB memory sticks are prone to corruption and hard drives may fail. Tapes are proven for long-term storage. CDs and DVDs are ok for 1 or 2 years but their long term reliability hasn´t been proven
- Security of storage – USB storage is very easy to lose or steal. Tapes are more secure they are less easy to steal and also they cannot be easily read, as they need special software.

There is no right or wrong media, but one which is most suitable, for a given a set of circumstances.

**Location of Backup Media**

Having gone to the time and trouble to create a backup copy, the company must now ensure that it is stored in a place where it is going to be safe. This will normally mean that it is in a separate location to the original data (termed off site). This is because any number of things may happen at the original premises. They may catch fire, there could be a bomb, and they may be damaged by storms or flooding. In such cases, the company will need to relocate and use another computer system. It will need to restore all its data from backup and if this were in the original building it would not be possible to access it.




An alternative to off site storage is to keep the backup in a fire proof safe in the same location as the original data. These will offer a high level of security from fire, water and physical damage **Physical Threats**

Digital storage media and hardware are subject to numerous internal and external forces that can damage or destroy their readability:

i. Material instability media threats
ii. Improper storage environment (temperature, humidity, light, dust)
iii. Overuse (mainly for physical contact media)
iv. Natural disaster (fire, flood, earthquake)
v. Infrastructure failure (plumbing, electrical, climate control)
vi. Inadequate hardware maintenance
vii. Hardware malfunction
viii. Human error (including improper handling)
Sabotage (theft, vandalism)

# CHAPTER SEVEN

# NETWORK DESIGN

***Effective network planning and design***

The network planning and design methodology describes a process with nine steps and a sequence for those activities. It is an engineering life cycle the support technical initiative such as windows. Good network design should enhance survivability i.e ability to remain alive or continue to exist with change of times and technology.

STEP 1: BUSINESS REQUIREMENTS

This begins with an understanding of their business model which rally describes how their company works from an operational and business perspective to generate revenues and reduce costs.

STEP 2: DESIGN REQUIREMENTS

The design requirements will build the framework that is used to define infrastructure, security and management. Design requirements are defined as standard and miscellaneous. The standard design requirement are generic and represent those consideration with many design projects. Miscellaneous requirements are those that are not defined with any of the standards requirements.

Standard design requirements

i. Performance
ii. Availability
iii. Scalability
iv. Stander compatibility
v. Rapid deployment

STEP 3 NETWORK ASSESSMENT

A network assessment is conducted after we have finished the business and design requirement of the company. A network assessment provides a quick snapshot of the current network with an examination of infrastructure, performance, availability, management and security.

The network assessment has three essential activities which are assessment, analysis and recommendation. The current network is examined using five primary surveys

i. Infrastructure
ii. Performance
iii. Availability
iv. Management and security

STEP 4: INFRASTRUCTURE SELECTION

After doing a network assessment, we are not ready to start selecting specific infrastructure components for the network design. This phase starts building the infrastructure with a specific sequence that promotes effective equipment selection and design.

It’s important that you consider business requirement, design requirement and network assessment when building your infrastructure.

Infrastructure components

The following numbered list describe the specific infrastructure components and their particulars sequence

i. Enterprise WAN topology
ii. Campus topology
iii. Traffic model
iv. Equipment selection
v. Circuits
vi. Routing protocol design
vii. Addressing
viii. Naming of convections
ix. IOS services
x. Domain name services (DNS)
xi. DHCP services

STEP 5: SECURITY STRATEGY

You must define a security strategy for securing the infrastructure. The need for enterprise network security should not be ignored with the proliferation of the internet. The security requirement and network assessment recommendations should drive the selection of security equipment, protocol and processes. It identifies what assets must be protected what users are allowed to access and how those assets will be secured.

TEP 6: NETWORK MANAGEMENT STRATEGY

This section will define a network management strategy for managing all equipment defined from the infrastructure and security. It is necessary to define how the equipment is going to be monitored an determine if the current management strategy is adequate or if new application, equipment, protocols and processes must be identified.

These primary elements comprises any well-defined management strategy and should be considered when developing your strategy

i. Management groups
ii. SNMP application
iii. Monitored devices and events

STEP 7: PROOF OF CONCEPT

All infrastructure, security and management components must now be tested with a proof of concept plan. It’s important to test the current design configuration and IOS versions in a nonproduction environment or the production network with limited disruption

The proof of concept model involves prototype design , equipment provisioning defining tests building equipment scripts and examining test results.

STEP 8: DESIGN PROPOSAL / REVIEW

With the proof of concept finished, you are now ready to build a design proposal for the design review meeting. Your intended audience could be directors, senior network engineers or anyone approving a budget for the project. Its important to present your ideas with clarity and professionalism

STEP 9: IMPLEMENTATION

The final step will have us defining an implementation process for the specified design. This describes a suggested implementation methodology of the proposed design which should have minimal disruption to the productive network. As well it should be efficient and cost effective as possible

## NETWORK DESIGN

Its an interactive process in which the designer examines users needs, develops an initial set of technology design assesses their cost and then revisits the needs analysis until the final network design emerges

### Traditional Network Design Process

It follows a very structured system analysis and design process similar to that used in building application systems i.e.

i. The network analyst meets the users to identify user need and the application systems planned for the network

ii. The analyst develops a precise estimate of the amount of data each user will send and receive and uses this to estimate the total amount of traffic on each part of the network

iii. Third the circuits needed to support the traffic plus a modest increase in the traffic are designed and cost estimates are obtained from the vendors

iv. One and two years later the network is built and designed

Forces making the traditional design process less appropriate for today's networks are:

i. The underlying technology of the client server computers networking devices and the circuits themselves is changing rapidly. There is more processing capability and network capacity than ever before

ii. The growth of network traffic is immense. The challenge is in the estimating the rate of growth. A minor mistake in estimating the growth rate can lead to major problem. Today, most network designers use three year planning horizon

iii. The balance of cost have changed dramatically

### The Building Block Network Design Process

1. NEEDS ANALYSIS

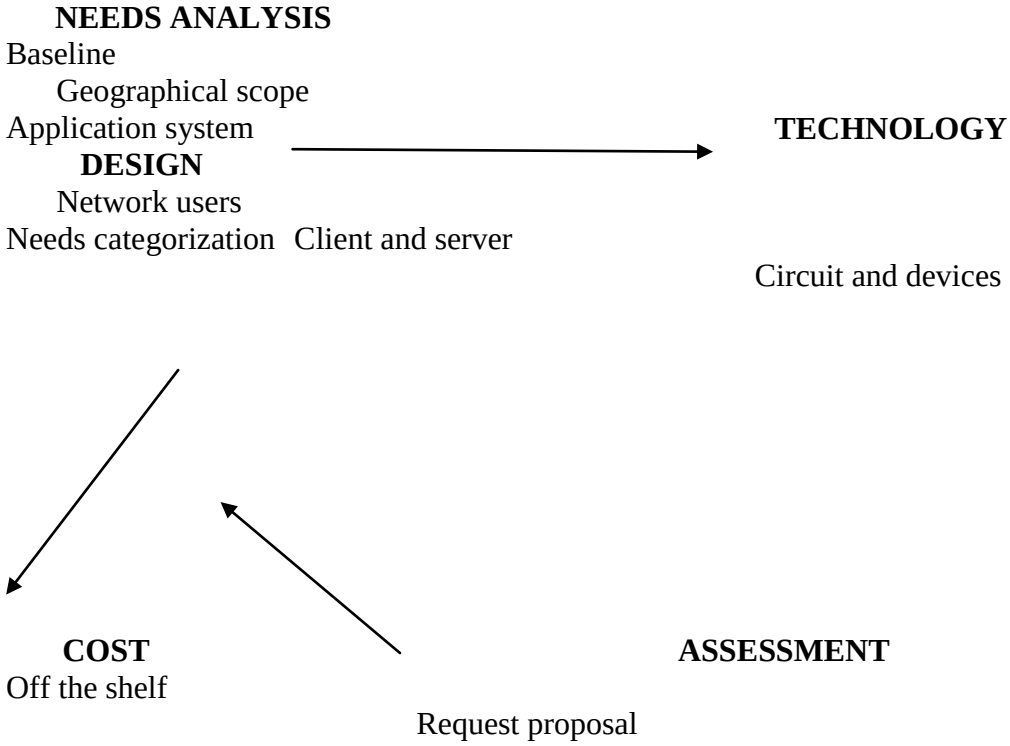
   The designer attempts to understand the fundamental current and future needs of the various users, departments and applications

   This is likely to be an educated guess at best. Users and applications are classified at typical or high volume. This step provides a baseline against which future design requirement can be gauged. Whether the network is a new network or a network upgrade the primary objective of this stage is to define

i. The geographical scope of the network. Access layer ( LAN or dial up connection)
ii. The user and the application that will use it .e.g. payroll or web servers

The goal of the needs analysis steps is to produce a logical network design which is statement of the network elements needed to meet the need of the organization

2. TECHNOLOGY DESIGN
   It examines the available technologies and assesses which option will meet user's needs. The designer makes some estimate about the network needs of each category or user and circuit in terms of current technology .e.g. 10BaseT, 100BaseT, 1000BaseT matches need of technology
3. COST ASSESSMENT
   This step assesses the cost of various physical network design alternatives produced in needs analysis and technology design. The main item are the cost of software hardware and circuits




The basic design process involves three steps that are performed repeatedly

i. Needs analysis
ii. Technology design
iii. Cost assessment

13.1. Building Home Network

Before pushing forward, we made the following assumptions

**i.** There is availability of DSL/Cable connection.
**ii.** Internet connection can be share with other computers.

The most common home network is Ethernet; it‟s a very popular LAN (Local Area Network) technology due to its inexpensive setup cost and reasonably fast speed. The other types of network are Token Ring, LocalTalk, and FDDI, but they are not important here. The speed (data transfer rate) of an Ethernet can be 10Mbps (Ethernet), 100Mbps (Fast Ethernet) and 1000Mbps (Gigabit Ethernet). Mbps is called Megabits per seconds. From our opinion, 100Mbps speed might be sufficient for the network set up here.

There is one rule here, make sure all your network devices (router, network card, switch, hub, network cable) are able to support the network with particular speed (10Mbps, 100Mbps, 1000Mbps) which you plan to set up. If you plan to set up a Gigabit Ethernet, although you have 100Mbps' network card, but your router can only support 100Mbps, then the network speed would be 100Mbps. See figure 71 for a usual network topology.

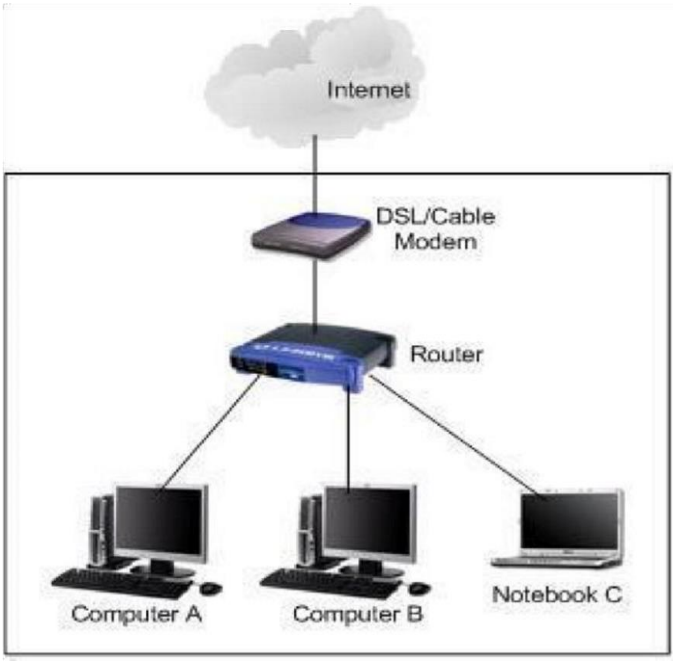



Figure 71: Usual network topology

13.2. Direct Connection of Two Computers

In this section we give the procedure for connectivity of two computers sometimes for file or printer sharing?

The two major network device required are: crossover cable and network cards. This is wired connection approach‟ it‟s effective and simple way if you want to connect the computers temporary. If the network card on computers supports auto MDI/MDIX feature, you could use crossover or straight through network cable to connect both computers. If not, crossover cable is needed.

Procedure

1. Plug in network card each to computer and then connect the network cable to both computers‟ network card. See figure 72.

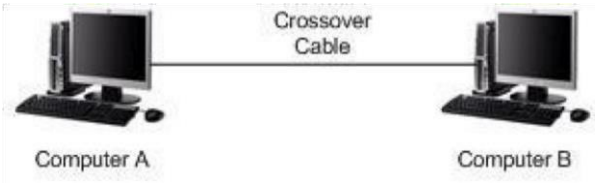



Figure 72: Direct connection of two computers

Network configuration

We assumed that network card on both computer are installed and working properly, for the network configuration, we create a simple network by assigning following IP address and subnet mask settings to each computer's network card, so that both computers know how to talk to each other:

| Computer A: | Computer B: |
|---|---|
| IP Address: 10.1.1.1 | IP Address: 10.1.1.2 |
| Subnet mask: 255.255.255.0 | Subnet mask: 255.255.255.0 |
| Gateway: [leave-it-blank] | Gateway: [leave-it-blank] |
| DNS Servers: [leave-it-blank] | DNS Servers: [leave-it-blank] |

As these 2 computers are directly connected, no gateway and DNS servers are required to be configured. After assigning IP address, try to ping the other computer from command prompt, you should be able to ping each other and then sharing printers or files as you wish.

## 13.3. Configuring of IP Address and Other Network Information in On Windows 7

IP address must be configured on computer in order to communicate with other computers, because this IP address is the standard address understood by computers and other networking devices in networking world. We can configure IP address, subnet mask, gateway and DNS servers manually on computer, we can also configure computer to obtain IP address and other network information from DHCP server (most of the time is configured on router).

Procedure

1. Go to Start and click on Control Panel.
2. Click View network status and tasks in Control Panel window. See figure 73.


Figure 73: Control Panel Window

3. Network and Sharing Center window will appear, and then click change adapter settings. See figure 74.


Figure 74: Network and Sharing Center window

**4.** Network Connections window will appear. Here you can right click on the network adapter (can be wireless adapter or wired Ethernet adapter) that you wish to configure and click

Properties. See figure 75.

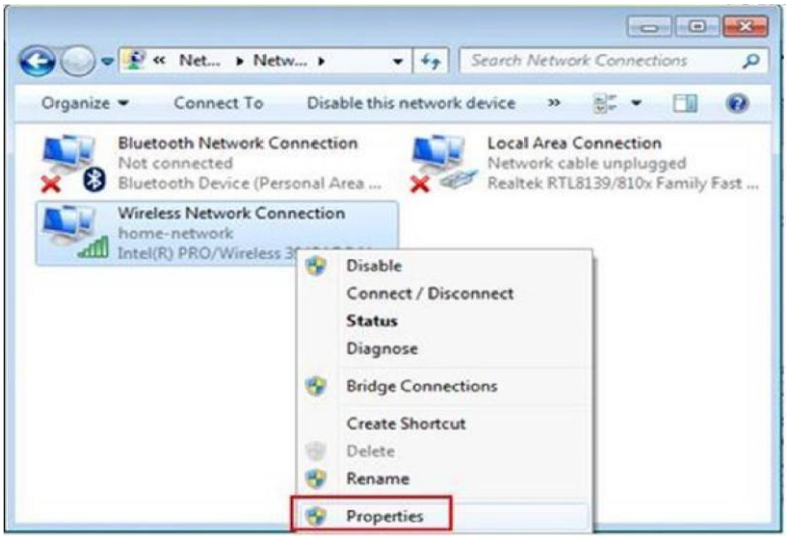



Figure 75: Network Connections window

5. In the Network Connection Properties window, tick on Internet

Protocol Version 4 (TCP/IPv4) and click Properties. See figure

76.

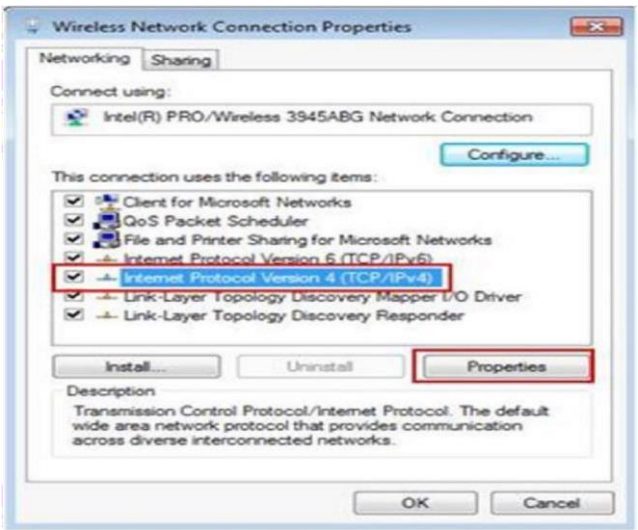


Figure 76: Network Connection Properties window

6. Assigning IP Address

**a)** After clicking properties, TCP/IPv4 window appear. (See figure 77) For manual IP Assigning we can now key in the IP address, Subnet mask, Default gateway and DNS servers. IP address of your computer must be unique. None of the 2 computers in the same network can share same IP address, because it will cause IP address conflict.

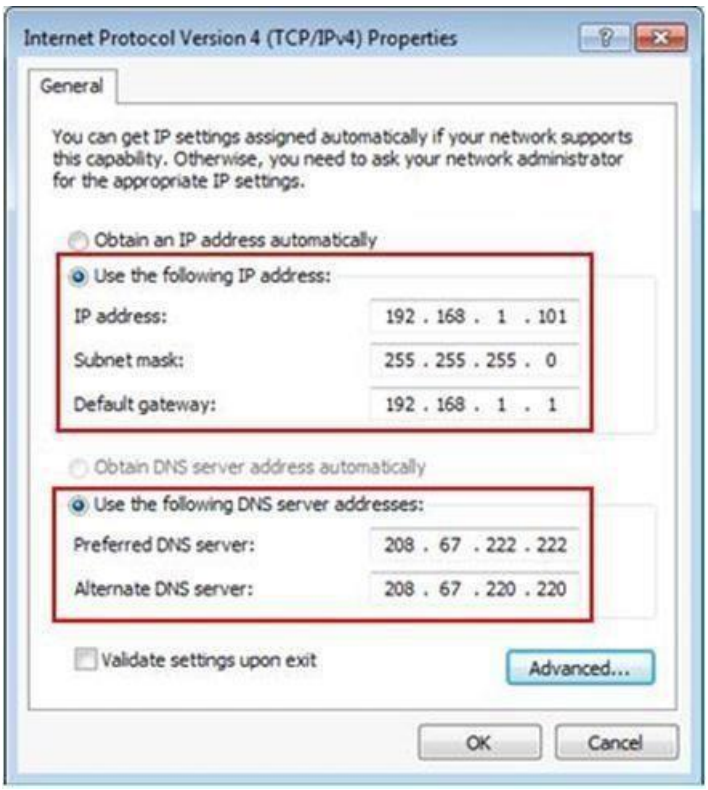
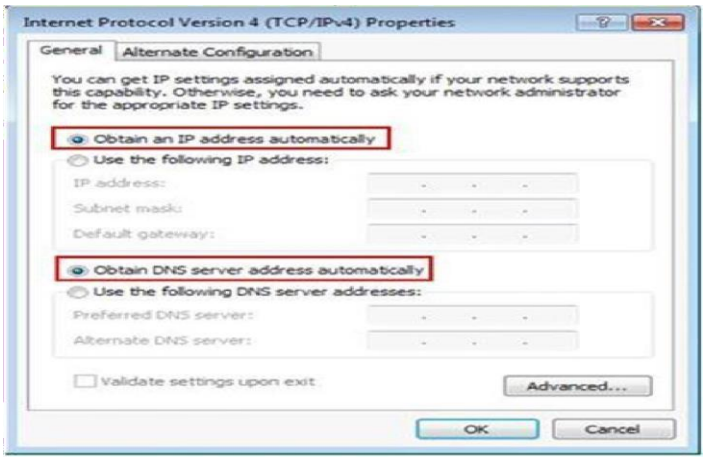



Figure 77: TCP/IPv4 window

Note: Default gateway is a router that can route the traffic to the other network or Internet. DNS server is an application server that can translate URL to IP address. Check with your ISP on what DNS servers you should use. If not, you can try this free Opendns or Google DNSservers.

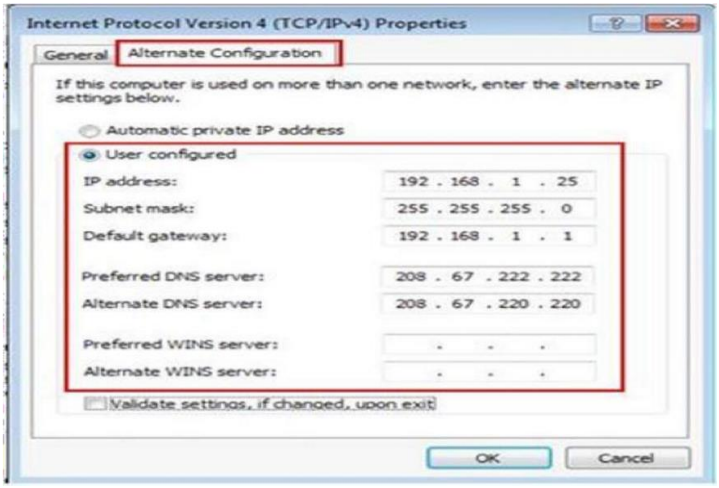
**b)** IP Assigned by DHCP server

If you have DHCP server setup on your router or you have dedicated DHCP server, your computer can be assigned IP address and other network information automatically by selecting Obtain an IP address automatically and Obtain DNS server address automatically. See figure 78.




IP Assigned by DHCP server

Note: If you have a laptop, and you use static IP at home and the IP assigned by DHCP server at the office, you can make use of alternate configuration to set IP and network information for these 2 different networks. Set Obtain an IP address and DNS automatically on General Tab as in the figure below so that the laptop will be assigned IP addresses automatically at the office. After that, click Alternate Configuration tab, select User configured option and key in your home network‟s static IP and other network information. By setting this, when there is no IP information assigned due to no DHCP server at home, this alternate configuration will be applied automatically, so that you don‟t have to spend time on configuring IP manually every time at home.




Using alternate configuration

Physical Network Setup

We will use D-Link's DI-604 broadband router as an example see figure 80. We can use other type of router according to your needs. Make available some straight network cable as well. Connect the WAN port on router to your cable/DSL modem using straight cable, then connect computers‟ network card to router‟s LAN ports using straight cable also. You can connect up to 4 computers to this router. Power on the router after finish connecting, you should be able to see the WAN and LAN lights on the router. Also you need to ensure that your DSL/Cable modem is configured in bridge mode, so that it can work well after connecting to router. Here is how to configure DSL/Cable modem in bridge mode.

This is very common setup after you have subscribed new DSL broadband service, you just need to configure the modem as a bridge, and after that configure PPPoE dialer in Microsoft Windows by providing username/password or other network information for accessing Internet.

If you plan to connect the modem to router and set up a home network, you must set bridge mode on modem too.

Procedure

1. Connect DSL modem‟s LAN port to computer‟s network card by using straight through network cable.
2. Read the modem manual, find out the default modem IP address, after that you need to set computer with the IP address in same network with modem, so you can access and configure it. As an example, if the modem IP is 192.168.1.1, I set computer IP as 192.168.1.10 (you can set 192.168.1.X, X= number between 2 and 254), netmask as 255.255.255.0 and gateway as 192.168.1.1.
3. Open a web browser and key in http://DSL-modemdefaultIP(example: http://192.168.1.1) into the address bar, after that hit Enter key.
4. The modem logon screen will appear, type in default username and password you found in modem manual. You will then log on to the modem management page.
5. Go to the correct configuration page by referring to modem manual, and then set the operation mode to Bridge mode. Here is an example:
6. The other important info for modem to work well is Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI), you need to set these numbers correctly. If you get the modem from ISP, most likely it‟s been preconfigured correctly.
7. Ok, at this stage you have done the modem configuration, you can then proceed to configure PPPoE dialer on connected computer. If you need help, here is PPPoE dialer setup in Windows 7, Vista and XP. If this modem is connected to router (wireless or wired), you can then proceed to configure that wireless router or Ethernet wired route.

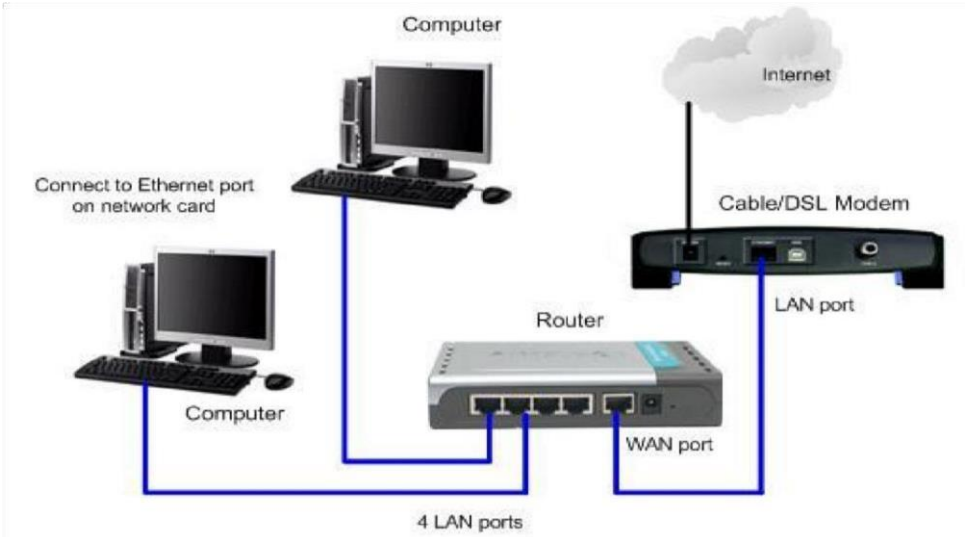



Figure 80: Physical Network Setup with D-Link's DI-604 broadband router

13.5. IP Logical Network Design

This is one of the task which we need to do is do after we have set up a network (wired or wireless) at home. This is the process to decide the IP addresses, netmask for computers, router and other network devices. Since each IP address assigned to your computer must be unique, you can‟t simply assign an IP address to your computer.

Here are 3 recommended IP ranges we can used in our network. These

3 blocks of private IP address space are reserved by Internet Assigned Numbers Authority (IANA) for private network, such as home network.

The three (3) Private IP address space: 10.0.0.0 - 10.255.255.255; 172.16.0.0 - 172.31.255.255; and

192.168.0.0 - 192.168.255.255. We can use the private IP address space in our network without worrying of conflict with the IP addresses in Internet.

After deciding the IP addresses to be used, the next is to decide what netmask to be used. Netmask will decide how many IP addresses available to be used in our network. Let use 255.255.255.0 for having 254 addresses to be assigned. There is a network address and broadcast address which can‟t be used for IP assigning. Network address is used to represent that particular created network, whereas broadcast address is used to talk to all computers in that particular network. Below are some examples for assigning IP addresses in on network.

**Example 1: 5 computers and a router on network**

Let us assign 10.0.0.1 to the router, 10.0.0.2 – 10.0.0.6 to other 5 computers. We use netmask 255.255.255.0 for this network, so that we can assign IP addresses 10.0.0.1 - 10.0.0.254 in the network. Network address is 10.0.0.0, broadcast address is 10.0.0.255.

**Example 2: 8 computers, 2 notebooks and a router on network**

Let us assign 172.16.10.1 to the router, 172.16.10.2 –

172.16.10.9 to other 8 computers and 172.16.10.10 – 172.16.10.11 to other 2 notebooks. We will use netmask 255.255.255.0 for this network, so that we can assign IP addresses 172.16.10.1 – 172.16.10.254 in the network.

Network address is 172.16.10.0, broadcast address is 172.16.10.255.

**Example 3: 8 computers, a router and a network printer on network**

Let us assign 192.168.1.1 to the router, 192.168.1.2 to the network printer and 192.168.1.3 – 192.168.1.10 to other 8 computers. we use netmask 255.255.255.0 for this network, so that we can assign IP addresses 192.168.1.1 – 192.168.1.254 in the network. Network address is

192.168.1.0, broadcast address is 192.168.1.255.

## Review Questions

1. Describe the procedure to connect two computer systems with only network card and cross over cable.
2. Under what condition can we use straight through network cable for connecting two computer systems.
3. Describe procedure for Configuring of IP Address on window 7
4. Describe how you can setup IP Logical Network Design for (1) 10 computers, 2 notebooks and a router on network; (2) 12 computers, a router and a network printer on network. Private IP addresses space: 10.0.0.0 - 10.255.255.255.
5. Why is it important to configure modem in bridge mode when setting up network? Hence describe the procedure to configure modem in bridge mode.

# CHAPTER EIGHT

# NETWORKING TROUBLESHOOTING

## Networking Troubleshooting Steps

When problems occurred in our network, there are one or more step the troubleshooter must follow. Some of these steps are:

Check the Cords & Power: The first thing you should always do is check to make sure everything is plugged in: your computer, router, device, etc. Many laptops have a button to turn off the wireless connection; the icon looks like a signal tower. When in doubt, read the manual.

Ping Yourself: You want to test that your machine is working properly. To do this, you want to ping yourself. You use the loop-back address (127.0.0.1) to do this. Pinging the loopback address tests to make sure software on your computer is working properly. Typically, if something is not working at this stage, you may just need to restart your computer.

Ping Your Router (AKA: the Default Gateway): The next step would be to ping your router. You can find your router‟s IP address with ipconfig as well (it should be on the bottom of the unit and listed in the manual too). Remember that ipconfig lists your router as the “Default Gateway.” It is very likely to be 192.168.1.1 or a similar number. This is done to test if your router is responding. If it is not, and you have already checked to make sure it is on, then it may need to be turned off and turned on. Every once in a while it may need a refresh.

If the problem continues, contact you ISP for assistance to see if they can help.

Ping Yourself with Your IP Address: We want to test to make sure everything is working correctly between your router and your computer. To do this, ping your IP address. It is listed in the ipconfig command at the same time the router IP number is. If this works, you can be confident that a problem is outside your network.

Ping and Tracert outside Your Network: From here, you want to test something outside your network. In a medium or larger network setting, a server on another branch of the network will do. For a home network, the Internet is often your only option. Since chances are the problem is that one or more websites are (or seem) down, this is a logical thing to check. You can use a few different tools. First try the ping command because it is the fastest. It will only tell you if the site is working or not.

For more detailed information, use tracert and pathping. They can give a better idea of what is going on. For instance, if you can reach your router, but no further, the node that connects you to the Internet may be down: an ISP issue. If you can reach only a couple (one or two) steps past your router, then it still is probably an ISP issue. Your Internet is down.

Ways to check if a website is down

Some of the ways to check if a website is down are.

**Ping:** A ping basically sends a Hello to a server waiting for a response. If the response takes too long a timeout will occur. Ping is measured in ms, if it is incredibly high something is wrong with either your computer, the route in between or the destination. The command is similar in Windows and Linux, just enter ping destination, with destination being an IP or domain name, and wait for the response.

**Traceroute**: You can compare Tracerouter with a list of all the roads that you travel until you reach your destination. Only that the roads are the servers in this case that your data is send through to reach their destination. If everything is fine the destination server should appear at the end, if it is not you could get timeouts for instance. Tracert is the command that you can use in Windows to trace the route between your computer and the destination. Use the command "tracert IP" or

"tracert domain" to achieve this. Traceroute is the equivalent in Linux.

Domain Name System (DNS): DNS errors most of the time occur when a website is freshly registered or moving to another server. It usually takes some time to update the DNS records to point at the new server. DNS is providing information much like your phone book is. Domain names are for us puny humans who have troubles remembering those server IP addresses (64.233.161.18 for Google for instance). Problems occur when the Nameservers who translate the human entered domain names into IP addresses have still the old IP in their records while the website is already up and running on the new IP. You can use the online script DNS Report to receive a detailed report. Green results are fine, red ones point to failures and yellow ones are warnings.

Proxies: Proxy"s can be used to establish connections to websites even if the direct route from your computer to theirs is somehow blocked. You can compare that to visiting a friend and using his computer to connect to a server that you cannot connect to. If it works it is somehow related to your computer or connection.

Troubleshoot Network Problem With "ping" Command Ping is a program used to check whether a host is up and active in network. It is commonly used to troubleshoot network problem. Figure 81 is typical home wired network design, let's explore how to use this ping tool to troubleshoot network problem and find the root cause.

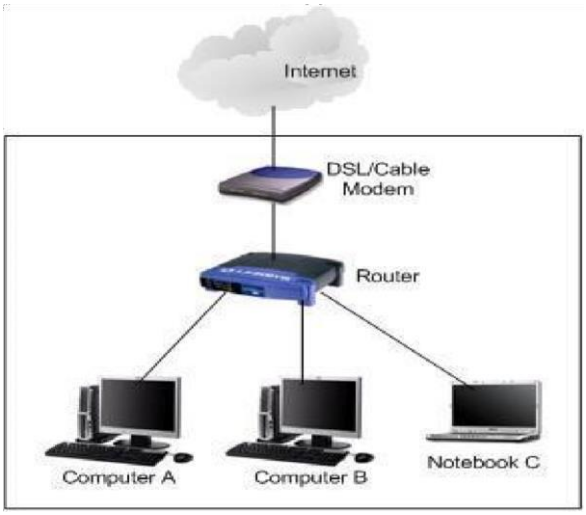


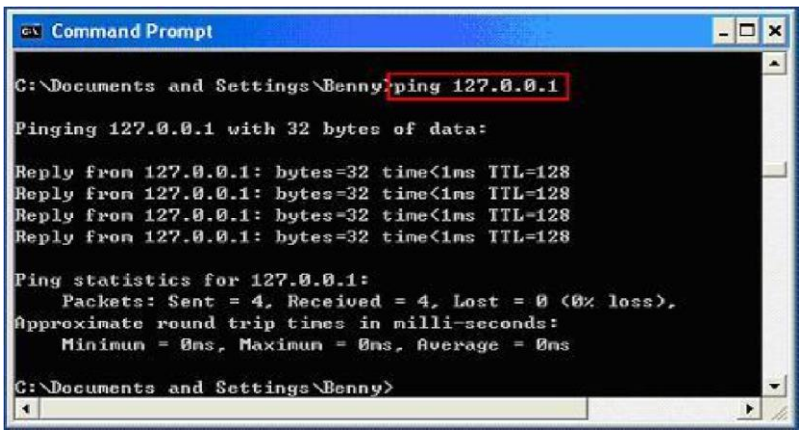

Figure 81: A typical home wired network

## PINGING

i. First thing you need to do is to make sure there is light on network card with cable connected. Sometimes network down is due to disconnected network cable or loose cable connection. If you notice no light on your network card after connecting with network cable, make sure the network cable is working and router that connected by this computer is up and active. If you see the light, then proceed to step 2.

Note: You need to make sure the network cable is connected to router's LAN port

2. Go to Start and click on Run.
3. Run window will appear. Type in cmd on Run window and click OK.
4. Key in ping 127.0.0.1 in Command Prompt window. This is network card loopback address. If you receive Reply from 127.0.0.1, it works. If you receive Request timed out, it means network card doesn‟t work properly. Unplug and re-seat the network card, connect with network cable then ping loopback address again. If still fails, check the network card driver status in Windows 7, Vista or XP to troubleshoot network card and make sure the card works well. If still fails, most probably the network card cannot be used anymore. Try again by using other network cards. However if you just cannot install network card driver correctly on this computer but it works on other computer, then maybe there is problem on Microsoft Windows OS or its TCP/IP function.



5. Ok, now you can proceed to ping your computer IP address. If you are not sure about computer IP, use ipconfig to find out. If you fail to ping this IP or no IP is configured on computer, check network configuration such as IP address (assigned manually or automatically?), subnet mask, gateway on network card to make sure it's configured correctly.
6. If you able to ping loopback address and your computer IP, proceed to ping router LAN IP address. If you receive Request timed out, make sure router is up and configured properly with correct IP, subnet mask, DHCP and other network settings.

Note: Ensure that your DSL/Cable modem is configured in bridge mode (not routing mode), so that it can work well after connecting to router. Even if router is up and it's configured properly, you need to check and ensure the computer is connected to correct and working router LAN port too, sometimes it might be connected to faulty port or incorrect port (such as uplink port). If you have enabled firewall on router, make sure firewall is configured correctly without dropping legitimate network packets.

7. If you can ping the router IP, then you should be able to ping the other computers or notebook in your network. If you still fail to ping the router IP or other computers, then you can take a look on this wired home network setup tutorial in order to get more helps.
8. If you have successfully done above steps and all are working properly, but you still fail to connect to Internet, then check your DSL, cable or wireless modem and router to make sure all cables are connected correctly. Reboot your DSL, cable or wireless modem and router and try internet access after that.

If still no Internet connection after that, connect computer to modem directly with network cable and test Internet connection. If this works, then I think the problem is on wired router configuration. If this fails too, contact your ISP for getting more helps to troubleshoot this network problem. This might due to some problems at your ISP side sometimes or the modem is broken.

## nslookup

Sometimes you might find out your computer is connected to network, but just cannot browse Internet websites. So what to do next? Just use nslookup to try resolving the domain name problem. If you wish to know what the IP address is resolved from domain name, you can use nslookup command to find out. This command is also useful to check whether the DNS servers configured in Microsoft Windows work well.

If the configured DNS server doesn‟t work well, the webpage will not be displayed on your web browser since the domain names will not be translated to IP addresses successfully.

Type in nslookup in command prompt window, you will enter interactive mode with > symbol. It also shows the DNS server (202.188.0.133) is being used to serve the system used in this case (different DNS IP address will be displayed in your command prompt). You can then enter the domain name which you want to check its IP address. For example, enter www.cisco.com and press Enter key, it will be resolved to 198.133.219.25. In another example, www.dlink.com will be resolved to 64.7.210.132. If the domain name can be resolved successfully, that means the configured DNS server works well on your computer. See figure 82.

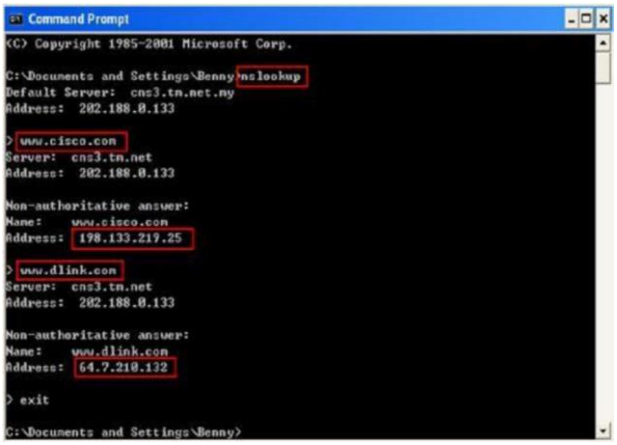
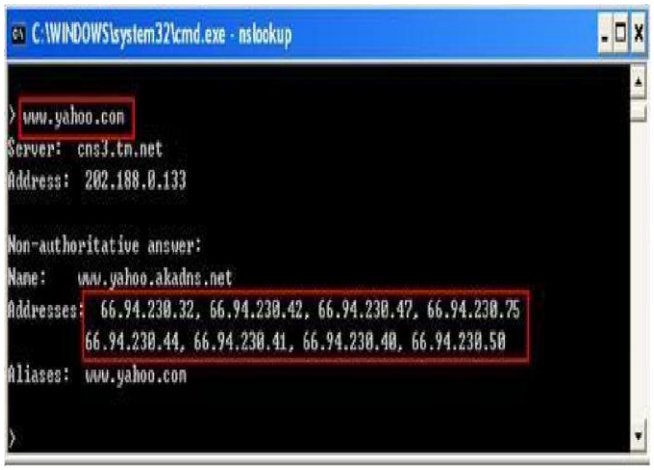


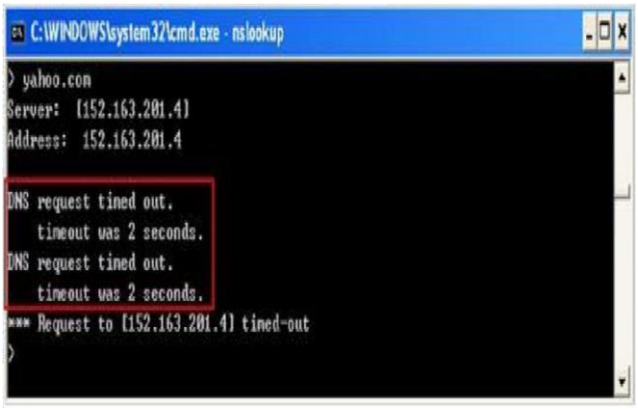

Figure 82: Command Prompt window for nslook

Don't feel surprise if sees multiple IP addresses share same domain name. Those domain names are usually popular domain names, such as www.yahoo.com, www.aol.com, www.microsoft.com, www.ebay.com, etc. Usually the main reason of having multiple IP addresses is to load balance the user access to those popular websites.

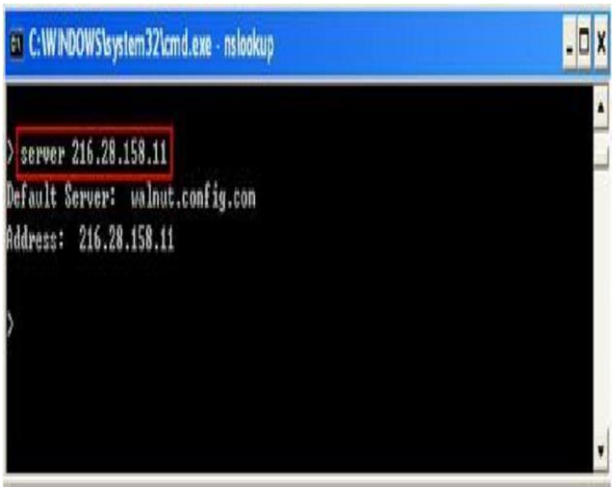



If you enter invalid domain name, the Non-existent domain message will be shown.


If you receive DNS request timed out messages which are shown as below, that means the domain name is failed to be resolved at the time being. The DNS server might be down or not valid, in this case you should try to resolve the domain name by configuring other DNS servers on your computer. If you are not sure which DNS servers to configure, feel free to use these free DNS servers from OpenDNS or Google to resolve domain names.




If you wish to check address translation by other DNS servers, such as your secondary DNS server, just enter this command server new-DNSserver-IP. I changed to DNS server 216.28.158.11.




## Review Questions

1. What are Steps towards Networking Troubleshooting
2. Describe Troubleshooting with Ping Commands
3. Describe the procedure for Troubleshoot Network Problem With “ping” Command.
4. On which condition can we require the use of nslookup command in network problem troubleshooting?

# CHAPTER NINE

# INTERNET AND EMAIL

## Introduction to the Internet

- ✓ It is a large no. of connected computers (or a large set of computer networks) linked together that communicate with each other, over telephone lines.
- ✓ It is a worldwide computer network connecting thousands of computer networks, through a mixture of private & public data using the telephone lines.
- ✓ It is a worldwide (global or an international) network of computers that provide a variety of resources and data to the people that use it.
- ✓ **Internet** refers to a global inter-connection of computers and computer networks to facilitate global information transfer. It is an interconnection of computers throughout the world, using ordinary telecommunication lines and modems.

## Features and functions of the Internet

**(i).** The Internet is a collection of networks; it is not owned or controlled by any single organization, and it has no formal management organization. However, there is an **Internet Society** that coordinates and sets standards for its use.
In addition, Networks have no political boundaries on the exchange of information.

**(ii).** Networks are connected by **Gateways** that effectively remove barriers so that one type of network can "talk" to a different type of network.

**(iii).** To join the Internet, an existing network will only be required to pay a small registration fee and agree to certain standards based on TCP/IP.
The costs are low, because the Internet owns nothing, and so it has no real costs to offset. Each organization pays for its own network & its own telephone bills, but these costs usually exist independent of the Internet.

**(iv).** Networks that join the Internet must agree to move each other's traffic (data) at no charge to the others, just as it is the case with mail delivered through the International Postal system. This is why all the data appear to move at the cost of a local telephone call, making the **Net** a very cheap communication media.

### *Functions of the Internet*

The Internet carries many kinds of traffic, and provides users with several functions. Some of the most important functions are:

1. **Communication.**
   Many people all over the world use the Internet to communicate with each other.

   Internet communication capabilities include; E-mail, Usenet Newsgroups, Chatting and Telnet. You can send e-mails to your friends anywhere in the world, chat with your friends, send instant messages, etc.

2. **Information retrieval.**
   The Internet is a library. Thousands of books, magazines, newspapers and encyclopedias can be read on the Internet.

3. **Easy-to-use offerings of information and products.**
   You can find information for your school assignments, buy books online, check what the weather is like anywhere in the world, and much more.

### Internet Services

The following are some of the services offered by Internet:

**(i).** Electronic mail (e-mail).
**(ii).** Fax services.
**(iii).** Conference services.
**(iv).** Online chatting.
**(v).** Downloading of programs.
**(vi).** Online shopping.
**(vii).** File transfer.
**(viii).** Entertainment (Games, Music and Movies).
**(ix).** Free information retrieval (e.g., Educational information).
**(x).** Formation of Discussion groups, e.g. Usenet Newsgroups.
**(xi).** Video Conferencing.
**(xii).** Access & Use of other computers.

### Electronic Mail (E-mail).

An **E-mail** is a system that enables sending & receiving of messages electronically through computers. It is used for communication between organizations or departments in the same organization. E-mail is a quick, cheap, efficient & convenient means of communication with both individuals and groups. It is faster than ordinary mail, easy to manage, inexpensive and saves paper.

With Internet mail, it is possible to send and receive messages quickly from businesses, friends or family in another part of the world. An E-mail message can travel around the world in minutes.

### Fax services.

Fax services enable individuals & businesses to send faxes through e-mail at a lower cost compared to the usual international Fax charges.

### Conference services.

**Conferencing on the Web** can be defined as the dynamic exchange of all kinds of information – text, graphics, audio, video, etc – in a situation whereby the conversations are organized by item and allows a participant to contribute spontaneous responses to any item in the conversation.

**Application of Conferencing on the Web.**

The conversation can:

- Provide important information that can assist in decision-making.
- Provide any required technical support.
- Help in community-building, project management & distance learning.

- Help to organize electronic meetings, etc.

The Internet also allows you to have access to various types of information you might require to make accurate and informed decisions, E.g., it provides information on business, education, sports, politics, etc.

### Chatting.

**Internet Relay Chat** (**IRC)** is a chatting system on the Internet that allows a large no. of people from various locations of the world who are on the computer to chat (i.e., simultaneously hold live and interactive electronic conversations) among themselves.

You can join discussion groups on the Internet and meet people around the world with similar interests. You can ask questions, discuss problems and read interesting stories.

Anyone interested in chatting can join a discussion forum on one of the listed topics. Only people who happen to be signed on at the same time are able to talk because messages are not stored.

This discussion can be an effective business tool if people who can benefit from interactive conversation set a specific appointment to meet and talk on a particular topic.

**Disadvantage.**

**(i).** Usually, the topic is open to all without security; so intruders can participate.

### Information retrieval.

The Internet is a voluntarily decentralized network with no central listing of participants or sites. Therefore, End-users, usually working from PCs are able to search & find information of interest located in different sites assisted by special software and data stored in readily usable formats.

The Internet gives you information on almost any subject. This is because of the Worldwide Web (www).

The **World Wide Web** is a global (an international) system of connected Web pages containing information such as, text, pictures, sound and video. The WWW is *hypertext based* (i.e., it is able to access text and graphical data formatted for easy search, retrieval and display).

With the WWW, you can review Newspapers, magazines, academic papers, etc. In addition, Governments, colleges, universities, companies and individuals offer free information on the Internet. E.g., you can inquire (find out) about universities in Britain or America.

**Note**. Its major problem is finding what you need from among the many storehouses of data found in databases and libraries all over the world.

### Dowloading of Programs.

There are thousands of programs available on the Internet. These programs include; Word processors, Spreadsheets, Electronic cards, etc.

You can therefore, look for the latest software over the Internet, e.g., you can get the latest Anti-virus software, and in addition, retrieve a free trial issue.

### Entertainment.

There are hundreds of simple games available on the Internet. These include; Chess, Football, etc. The Internet also allows you review current Movies and hear Television theme songs.

### Online Shopping.

You can order goods and services on the Internet without leaving your desk. E.g., you can view a catalogue of a certain clothes shop over the Internet and fill in an online Order form.

Commercial enterprises use the Web to provide information on demand for purposes of customer support, marketing and sales.

### File Transfer.

Data in the form of files can be transferred across the Internet from one site to another using the **File Transfer Protocol** (**FTP**). FTP software is needed at both ends to handle the transfer. It is through FTP that the two pieces of software manage to 'understand' each other.

### Discussion Groups.

A **Discussion group** is a collection of users who have joined together to discuss some topic. There are many discussions on different topics including Cooking, Skydiving, Politics, Education, recreational, scientific research, etc.

Two of the commonly used discussion groups for business are;

- Usenet newsgroups.
- List Servers.

**(a). Usenet newsgroups.**

These are the most formally organized of the discussion groups.

Using a facility on the Internet called **USENET**, individuals can gain access to a very wide variety of information topics.

**Usenet Newsgroups** are usually worldwide discussion groups in which people share information and ideas on a defined topic through large electronic Bulletin Boards where anyone can read any articles or write articles and post messages on the topic for others to see and respond to.

The individuals can add messages to different topics and read those contributed by others. For instance, users such as students can ask questions about problems they face, or they could contribute or give an advice on how to improve the teaching of the subject.

Messages can be easily linked so that it is easy to know messages that are related.

Establishing a new newsgroup requires a vote of all interested people on the Internet. If enough people express interest, the new topic is established.

**Note**. To join a Newsgroup and be able to read messages on various topics, your computer must have Newsreader software such as **Outlook Express**, or **Internet News**.

Any Internet user can access some of these newsgroups, while other newsgroups will require to subscribe to a specific topic or set of topics.

Once you have subscribed, each time you access the newsgroups you are informed of any new messages added to the topics. You can then read these messages and respond to them by adding your own message.

The Usenet software receives "postings" of information and transmits new postings to users who have registered their interest in receiving the information. Each individual posting takes the form like that used for e-mail.

There are over 10,000 such newsgroups; however, each Usenet site is financed independently & controlled by a **Site Administrator**, who carries only those groups that he/she chooses.

### (b). List Server

A **List Server** (or list serve) group is similar to the Usenet newsgroups, but is generally less formal.
Anyone with the right e-mail server software can establish a list server, which is simply a mail list.
The processor of the List Server processes commands such as request to subscribe, unsubscribe, or to provide information about the list serve. The List serve mailer directs messages to everyone on the mailing list.
To use a List server, you need to know the addresses of both the Processor and the Mailer. To subscribe to a List server, you send an e-mail message to the List server processor, which adds your name to the list. Many different commands can be sent to the List server processor to perform a variety of functions. These commands are included as lines of text in the e-mail messages sent to the processor.

List servers are more focused that the Usenet newsgroups and have fewer members. They are harder to find than the Usenet newsgroups because literally anyone can create one.

## Video Conferencing.

Video conferencing provides real-time transmission of video & audio signals to enable people in 2 or more locations to have a meeting.
The fastest growing form of video conferencing is **Desktop video conferencing**.

Small cameras installed on top of each camera enable meetings to take place from individual offices.

Special application software (e.g., **CUSeeMe**) is installed on top of each client computer. It transmits the image across a network to application software on a video-conferencing Server. The server then sends the signals to the other client computers that are to participate in the video conference. In some areas, the clients can communicate with each other without using the server.

Some systems have integrated other types of GroupWare with desktop video conferencing, enabling participants to communicate verbally to attend the same "meeting" while sitting at the computer in their offices.

**Advantage of Video conferencing.**

**(i).** Saves time & cost, as it reduces the need to travel.

## Access & Use of other computers.

The Internet has a facility called **TELNET** that enables a user on one computer to use another computer across the network, i.e., the user is able to run programs on the other machine as if he/she is a local user.

**Telnet** is a protocol, which enables a user on one computer to log in to another computer on the Internet.

TELNET establishes an error-free, rapid link between two computers, allowing a user to log on to his/her home computer from a remote computer even when traveling. You can also log on to and use thirdparty computers that have been made available to the public.

TELNET will use the computer address you supply to locate the computer you want to reach and connect you to it. You will, of course, have to log in & go through any security procedures you, your company, or the third-party computer owner have put in place to protect that computer.

Telnet requires an application image program on the Client computer and an application layer program on the Server of the host computer. Many programs conform to the Telnet Standard (e.g., **EWAN**).

Once Telnet enables the connection from the **Client** to the **Server**, you can log in by use of commands. The exact commands to gain access to these newsgroups vary from computer to computer.

Telnet enables you to connect to a remote computer without incurring long-distance telephone charges.

Telnet can be useful because, it enables you to access your Server or Host computer without sitting at its Keyboard.

Telnet can be faster or slower than a modem, depending on the amount of traffic on the Internet.

**Note**. Telnet is insecure, because everyone on the Internet can attempt to log in your computer and use it as they wish. One commonly used security precaution is to prohibit remote log ins via Tel-net unless a user specifically asks for his/her account to be authorized for it, or permit remote log ins only from a specific set of Internet addresses., e.g., the Web server at a university can be configured to only accept telnet log ins from computers located on the Kabete Campus network.

## Electronic Commerce.

Many people are actively using the Internet for Electronic Commerce (i.e., doing business on the Internet).

The use of the Internet in E-commerce is not necessary for making money as such, but mainly to find information, improve communication and provide information.

Many people automatically focus on the retail aspect of e-commerce, i.e., selling products to individuals. However, this is just one small part of e-commerce. The fastest group and the largest segment of ecommerce is business-to-business settings.

There are 4 ways in which the Web can be used to support E-commerce;

**(i). Electronic Store.**

**Electronic Store** is a Website that lists all the products or services a business wishes to sell, thus enabling customers to purchase them by using the Internet itself.

E-store sites provide physical goods and services.

The cost of providing information on the Web is low (unlike a Catalog, in which each page adds to the cost), and therefore, electronic stores can provide much information. In addition, electronic stores can also add value by providing dynamic information.

E-mail can also serve the purpose of E-store. This is because, e-mail is essentially a collection of estores. The mail usually provides all the computer information needed for e-commerce, and advertises the mail to potential customers. In return, the stores pay the mail a monthly fee or some percentage of sales.

**(ii). Electronic Marketing.**

E-marketing sites focus on the products or services of one company with aim of increasing sales.

This type of site supports the sales process, but does not make actual sales. The goal is to attract and keep customers.

By doing so, such sites provide a wealth of information about the firms and products complete with technical details and photos. Customers can review these but cannot buy over the Web. The idea is to encourage the user to visit a local dealer, who will then make a sale.

Computers also use e-marketing sites to provide newsletters with information on the latest products and tips on how to use them. Other companies enable potential customers to sign up for notification of new product releases.

E-marketing is cheaper in many ways than traditional marketing (radio, direct marketing, TV or print media). This is because while it costs the same to develop these traditional media, it costs nothing to send information to the customers. It is also easier to customize the presentation of information to a potential customer, because the Web is interactive. In contrast, the other media are fixed once they are developed, and they provide the same marketing approach to all who use it.

**(iii). Information / Entertainment provider.**

The Information/Entertainment provider supplies information (in form of text or graphics) or entertainment. These providers provide information from many sources with an aim of helping the users.

Several radio and TV stations are using the Web to provide broadcast of audio and video. The Web also offers new forms of real entertainment e.g., enables new multiplayer interactive games, which are not available in any other media. The information / entertainment providers generate revenue by selling advertisement printouts.

**(iv). Customers Service sales.**

This provides a variety of information for customers after they have purchased a product or service – to allow customers access most commonly needed information 24 hrs a day.

Many software companies post updates that fix problems so that customers can download for themselves.

Customer service sites benefit both the company and the customers. They enable customers to get a 24 hr support and easy access to needed information.

They often reduce the no. of staff needed by automating routine information requests that previously had to be handled by an employee.

## GroupWare.

**GroupWare** is a software that helps groups of people to work together more productively.

They are often organized using a two-by-two grid.

| Same place | Same time | Different time |
|---|---|---|
| | Group support systems | Group support systems |
| **Different place** | Video teleconferencing, Desktop video teleconferencing | E-mail, Discussion groups, Documentbased GroupWare |

GroupWare allows people in different places to communicate either at the same time (as on a telephone) or at different times.
GroupWare can also be used to improve communication and decision-making among those who work together in the same room, either at the same time or at different times.
GroupWare allows people to exchange ideas, debate issues, make decisions, and write reports, without actually having to meet face to face. Even when groups meet in the same room at the same time, GroupWare can improve meetings.
The major advantage of GroupWare is its ability to help groups make faster decisions, particularly in situations where it is difficult for group members to meet in the same room at the same time.

The 3 most popular types of GroupWare are; - Discussion groups.

- Group support systems.
- Video Conferencing.

### Group Support Systems (GSS).

Both e-mail and documents-based GroupWare are designed to support individuals and groups working in different places at different times. They are not suited to support groups working together at the same time and in the same place. In addition, they don't provide advanced tools for helping groups to make decisions.

**Group Support Systems** (**GSS**) are software tools, designed to improve group's decision-making. GSS are used with special-purpose meeting rooms that provide each group member with a network computer plus a large screen video projection system that acts as electronic blackboards. These rooms are equipped with special-purpose GSS software that enables participants to communicate, propose ideas, analyse options, evaluate alternatives, etc. Typically, a meeting facilitator assists the group.

The group members can either discuss verbally or use computers to type ideas and information, which are then shared with all other group members via the network. For large groups where only one person can speak at a time, typing ideas is faster than talking. Everyone has the same opportunity to contribute and ideas can be collected much faster. In addition, GSS enables users to make anonymous comments. Without anonymity, certain participants may withhold ideas because they fear their ideas may not be well received.

The system also provides tools to support voting and ranking of alternatives, so that more structured decision-making process can be used.

Just like in document-based GroupWare, vendors use the Web browser as their client software. So, almost anyone can access GroupWare Server.

**Note**. Discussion groups, document-based GroupWare and GSS all focus on the transmission of text and graphical images.

## Importance of services provided on the Internet.

The services offered by the Internet can be used as important tools in various ways:

**1).** As a research tool:

To learn about new developments or products, competitors, market news and customer opinions.

**2).** As an advertising / trading tool:

To help in selling goods or delivering information through the Web pages to customers on a 24-hour basis.

**3).** As a communication tool:

To support communication with customers, suppliers or staff through Electronic mail (e-mail).

**4).** As an Entertainment channel:

Most of the Games, Movies, and Television theme songs are available for free on the Internet.

In addition, you can have live, interactive conversations with people around the world including celebrities.

### Browsing the Web

This is also known as **Navigating** or '**Surfing' the Web**.

- To **Browse** is to navigate the Internet or the contents of your computer.
- **Browsing** can also be defined as moving around and between Web pages.

Using a Web browsing software you can read documents, listen to music, watch videos, make purchases, participate in surveys, advertise products, do research, share interests and download files on the Web.

**EXPLORING / BROWSING THE INTERNET.**

Use the **Internet Explorer** on your Windows desktop to browse the Web.

There are several ways in which you can browse the Web pages or "surf the net".

**(a).** When viewing a Web page, you can navigate the Internet by clicking *Links*, *Underlined text* or special features that cause you to jump to another Web page.

***Hyperlinks.***

A ***Hyperlink*** is a coloured or underlined text or a graphic that you click to 'jump' from one location to another. The hyperlinks enable the user to 'jump' to another file, or to another location in the same file.

All Web pages have hyperlinks. These links:

**(i).** Connect one part of a Web page to another part of the same Web page. This is useful if the Web page is large.

**(ii).** Connect one Web page to another Website somewhere on the Web.

**(iii).** Connect a page to a file, such as a sound clip, video, a Spreadsheet or a Word document.

The links can connect to objects stored anywhere on the Internet.

*Hypertext links* are indicated by underlined text highlighted usually in blue. Hyperlinks can also be represented by buttons, graphics or pictures.

To find hyperlinks on a page, move your mouse pointer over the page and where there is a hyperlink, the mouse pointer will change into a hand with a pointing finger. When you click a link, another Web page appears.

As you browse the Web, **Internet Explorer** stores the sites and pages that you visit. Usually, the hyperlinks you previously selected are colored differently. Internet Explorer does this to remind you that you have already visited the page identified by this link.

**(b).** You can also use the Standard toolbar buttons in the Internet Explorer to move between Web pages, or to search the Internet.

***History.***

**Internet Explorer** remembers the Websites and Web pages that you have visited. It keeps record of each Web page as it is downloaded. This is the *History* feature.

You can therefore, easily return to the page you have visited. To redisplay the page you have just left, click on the **Back** button. To move to the next page (available only if you have moved back), click the **Forward** button.

## Web Hosting.

A World Wide Web **Server** is a computer with programs that answer requests for documents from **Clients** (browsers) over the Internet. Files containing Web sites are placed on these servers.

A **Host computer** is any computer connected to the Internet and stores information that has been made available to the Web.

ISPs also use host computers to store user's electronic mail messages, Web sites and other related facilities such as, support software and appropriate security.

## Web Address (Uniform Resource Locator – URL).

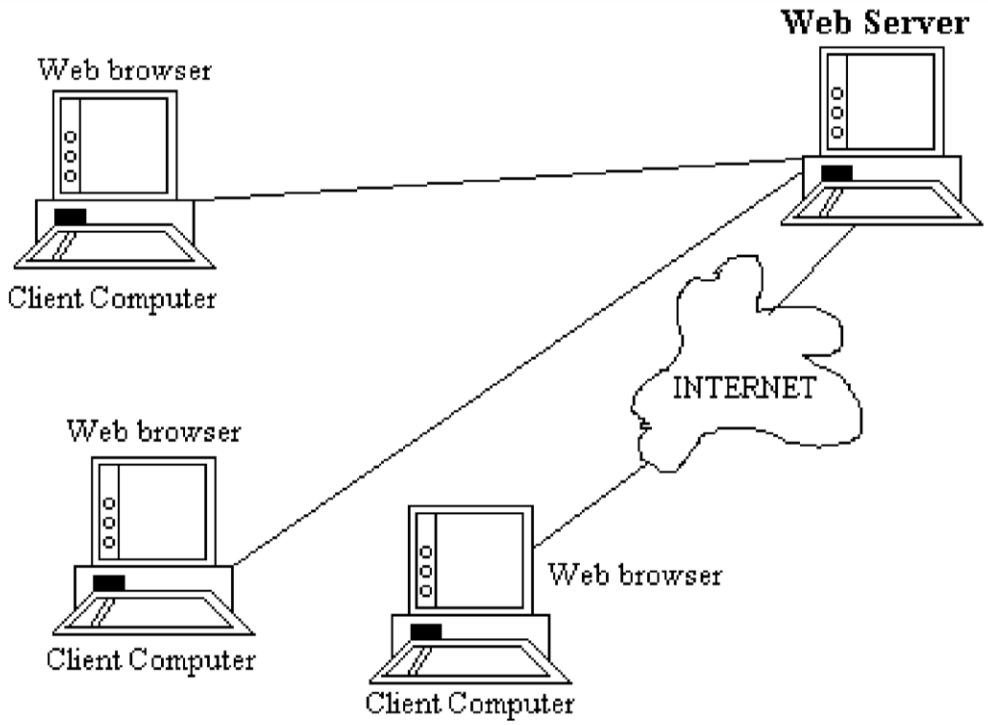
An **Address** is the location of a file.

Each Web page in the world has a unique Internet address or location. Internet addresses are also called the **Uniform Resource Locator** (**URL**). E.g., the general URL for Microsoft is http://www.Microsoft.com./

You can use addresses to find files on the Internet & your computer. You can instantly display any Web page if you know its URL. E.g., http://www.compaq.com.

**AutoComplete** - A feature in the Address Bar. When you begin typing a previously used address, this feature finishes it as you type.

*How the Web Works.*




Each Client computer needs an application software package called a **Web browser**, such as **Navigator**, **Internet Explorer**.

Each Server on the network needs an application software package called a **Web Server**. There are many different Web servers, such as those produced by Netscape, Microsoft and Apache.

In order to get a page from the Web, the user must type the **Uniform Resource Locator** (**URL**) for the desired page, or click on a link that provides the URL. The URL specifies the Internet address of the Web Server, the directory and the name of the specific page required. If no directory or page is specified, the Web server will display whatever page has been defined as its Home page. If no server name is specified, the Web browser will assume that the address is on the same server and directory as the last request.

In order for the Web server to understand requests from the Web browser, they must use the same standard protocol. If there was no standard, then each Web browser would use a different way to request pages. This means that, it would be impossible for a Web browser from Netscape to communicate with a Web server from Microsoft.
The standard protocol for communication between a Web browser and a Web server is the **HyperText Transfer Protocol** (**HTTP**). An HTTP request for a Web browser to a Web server has 3 parts, but only the 1st part is required, the other two are optional.

- The **Request Line**, which starts with a command (e.g., GET), provides the URL, and ends with HTTP version number that the browser understands.

- The Request **Header**, which contains a variety of optional information such as the Web browser being used (e.g., Internet Explorer), the date, the User ID and Password for using the Web pages as password protected.

- The Request **Body**, which contains information sent to the Server, such as information from a firm.

**Note**. Every Web user must provide the Internet address of the receiving computer, otherwise, the server would not know where to send the requested page.
Some browsers also provide the requestor‘s e-mail addresses as well. Most Web servers keep a record of Internet addresses of all the requests (and the e-mail address, if provided by the browser). Some companies use this information to make a follow up with prospective customers.

An HTTP response for a Web server to a Web browser also has 3 parts, but only the last part is required, the first two are optional.

- The Response **Status**, which contains the HTTP version number the server has used as status code (e.g., 200 means *‗OK*‘, 404 means *‗Page not found'*), and reason phrase (i.e., a text description of the status code).

- The Response **Header**, which contains a variety of optional information such as the Web server being used, the date, the exact URL of the page in the response body, and the format of the body (e.g., HTML).

- The Response **Body**, which is the Web page itself.

### Internet Addresses.

Internet addresses are strictly regulated, otherwise, someone could add a computer to the Internet that had the same address as another computer.
Each address has 2 parts; The *computer name* and its *domain*.

The **Domain** is the specific part of the Internet to which the computer is connected (e.g., Canada, Australia, etc).

The general format of an Internet address is therefore: **computer.domain**. Some computer names have several parts separated by periods. For example, the main university Web server of an imaginary University like Yairobi can be www.Yairobi.edu, while the college of Humanities and Social Sciences server can be www.chss.Yairobi.edu.

Each domain has an address board that assigns address for its domain. The boards ensure that there are no duplicates.

### *Finding Web pages (information) on the Web.*

There are 3 ways you can use to find interesting and useful Web pages on the Web;

**1).** You could get the **Web address** from an advertisement.
Many businesses include their Web addresses in their Television and Print advertisements.

**2).** You click a **link** that will enable you jump from one page to another.
Many industries or organizations, magazines and topic experts maintain pages that provide links from page to page.

**3).** Use of **Search Engines**.

## *Search Engines / Search Services.*

- A **Search engine** is software that helps in locating information in the Web.
- **Search engine** is a tool that searches the Web for information that you want to find.

**Purpose.**

√ If you want to get some information concerning an area or subject of interest over the Web but you do not know where to find it, you can use a Search engine to locate sites that contain the information.
√ Locate particular information in a Website, e.g., if you wish to read the Sports news you can load a Web site like http://www.cnn.com/, and then use a search engine within that site to locate information on Sports.

The following are the various search engines:

**1).** Yahoo – www.Yahoo.com.
**2).** AltaVista – www.altavista.digital.com.
**3).** Excite – www.excite.com.
**4).** Meta Crawler – www.metacrawler.com.

**5).** Infoseek.

**6).** Lycos.

These search engines offer different kinds of searching capabilities. However, they differ in the way they organize information in response to your request.

**Yahoo** focuses on the largest & most important Websites and organizes them in a directory format. Small and little known Websites are excluded. Therefore, if you are looking for the address of a wellknown company or product or a popular topic, Yahoo is probably the easiest way to find it.

**Alta Vista** is the broadest of all. It lists almost everything it can find. It is probably the best choice if you are looking for an unclear topic or a very specific combination of topics or words (e.g., to find a famous quote).

The major disadvantage of Alta Vista is that, you may have to look through dozens of sites before you find the ones you want. In addition, Alta Vista does not provide some help in focusing your search.

**Excite** is easier to use in that, it uses advanced special intelligence techniques to help you search those pages that best match your interest. E.g., after looking at the result of a search, you can tell Excite to find more pages that are similar to a specific page it has found. Excite will then search again and present those pages first. In this case, Excite refines the search based on the characterization of the page you have selected.

**Meta Crawler** provides the best search facilities. It does not search the Web and provide a list of what it finds. Instead, whenever you enter a search request, it simultaneously sends that request to several search engines (including Yahoo & Alta Vista), then combines, and organizes the information it receives from all the search engines into one display.

### *How Search Engines find Web pages.*

Hundreds of thousands of new Web pages are created each day. There are 2 ways that search engines use to locate Web pages:

- Use of Spiders / Robots.
- Through Submissions.

**(a). Spiders.**

**Search Engines** normally use software spiders to explore the Web. The **Spiders** are usually automated robots that travel around the Web looking for new pages, and creating links to them.

These spiders methodically search all the pages on the Websites they can find and report back their discoveries. The search engine builds an index to these pages based on the words they contain. When you connect to a search engine, and type a few words describing what you want, the Search engine will search its index for these keywords and provide you with a list of pages that contain them.

**(b). Submissions.**

These are derived from people who have created new Web pages and then submit information about the pages they have created.

1. Select a search engine, e.g., Yahoo, and type its address in the **Address** box, i.e., http://www.yahoo.com/.
   Once the search engine home page appears, type a keyword or phrase in the **Search** box, e.g., Kenya, then click the **Search** button.

   **Note**. The steps may vary depending on the search engine you are using.
2. When the search is completed, a list of sites that contain the keyword or phrase you are looking for is displayed. Select a site whose description comes closest to the information you desire and click on its link.
3. If there are many sites, an option that allows you to view the next 10 or so matches is displayed. Click on this if necessary to view the next set of links.
   If there are too many matches, you may want to use an additional keyword to narrow down the search. E.g., to find the sites that contain information about the economy in Kenya, in the **Search** box, type phrase "*Kenya AND Economy*".
4. Click the **Search** button.
5. From the search results, select the links that may help you get the information you require.

## Locate information within a Website.

Once you access a Website, you can search for specific text or information on that site or page. Unlike search engines like Yahoo, Infoseek, Lycos, Web Crawler, and Excite that present you with the URLs or links of sites that hold information you are looking for, search engines within a Web page locate information within that Web page.

1. Load the Web page to browse. E.g., let's use a Website: http://www.carleton.ca.
2. Click in the **Search** box, and type a keyword(s), e.g., *International AND Student*.
   **Note**. When typing in a keyword, you can use logical words or operators like **AND** (when you want to display results that meet both criteria) and **OR** (when you want to display results that meet one of the two criteria).
3. Click the **Search** button, to begin the search.
4. From the **Search Results** screen, click on a link that is closest to your requirements.

**To open a favorite Web site from the Start menu.**

**1.** Click the **Start** button, point to **Favorites**, and then click the Web page you want.

### To search the Web from the Start menu.

**1.** Click the **Start** button, point to **Find**, then click **On the Internet**.

### To use the Run command to open a Web page.

**1.** Click **Start**, click **Run**, and then type the Internet address you want.
   If the page you are opening is one you've viewed before, **the AutoComplete** feature can complete the address for you.

**To find pages you've recently visited.**

To find Web sites and pages you've viewed in the last few days, hours, or minutes.

1. On the toolbar, click the **History** button.

The **History bar** appears, containing links for Web sites and pages visited in previous days and weeks.

2. In the History bar, click a week or day, click a Web site folder to display individual pages, and then click the page icon to display the Web page.

**Notes.**

- To return to the last page you viewed, click the **Back** button on the toolbar.
- To view one of the last nine pages you visited in this session, click the arrow to the side of the **Back** or **Forward** button, and then click the page you want from the list.

### To enter Web information more easily.

The **AutoComplete** feature saves previous entries you have made for Web addresses, forms, and passwords.
When you type information in one of these fields, AutoComplete suggests possible matches.

3. When typing an information in the Address bar, and the **AutoComplete** feature suggests what you want to enter in that field, click the suggestion. If not, continue typing.

## Setting or changing a Home Page.

**Home page** is the page that is displayed every time you start **Internet Explorer**.

**Note**. Make sure it is a page that you want to view frequently, or make it one that you can customize to get quick access to all the information you want, such as the Msn.com home page.

√ To enable the user to choose or specify a page that will provide a good starting point for exploring the Web.
The **Home page** will appear each time the user accesses the Web.

1. Go to the page you want set as your Home page.
2. On the **Tools** menu, click **Internet Options...**. The **Internet Options** dialog box appears.
3. Click the **General** tab.
4. Under the **Home Page** section, type the address of the new home page in the Address box.
   Alternatively, click **Use Current** to make the current Website the home page.
5. Click the **OK** button.

**Tips.**

- To restore your original home page, click **Use Default**.
- You can return to your home page anytime by clicking the **Home** button.

## Downloading Web pages and programs from the Internet

√ To enable the user to view Web pages without being connected to the Internet.
√ To be able to browse a site in a location that does not provide any network access.
√ In order to free your telephone lines.

## Downloading a Web page

1. Load the Web page you want to download, e.g., http://www.nationaudio.com.
2. Access all the links that you would like to read offline. Make sure that the whole Web page is fully loaded before moving to the next one.
3. On the **Favorites** menu, click **Add to Favorites**.
4. Select the option **Yes, notify me of updates and download the page for offline viewing**.
5. Click **OK**, and then Logoff.

## Downloading a program

√ Programmers and software houses like Microsoft usually develop programs and may decide to send a test copy to their existing clients or to publish it on the Internet for interested users to test it for a specified period of time.

To test such software, a user will have to download the program onto the hard disk. A user can also download a movie clip or games, etc, and view it offline to save on costs.

1. Locate a site from which you wish to download a program, e.g., http://softwarenow.iboost.com.
2. Select the category of programs you want to download, e.g., Games.
3. Select a game category, e.g., Racing Games.
4. Select a game you want to download.
   **Note**. The window lists the properties of the program, e.g., version, file size. Ensure that you understand the licence agreement, i.e., whether the program is freeware or shareware.

   *Freeware* is a program that is absolutely free, while *Shareware* program is available for a limited period of time.

5. To download the program, click on the download link, e.g., **Download Cars & Brix**.
6. From the **File Download** dialog box, select **Save this program to disk** option, then click **OK**.
7. In the **Save As** dialog box, select the folder in which you wish to store the downloaded program, then click **Save**.
   Once the program is loaded, you can access the folder it was saved in and load it without being connected to the Internet.

*Saving pictures or text from a Web page.*

√ You can save information for future reference or in order to share with other people. You can save the entire Web page or any part of it: text, graphics, or links.

√ You can print Web pages for people who don't have access to the Web or a computer.

**To copy information from a Web page into a document,**

1. Select the information you want to copy, on the **Edit** menu, click **Copy**.

**To use a Web page image as desktop wallpaper.**

**1.** Right-click the image on the Web page, then click **Set as Wallpaper**.

## Saving information (a Web page) from the Internet to the Hard disk.

√ When you come across a Web page you would want to read, but it is too long, you can save the Web page onto your hard disk so as to read it later on when you are off-line. This helps in reducing the costs of browsing while online.

**1.** Load the Web page you want to download.
   - ❖ Make sure the Web page you want to save is completely transferred to the screen of your Web browser.

**2.** On the **File** menu, select **Save As**.
**3.** In the **Save HTML Document** dialog box that appears, select the drive & folder where you want to save the page in.
**4.** In the **File name** box, type a name for the page.
**5.** In the **Save as type** box, select a file type.
   - ❖ To save all of the files needed to display this page, including graphics, frames, and style sheets, click **Web Page, complete**. This saves each file in its original format.
   - ❖ To save just the current HTML page, click **Web Page, HTML only**. This will save the information on the Web page, but it does not save the graphics, sounds, or other files.
   - ❖ To save just the text from the current Web page, click **Text Only**. This saves the information on the Web page in straight text format.

**6.** Click **Save**.
   The Explorer program automatically assigns the extension **.htm** to the file name.

## To open a saved file.

√ After saving a Web page, you may want to read and analyze the information at a later time.

√ You may also want to send the saved file to another person via e-mail as an attachment.

1. On the **File** menu, select **Open**. This displays the **Open** dialog box.
2. Click on the **Browse** button in order to locate the folder where the file is stored.
3. Click the file, then choose **Open**.

**Note**. When you save a file in a local disk, only the text on the page is shown. The graphics in a site are displayed in graphics placeholders (which appear as small rectangles).

### *Graphics and Download time.*

When designing Web pages, graphics have to be incorporated sensibly into the Web page. Although they are appealing to the eye, the more graphics you use on a Web page, the longer the Web browser will take to download the page.

### *File Formats.*

The most common file formats found on the Internet are:

- Graphic Interchange Format (GIF), and - Joint Photographic Experts Group (Jpeg).

Generally, GIFs are used for simple page design elements like lines, buttons and dividers, while JPEGs are mostly used for complex photographs and images.

Movie (video) files usually have the extension **.avi**, **.mpg**, or **.mov**, while Sound (audio) files have the extension **.au**, or **.ra**, or **.ram**, or **.wav**.

### Printing Web pages.

√ To obtain a hard copy of the information that you have researched on and collected, for the purposes of reviewing later or filing.

## Change how a page looks when it prints.

Before printing a Web page, it is advisable to check the settings in the **Page Setup** dialog box.

This will ensure that the right Paper size, Margins and Orientation of the page are set correctly. You can also add headers and footers to a Web page.

On the **File** menu, click **Page Setup**.

1. In the **Margins** boxes, type the margin measurements (in inches).
2. In the **Orientation** area, click either **Portrait** or **Landscape** to specify whether you want the page printed vertically or horizontally.
3. In the **Header** and **Footer** boxes, specify the information to be printed, then click **OK**.

## Printing the Web page

1. On the **File** menu, click **Print** to display the **Print** dialog box.
2. Set the printing options you want, then click **OK**.

### Creating a Bookmark

√ When you browse the Web, you may come across sites that you want to visit regularly. Examples of such sites include; news sites like CNN or BBC. You can decide to _bookmark' the Web page.

The **Bookmark** feature (also known as a **Hotlist** or **Favorites** feature) allows you to store the addresses of Web pages that you frequently visit. Hence, you do not have to constantly retype your favourite Web page addresses. When you want to visit the site, simply select the bookmark from a list.

1. Open the Website that you want to create a shortcut to. E.g., http://www.cnn.com.
2. On the **Favorites** menu, choose **Add to Favorites**.
3. The **Add to Favorites** dialog box appears. The name of the site you are in appears on the **Name** box.
4. Under **Create in**: click the folder you want to add the site to, e.g., *Links*, then click **OK**.
5. This will add the title of the Web page in the Favorites list.

### To go to a site using a Bookmark

1. On the menu bar, select **Favorites**.
2. Select the folder that holds the favorites item, e.g., Links.
3. From the drop-down list, click **CNN.com**.

### To delete a Bookmark

1. On the menu bar, select **Favorites**.
2. Point to the item from the Favorites list, e.g., CNN.com.
3. Right-click the item, and then click **Delete**.
4. The **Confirm File Delete** dialog box appears.
5. Click **Yes**, to remove the item from the list.

### Working Offline

Connection to the Internet usually means that you are using telephone lines, and therefore incurring telephone charges and usage on your ISP account.

**Offline** - Not connected to a network or the Internet.

**BROWSING THE WEB (INTERNET) OFFLINE.**

√ To enable the user to save on the time spent connected to the Internet, and hence reduce the general costs of being online.

1. Access the Web site that you want to browse offline.
2. Access all the links to download all the information you require.
3. Ensure that each Web page is downloaded completely before going to the next one.
4. On the Taskbar, right-click the **Connection Indicator** button, then choose **Disconnect**.

The **Connection Indicator** disappears from the Taskbar showing that you are now working offline.

After disconnecting the user can go ahead and read all the downloaded information. The user can also "browse" through the site while offline provided all the pages and links are downloaded.

**Note**. Some services like Internet, Usenet, Newsroom, or Shopping will not be available when you are offline. To use these services, you need to re-establish the connection.

## Making Web pages available for offline viewing.

**Offline Reading -**To view a Web page without being connected to the Internet.

You can download the page to your hard disk, disconnect from a network or the Internet, and read the material later.

When you make a Web page available offline, you can read its content when your computer is not connected to the Internet.

E.g., you can view Web pages on your Laptop computer when you don't have a network or Internet connection.

1. On the Favorites menu, click Add to Favorites.
2. Select the Make available offline checkbox.
3. To specify a schedule for updating that page, and how much content to download, click Customize.
4. Follow the instructions on your screen.

**Note.** Before you go offline, make sure you update your pages. To do this, click the Tools menu, then click Synchronize.

### To make an existing favorite item available offline.

1. On the Favorites menu, click Organize Favorites.
2. Click the page you want to make available offline.
3. Select the Make available offline checkbox.
4. To specify a schedule for updating that page, and how much content to download, click Properties.

## Get Help with Internet Explorer.

### Purpose.

√ While working with **Internet Explorer**, you may sometimes need help on how to perform certain tasks or help on a particular topic of interest.

1. On the **Help** menu, select **Contents and Index** (or press **F1**).
2. The **Internet Explorer Help** window is displayed.
3. Click the **Contents** tab.
4. Click a book in the list, and then click a Help topic you want to look at.
5. The Help topic contents are displayed on the right-hand side of the Help window.
6. Read the help and click the **hyperlinks** (blue, underlined text) if you want to see help on related topics.
7. When you have finished, click the **Close** button to exit help.

### Using the Index to get Help.

1. On the Help window, click the **Index** tab.
2. Type in the first few letters of the word or topic that you are looking for.
3. In the **Index** box, all the help topics are listed in alphabetical order.
4. Click the **Display** button to view the information about the topic selected.

## Advantages of the Internet.

i. One can download (copy) information from a Website.

ii. The Internet has enabled the interlinking of people worldwide / globally. iii. It is convenient in the sense that you can access data 24 Hrs. iv. It is cheap, i.e., the operational cost that one may incur is low.

v. It has brought in the technology of doing the following; E-learning, E-Agriculture, Ecommerce, E-governance, etc.

vi. Provides up-to-date information.

vii. It doesn't require a lot of training to browse. viii. It provides entertainment facilities. ix. Can be used for research.

x. Brings harmony in the world, because people can communicate and exchange ideas.

xi. The Internet can be accessed at any part of the world. xii. There is always a full backup provided by the Servers, hence no data loss. xiii. It's a fast way of communicating. xiv. It provides an easy way to use offers in Information and products.

Internet provides information from almost all parts of the world that you need in order to make accurate and informed decisions.

You will get information you need from business to education, from sports to politics, from arts to eating out.

## Disadvantages of Internet.

i. It's a technology, which is fetched for (imposed/forced on) the Third world countries.

ii. The cost of the Internet Service Provider is high.

iii. It is leading to exposure of morally harmful shows such as Pornography. iv. It leads to spread of viruses.

v. Has proved to be unreliable especially accessing information. vi. No copyright rules meant to protect the property of an organization.

### Electronic Mail (E-Mail).

## *About e-mail.*

**Electronic mail** (also known as **e-mail**) is one of the common services provided by the Internet.

- **E-Mail** is a worldwide system for sending & receiving electronic messages from one computer to another.
- **E-Mail (Electronic mail)** refers to electronic messages sent over the Internet or a network. Email can contain both text & files.

With e-mail, users can create and send messages to one user, several users, or all the users on a distribution list.

Most e-mail software enable users to send text messages. In addition, users can attach files from Word processors, Spreadsheets, Reports, production data, etc, and then send them by e-mail.

Most E-mail packages allow you to do the same things you do with regular paper mail. You can file messages in electronic file cabinets, forward copies of messages to other users, send "carbon copies" of messages, and so on. The E-mail packages also allow you to filter or organize messages by priority. E.g., all messages from a particular user (e.g., your boss) could be given top priority, so that they always appear at the top of your list of messages.

However, E-mail is a much faster, economical & convenient way of sending messages to family, friends and colleagues than the paper mail (usually called "**Snail mail**"). Messages can be sent or received 24hrs a day. With "Snail mail" a message or a letter is sent to the recipient through the Post office and takes days or weeks before reaching the destination.

### *Components required.*

For one to be able to communicate using e-mail, the following components are needed: **1).** A **Computer** - where you will send or receive the e-mail messages.

**2).** An **E-mail program.**

Your computer must be installed with an e-mail program that lets you send, receive and manage your e-mail messages.

Examples of E-mail programs;

- **Microsoft Outlook**, **Outlook Express**, & **Microsoft Exchange** from Microsoft.
- **Communicator** from Netscape.
- Lotus Notes.
- Eudora.

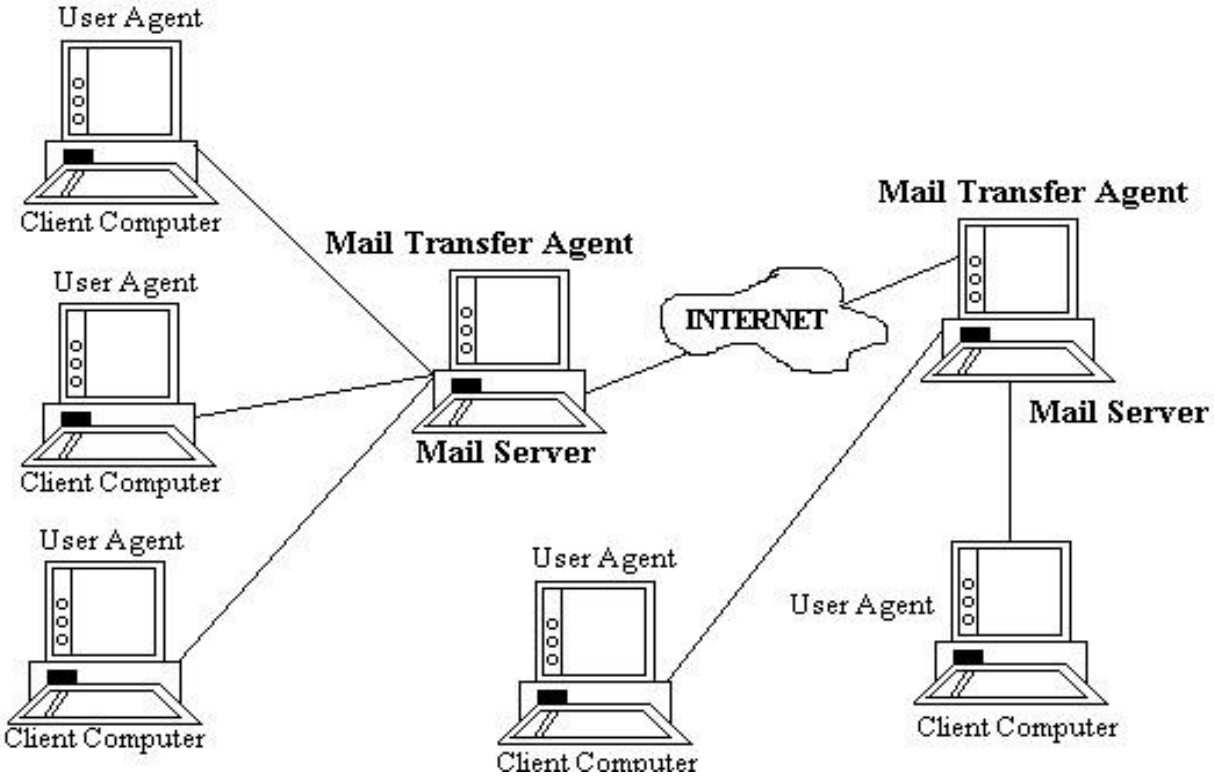
**3). E-mail address** of the sender & the address of the receiver.

**4).** An **Internet Service Provider** (**ISP**) - company who will deliver your message to the receiver.

Once you send a letter or a message, it travels from your computer through a Modem, which connects your computer to the Internet using the Telephone network. The Mail passes through various computers, until it reaches the final destination.

## How E-mail Works.

The figure below shows how an e-mail message can travel over a Wide Area Network (WAN) such as the Internet.




Each Client computer in the Local Area Network (LAN) runs an e-mail software package called **User Agent**, e.g., Eudora, Lotus Notes, Outlook Express, Microsoft Outlook, etc.

The user writes the e-mail messages using one of the User Agents, which formats the message into 2 parts;

**(i).** The **Header**, which lists the source and destination e-mail addresses. **(ii).** The **Body**, which is the message itself.

The User agent sends the message header & body to a **Mail Server** that runs a special application package called a **Message Mail Transfer Agent**. The Message Mail Transfer Agent in the Mail Server reads the envelope & then sends the message through the network (possibly through dozens of Message Transfer Agents) until the message arrives at the Mail Server of the receiver.
The Message Transfer Agent on this server then stores the message in the receiver‘s mailbox on the server.

When the receiver accesses his/her e-mail, the User Agent on the receiver‘s Client computer contacts the Message Transfer Agent on the Mail Server, and asks for the contents of the user‘s mailbox. The Message Transfer Agent sends the e-mail message to the client computer, which the user reads using the user agent.

## E-MAIL STANDARDS.

Several standards have been developed to ensure the compatibility between different e-mail software packages.

The 3 commonly used standards are:

**1).** Simple Mail Transfer Protocol (SMTP).
**2).** X-400.
**3).** Common Messaging Calls (CMC).

All the 3 e-mail standards work in the same basic fashion. **Simple Mail Transfer Protocol (SMTP).**

SMTP is the most commonly e-mail standard used on the Internet.

SMTP defines how Message Transfer Agents operate and how they format messages sent to them. As the name suggests, SMTP is a simple standard that permits only the transfer of text messages. Non-text files such as graphics or Word processing documents are not permitted.

However, several standards for non-text files have been developed that can operate together with SMTP. They include; **Multi-Purpose Internet Mail Extension** (**MIME**), **Unencoded** & **Bin Hex**.

A different standard called **Post Office Protocol** (**POP**) defines how User agents operate and how messages to & from the Mail Transfer Agents are formatted.

POP is gradually being replaced by a newer standard called **Internet Mail Access Protocol** (**IMAP**).
The main difference between POP & IMAP is that, before a user can read a mail message with a POP user agent; the e-mail message must be copied to the client's hard disk and deleted from the mail server. With IMAP, e-mail messages can remain stored on the mail server after they have been read. Therefore, IMAP is beneficial to users who read their e-mail from many different computers (e.g., at home, in office & in computer labs), because all e-mail is stored on the server until it is deleted.

## X-400

The X-400 e-mail standard was developed in 1984. It is a set of seven (7) standards that define how e-mail is to be processed by the User agents and the Mail Transfer Agents.

## Common Messaging Calls (CMC).

The CMC standard is a simpler version of the X-400 standard.

It was developed in 1994.
It is more popular than X-400, because it is simple & it is also supported by a large no. of leading vendors/sellers.

## File Transfer Protocol (FTP).

FTP enables you to send and receive files over the Internet. FTP requires an application program on the client server and an application program on the FTP Server. Many application packages use the FTP standard (e.g., WS-FTP).

Almost anyone can establish a FTP server, which permits anyone on the Internet to log in, send and receive files.

There are 2 types of
FTP sites; **(i).** Closed.
**(ii).** Anonymous.

**Closed FTP site.**

A Closed site requires users to have permission before they can connect and gain access to the files. Access is granted after the user provides an Account name with a secret password. For example, a **Network Manager** would write a Web page using software on his/her client computer and their user FTP to send it to a specific account on the Web Server. **Anonymous FTP site.**

Anonymous is the most common type of an FTP site.
It permits any Internet user to log in using the account of anonymous.

When using the anonymous FTP, you will still be asked for a password. You can enter your Internet e-mail address as the password.

Many files and documents available via FTP have been compressed to reduce the amount of disk space they require.
**Note**. If a file that you want has been compressed by a compression program that is not in your computer, you cannot access the file until you get the decompression program it used.

*Using Lotus Notes.*

One of the problems with e-mail is that, it lacks a structured way to support an ongoing discussion. Each mail message is a separate item, unrelated to the other

messages. Usually, you can group and file e-mail messages into separate file folders, but it not possible to combine them.

Using **Lotus Notes** (a document database of text and graphics), documents with different sections can be organized into a hierarchical structure of sections, documents and folders.

Lotus Notes can be used as a computer Bulletin board to support ongoing discussions. Several topics and sub-topics can be created, and everyone or selected individuals in the organization can be given access.

Lotus Notes can also be used to organize a discussion among certain people such as a Project team working to improve manufacturing quality. It might reduce the amount of time the team spent in face-to-face meetings, because many of the issues might be discussed before the meeting actually starts.

Lotus Notes also could be used to replace standard Word processors in preparing reports. Each team member could use Lotus Notes to write a portion of report, which could then be passed to other team members for editing or comments.

Lotus Notes can also automate certain document-based processes (called **Workflow automation**). For example, insurance claims require people from several different parts of an Insurance company to work together to process the claim. One person might handle the initial claim, which would then be passed to an Insurance adjuster to finish a report. Another person would process the payment. All this paperwork could be replaced if Lotus Notes were used to prepare and pass the documents from one person to another.

**Note**. Lotus Notes has the ability to replicate. **Replication** is the automatic sharing of information among servers when information changes. E.g., Lotus Notes servers can be set to replicate information they contain within any other Lotus Notes server on the network, so that a change to a document on the server will automatically be shared with all other servers that contain the same document.

### *Setting up (adding) an E-mail or News account.*

To set up an e-mail account, use an e-mail program such as **Outlook Express**. **Outlook Express** is a Web browsing software that can help you exchange e-mail messages with colleagues and friends on the Internet or join newsgroups to trade/share ideas and information.

You will need the following information from your Internet Service Provider (ISP) or Local Area Network (LAN) administrator:

- For e-mail accounts, you'll need to know;
  - The type of Mail server you use (POP3, IMAP, or HTTP) - Your Account name and Password.
  - Name of the incoming mail server and,
  - If you are using POP3 or IMAP, the name of an outgoing mail server.

- For a news account, you'll need to know;

- The name of the news server you want to connect to and, if required, your account name and password.

## To add a mail or news account.

**1.** On the **Start** menu, point to **Programs**, then click **Outlook Express**.
**2.** On the **Tools** menu, click **Accounts**.
**3.** In the **Internet Accounts** dialog box, click the **Add** button.
**4.** Select either **Mail** or **News** to open the Internet Connection Wizard, and then follow the instructions to establish a connection with a mail or news server. **Tips.**

- ❖ After you set up your account, just double-click the **Outlook Express** icon on the desktop to begin sending and receiving e-mail.
- ❖ You can get a free mail account from *Hotmail*, which uses HTTP servers.

## *E-mail addresses.*

Each user has his own **e-mail address** (or mailbox) in form of computer storage space to receive messages. The mailbox is accessed via a computer terminal within the system. In addition, each user has a password to protect access to his/her own mailbox.
Messages are drawn to the user's attention when they enter the system.

### Components of an E-mail address.

An e-mail address consists of two parts separated by the **@** symbol. For example, if your e-mail address is Drg@tropicalheat.com:

**(i).** The 1st part of the address to the left side of the @ symbol refers to the *person's identity* or *login name*. It is the name or identifier of the specific individual or organization, e.g., "drg".
**(ii).** The 2nd part following the "@" symbol is the *computer address*. It is usually made up of 2 to 3 sub-parts to further identify the individual, organization, ISP or a country. In this case:

- ❖ "tropicalheat" identifies the business.
- ❖ ".com" is the extension, which identifies the type of the organization.

The table below shows some extensions and what they represent: -

| Extension | Represents |
|---|---|
| .org | A non-profit making organization |
| .edu | An educational institution or organization |
| .com | A commercial organization |
| .net | Network |
| .mil | Military |
| .gov | government |

Sometimes, the name of the country is included in the e-mail address. E.g., Skynews@sky.co.uk or Nation@africaonline.co.ke.

In this case, ".co.uk" refers to a company in the United Kingdom, while ".co.ke" refers to a company in Kenya.

Examples of E-mail addresses;

Smith@CompuServe.com

Iat@Africaonline.co.ke

Were@Egerton.edu

Manager@Kenyapower.org

Bridge@arcc.or.ke

Tim@Yahoo.com (free e-mail address)

Douglas@hotmail.com (free e-mail address)

## Reading E-mail Messages.

√ Once an e-mail message that has been sent to you arrives at your computer, to read the contents you must open it using the program you have installed for sending e-mail, e.g., **Microsoft Outlook** or **Outlook Express**.

1. Open the e-mail program, e.g., **Outlook Express** from the **Start** menu or a shortcut on the desktop. The **Choose Profile** dialog box appears to allow you to select your profile.

   **Note**. A ***User Profile*** is a group of settings that define how the e-mail program is set up for a particular user. It also defines through the information services how a user can send, store, and receive messages.

2. Select your profile by clicking the down arrow on the **Profile Name** box, and then click **OK**. Usually, all incoming messages are stored in the **Inbox** when you connect to **Outlook Express**. The Inbox displays all the e-mail messages that you have received.

3. To open and read e-mail messages, click the **Inbox** icon either on the Outlook bar or on the Folders list, and then choose the message that you want to read.
   - ♣ To view the message in the preview pane, click the message in the message list.
   - ♣ To open the message in a separate window, double-click the message in the message list.

   The lower grid of your screen will have the full message.

4. When you have finished reading a message, you can close the window. Choose **Exit** on the **File** menu. This will take you back to the Outlook Express window. If there are any e-mails in the Outlook that have not been sent, a message will appear prompting you to send the e-mail(s) at that particular time or you can send it later.

**Tips**

- After **Outlook Express** downloads your messages, you can click the **Send/Recv** button on the toolbar, to read messages either in a separate window or in the preview pane.
- To view all the information about a message, such as when it was sent, click the **File** menu, and then click **Properties**.
- As you read the items in your items in your Inbox, you can reply to, forward, or file them in other folders that you create.

- To save the message in your file system, click **Save as** and then select a format (mail, text or HTML) and location.

## Reply to E-mail Messages.

√ If you have read a message, you may want to send a reply to the original sender.

√ If the original message that you are replying to was also copied to a no. of other people, you may want to send a reply to all of them.

When replying to a mail message, you can choose to reply with or without the original message insertion. The original message, sometimes referred to as the **History**, appears in the body of the message, and is used for reference purposes.

***Reply with the original message insertion.***

1. Open the message you want to reply.
2. Click the **Reply** button in the **Mail** window. The **Reply** message window appears containing the message you are replying to at the bottom.
3. Type the reply where the insertion point is.
4. When you have finished typing and editing the reply, click the **Send** button (if you are online) to send the message.

**Note**. If you click the **Send** button while you are offline, the mail will be placed in the **Outbox** folder and will automatically be sent the moment you are online.

***Reply without the original message insertion.***

To remove the original message, select the text, and then press the **DELETE** key or set options in the **Options** dialog box.

1. On the **Tools** menu, click **Options**.
2. Click the **Reading** tab.
3. Under **When replying to a message** box, click the down arrow, then select **Do not include original message**, then click **OK.**
4. Follow the procedure used to reply a message with the original message insertion. This time, the **Reply** message window will not contain the message you are replying to at the bottom.

**Note**. After replying to an e-mail, the **E-Mail** icon will indicate a checkmark showing that the mail has been replied to.

## Creating and sending an e-mail message.

√ To communicate with another user who has an e-mail address. This is cheaper than sending fax or using the telephone especially for long distance calls.

√ It is also faster to send e-mail than to post a letter.

E.g., to send a letter around the world using e-mail takes some few minutes as compared to the weeks ordinary mails take.

1. Start the **Microsoft Outlook** window.
2. On the toolbar, click the **New Mail Message** button. The message composition window is displayed.

3. In the **To…** and/or **Cc…** boxes, type the e-mail addresses of each recipient.

- If you want to sent copies of the message to other people, type in their e-mail addresses in the **Cc…** box, separating the addresses with a semicolon (**;)**.
- To add e-mail names from the **Address Book**, click the book icon in the **New Message** window next to **To**, **Cc**, and then select names.

- You can also send a **Blind Carbon Copy** (**Bcc**). In this case, the recipients entered receive the message but their names are hidden from other recipients of the message. To use the **Bcc** box, click the **View** menu, and then select **Bcc field.**

**4.** In the **Subject** box, type a message title.

**5.** In the lower grid of the message composition window, type in the message that you want to send. You can format the e-mail message using the formatting tools like, Bold, Font size, Underline, etc.

**6.** When you have finished typing the message, editing, and spell checking, click the **Send** button on the **New Message** toolbar.

**Notes.**

- To save a draft of your message to work on later, click the **File** menu, then click **Save**. You can also click **Save as** to save a mail message in your file system in mail (.eml), text (.txt), or HTML (.htm) format.
- A message that returns to the sender because it cannot reach its destination is referred to as a **Bounced message**.

## Checking the spelling in mail messages.

Before sending a mail message, you can spell check it to correct any spelling mistakes in the mail. **Outlook Express** uses the spelling checker provided with Microsoft Office 97 programs, such as Microsoft Word, Microsoft Excel, and Microsoft PowerPoint.

**1.** In the **New Message** window, click the **Spelling** button on the toolbar, (or click the **Tools** menu, and then choose **Spelling)**.

**2.** The **Spelling** dialog box appears. The misspelt words are highlighted and shown in the dialog box.

Choose the correct word by selecting it, and then click the **Change** button. If the word or phrase is correct but is not in the dictionary, click **Ignore**.

**3.** Once spell checking of the mail is complete, and a dialog box appears, click **OK**.

## Formatting e-mail message text.

To add special emphasis or structure to message text-such as bold, color, or bulleted lists, and also to add graphics and links to Web sites in your mail messages, use **Hypertext Markup Language (HTML)** - the standard language for formatting text for the Internet. **To use HTML formatting on all outgoing messages.**

❖ When you create messages using HTML formatting, only mail programs that support HTML can read the formatting. If the recipient's mail or newsreading program does

not read HTML, the message is displayed as plain text with an HTML file attached. The recipient can view the attached file by opening it in any Web browser.

To send the message in HTML formatting;

1. In the main window, click the **Tools** menu, click **Options**, then click the **Send** tab.
2. In the **Mail Sending Format** or **News Sending Format** sections, click **HTML**.

**To use HTML formatting on an individual message.**

In an e-mail message window, make sure HTML formatting is turned on, i.e., Click the **Format** menu, then choose **Rich Text (HTML)**. A black dot appears by the command when it is selected.

## To change the font, style, and size of text.

You can change the way the text looks for all your messages or you can make changes to selected text within a message.

**To change the text style for all messages.**

1. On the **Tools** menu, click **Options.**
2. Click the **Compose** tab, then click the **Font Settings** button.

**To format text within individual messages.**

1. Select the text you want to format. To change the font for an entire message, click the **Edit** menu, then click **Select All**.
2. On the **Formatting** toolbar, click the buttons for the options you want.

**To format a paragraph.**

1. Click anywhere in the paragraph, or select the text you want to format.
2. Use either the **Formatting** toolbar or the commands on the **Format** menu to change the text.

### Inserting items in a message.

**To insert a Business card in all messages.**

1. On the **Tools** menu, click **Options**, then select the **Compose** tab.
2. In the **Business Cards** section, select the **Mail** or **News** check box, and then select a business card from the drop-down list.

**Notes.**

- To change information in a business card, click the **Edit** button.

- To add a business card or signature to an individual message, in a message window, click the **Insert** menu, then click either **Signature** or **My Business Card**.

**To include a sound in a message.**

1. Click anywhere in the message window.
2. On the **Format** menu, point to **Background**, and then click **Sound**.
3. Enter the name of the file you want to include and the number of times you want the file to play.

**To insert a picture in a message.**

1. In the message, click where you want the image to appear.
2. On the **Insert** menu, click **Picture**, then click **Browse** to find the image file.
3. Enter Layout and Spacing information for the image file as needed.

**Notes.**

- If message recipients are not able to view your inserted images, click the **Tools** menu, and then click **Options**. Click the **Send** tab, click **HTML Settings**, and then make sure that **Send pictures with messages** is selected. Then resend your message.
- To insert a background picture in your message, in the message window, click the **Format** menu, point to **Background**, then click **Picture**. Click the **Browse** button to search for the file you want to use.

## Attaching files to e-mail messages.

√ You can attach a copy of any type of file such as a document, spreadsheet, graphic image or a presentation to your e-mail messages.

1. Click the **New Message** button.
2. In the **Message Composition** dialog box, enter the e-mail address and type in the message to be sent.
3. Click where you want the file attachment to appear, then click the **Insert File** button to display the **Insert File** dialog box.
4. Locate the folder that contains the file you want to attach, and then click the file.
   To select multiple files, hold down the CTRL as you click each of the files.
5. Click the **OK** button.
   The attached file is displayed as an icon in the body of the message. The icon indicates the file type and name. e.g., *Sales Results.xls*
6. Click the **Send** button.

**To open or view the attached file.**

Documents that contain file attachments display a paper **clip** image in the view or folder next to the document file.
Once the document is open, Microsoft Outlook displays an icon representing the attachment.

**Note**. You must have the application in which the attachment was composed in order to open it. The **MIME** (**Multi-purpose Internet Mail Extension**) type of file enables Internet browsers to access an Internet mail file without prompting the user to specify the program used to create the attached file.

1. In the **Inbox**, select the e-mail message that contains the attachment.
2. Double-click the e-mail message to open it.
3. Double-click the icon that represents the attachment.

**Deleting an attachment.**

1. Open the e-mail message that contains the attachment.
2. To delete the attached file, click the file icon, then press the **Delete** key.

Organizing E-mail messages.

√ You can use Outlook Express to organize your incoming messages and make it easy to send mails.

To use your online time efficiently, use Outlook Express to find messages, automatically sort incoming messages into different folders, keep messages on a mail server, or delete them entirely.

## Organizing the Inbox.

You can organize the messages in your Inbox quickly by sorting them.

To quickly sort messages by *Subject*, *Sender* or the *Date received*, click on the respective column header. E.g., to sort your messages in alphabetical order by sender, click on **From** in the column header.

## To create a Mail folder.

1. On the **File** menu, click **New**, then choose **Folder**.
2. Enter the name of the folder in the **Name** box, e.g., *My Own*.
3. Select the **Inbox** folder so that the mail folder created will become a subfolder of the Inbox.
4. You can add details, such as a description of the folder in the **Description** box, then click **OK**.

## To move or copy a message to another folder.

1. In the message list, select the message (s) you want to move or copy.
2. On the **Edit** menu, click **Move to Folder** or **Copy to Folder**, then select the folder you want to move or copy the message to.

## To delete a mail message.

1. In the message list, select the message.
2. On the toolbar, click the **Delete** button (or press the **Delete** key).

**Notes.**

- To restore a deleted message, open the **Deleted Items** folder, and then drag the message back to the **Inbox** or other folder.
- If you don't want messages to be saved in the **Deleted Items** folder when you quit Outlook Express,
  1. Click the **Tools** menu, then click **Options**.
  2. On the **Maintenance** tab, select the checkbox labeled **Empty messages from the 'Deleted Items' folder on exit**.
- To manually empty all deleted items,
  1. Select the **Deleted Items** folder.
  2. On the **Edit** menu, click **Empty Deleted Items Folder**.

## Sending a Web page by e-mail.

√ You may find some interesting and useful material on the Internet that you would like to share with friends and colleagues.

You can send Web pages by e-mail to other people even if the recipients are not connected to the Internet.

1. Access the Web page you want to send.
2. Click the **File** menu, point to **Send**, then click **Page By E-mail** or **Link By E-mail**.
3. If necessary, choose the correct profile to use from the **Profile** dialog box, i.e., Outlook Express, and click **OK**.
4. In the **Message** dialog box, enter the address of the recipient, then click the **Send** button.

**Note**. You must have an e-mail account and an e-mail program set up on your computer.

### *Blocking Unwanted messages.*

You can control the mail and news messages you get in Outlook Express . You can block certain people from sending you mail, you can hide conversations that don't interest you, and you can guard against being sent damaging code in mail by setting security levels. **To block messages from a sender or domain.**

You can block messages from a particular sender or domain.

- The **Domain** is the name following the **@** symbol in an e-mail address.
- **Domain** - A group of networked computers that share information & resources.

When you block a sender or domain, no e-mail or news message from that sender or domain will arrive in your **Inbox** or in the news messages you read.

E-mail from blocked senders goes directly into your **Delete** folder while Newsgroup messages from blocked senders are not displayed.

1. From your e-mail Inbox or the list of messages in a newsgroup, select a message from a sender you want to block.
2. On the **Message** menu, click **Block Sender**.

The e-mail address of the sender will appear in the **Address** box. You can type a different address or domain in the **Address** box if you wish.

3. Select the blocking option you want: mail, news, or both kinds of messages.

**Important.** Blocking a sender applies to standard POP mail only. It does not apply to HTTP mail (Hotmail) or IMAP messages

## Differences between E-mail and General Post office mail.

**1).** E-mail is computerized, while Post office mail is manually operated.
**2).** Post office mail is slow, while E-mail is fast & has a wide area of coverage. **3).** E-mail is more secure.

**Advantages of E-mail.**

Electronic mail has several advantages over regular mail.

**(i).** It is cheap & economical.
It costs almost nothing to transmit an e-mail message over the network, i.e., there is no need for stamps, envelopes, etc.

**(ii).** It is secure, i.e., access to a user's mailbox can be restricted by use of a password.

**(iii).** It is faster, i.e., mails can be sent instantly.
The delivery of an e-mail message normally takes seconds or minutes, depending on the distance to the receiver.

**(iv).** It is efficient, i.e., a message prepared only once can be sent to several people.

**(v).** It is convenient.
With E-mail, you can send your messages when it is convenient for you and your recipients respond at their convenient times.

**(vi).** E-mail is cheaper in terms of the time invested in preparing the message.
The expectations and culture of sending & receiving e-mail are different from that of sending regular letters. Regular business letters & inter-office memos are expected to be error-free and formatted according to certain standards. In contrast, most e-mail users accept less wellformatted messages and slight typographical errors are overlooked. So, less time is spent perfecting the appearance of the message.

**(vii).** E-mail can act as a substitute for the Telephone calls, thus allowing the user to avoid **telephone tag** (i.e., the process of repeatedly exchanging voice mail messages because you or the other person may not be available when the other calls).
E-mail can often communicate enough of a message so that the entire "conversation" will take less time than a phone call.

E-mail is particularly effective for multinational organizations, which have people working in different time zones around the world.

**Disadvantages of E-mail.**

**(i).** The initial installation cost is higher.

**(ii).** Messages may be lost before they are read due to virus infections.

**(iii).** Messages may not be kept for future reference due to the high cost of storage, i.e., it requires regular deletion of messages from the hard disk.

## Using the Address Book.

√ The **Address Book** is a directory of personal details, including e-mail addresses, for the people to whom you send messages (called **Contacts**).

It is used to store/keep track of e-mail addresses, mailing addresses, phone numbers, and other information about your friends and also provides space for notes.

You can store such addresses in the Address Book so as to address mails more easily, i.e., each time you want to send e-mail messages, you simply select the names from the list of addresses.

This will save the time used to enter lists of e-mail addresses as well as help maintain their accuracy. E.g., an e-mail address like Njiiri.mworia@mit.edu.uk can be difficult to remember. In addition, one can easily make a typing error when typing the address.

The Address Book is accessible from **Internet Explorer**, **Outlook Express** and **NetMeeting**, thus enabling you to keep one list of addresses that are accessible by various programs.

**To add a contact to the Address Book.**

1. To open the Address Book, click the **Address Book** button.
   There can be several types of address books in the Address Book dialog box including the Global Address list and Personal Address Book.

2. In the **Show names from the** box, select the type of address book you want to use.

   The **Global Address list** is the address book that contains all e-mail addresses for users, groups, and distribution lists in your organization that you can address messages to. The Administrator creates and maintains this address book.

   The **Personal Address Book** is the address book used to store personal distribution lists you frequently address messages to, such as a list of your friends.

3. Click the **New Entry** button.
4. Specify the entry type of the contact, i.e., whether it is an Internet address or an entry for a distribution list.
5. Type in the display name for the address as well as the full e-mail address.
6. Complete the dialog box with the rest of the contact details using the other tabs, e.g., Business or Phone Numbers, then click **OK**.
   The contact address is added to the Address Book.

## To edit a contact in the Address Book.

1. Open the Address Book.
2. Select the contact that you want to edit.
3. On the File menu, click Properties.
4. Make the necessary changes to the information, then click **OK**.

## To create a contact from a mail message.

When you receive a mail message, you can add the sender's details (name and e-mail address) to your Address Book.

1. From the **Inbox**, right-click a message.
2. Select **Add sender to Address Book**, from the shortcut menu that appears.

## To delete a contact from the Address Book.

1. Open the Address Book.

2. Select the address that you want to remove from the Address book.
3. Click the **Delete** button (or press the **Delete** key).
4. Click **Yes** to confirm that you want to delete the name or entry.

## To create a distribution list.

If you send mails to the same group of people frequently, you can create a group address list. Group address lists are known as **Distribution lists**.

When you address a message to that group, each individual in the group receives it.

**Note**. You must have a Personal Address Book set up in order to be able to create a personal distribution list.

1. Open the **Address Book**.
2. Click the **New Entry** button.
3. In the **Select the entry type** box, click **Personal Distribution List**, and then click **OK**.
4. In the Name box, type a name for the group, e.g. Sales Dept., then click the **Add/Remove Members** button.
5. To add members to the group, select a contact or name from the left hand list box, then click the **Members** button (or double-click on a name) to move the name to the right list box. The contact is copied to the Personal Distribution List box.

6. Repeat step 5 until you have all the names you want in your group in the Personal Distribution List, then click OK.

   The group or distribution list is usually listed in the Address Book.

## To send a message using the Address Book or distribution list.

1. In the Microsoft Outlook window, click **File** then select the **New Mail Message**.
2. Click the **To…** button to open the Address Book.
3. Select the contact names from the list or select the distribution list, then click on **To ->**.

   **Note**. To see the full e-mail addresses, select the name of the person from the lists and click on **Properties** button.

4. Click **OK** to return to the message composition dialog box.
5. Type out the rest of the message and click on **Send**.

**READING MAIL MESSAGES OFFLINE.**

Once you have opened the E-mail program, it is not necessary for you to be connected directly so that you can read & write your e-mail messages. You may choose to work offline to save on costs. When you are offline, **Outlook Express** downloads mail messages to your local computer. When you connect (or choose to work online) again, messages in your Outbox are sent, messages you marked for deletion are removed, and all other actions taken offline are completed at once.

There are 2 situations where it is beneficial to use Outlook Express offline:

**(i).** If your ISP charges you by the hour or if you have only one phone line. Under these conditions, you might want to reduce time spent online.

**(ii).** If you use a Laptop to read your messages while you are traveling or any other time you are not connected to the Internet.

**To set up Outlook Express to reduce online time.**

1. On the **Tools** menu, click **Options**.
2. On the **Connection** tab, select **Hang up after sending and receiving.**

If you connect to an IMAP or HTTP server, click the server name in the folder list, and then make sure that the items you want to view offline are checked.

This procedure can be used to set up Outlook Express so that it automatically disconnects after you select **Send and Receive** from the **Tools** menu.

You can then read and compose messages offline without incurring charges or tying up a phone line.

**Note.** To reconnect to send or receive messages, click the **Tools** menu, point to **Send and Receive**, and then select the option you want.

**To read messages while you are away from your Internet connection.**

1. On the **Tools** menu, select **Options,** then click the **General** tab.
2. Under the field labeled **If my computer is not connected at this time**, select **Connect only when not working offline**.

   If you connect to an IMAP or http server, click the server name in the folder list, make sure that the items you want to view offline are checked, and then click **Sync Account.**

3. On the **File** menu, click **Work Offline.**

**Note.** To check the type of account you have, click the **Tools** menu, and then click **Accounts**. Select your e-mail account and then click **Properties**. The account type is listed on the **Advanced** tab.

As social media, app stores and global availability become standard, many companies are looking to enhance the online customer experience. And while retail and other transactions via Internet are customary, more than ever companies are simplifying the ways in which customers interact with their website and ultimately make online purchases. Here are eight trends happening right now in global ecommerce that seek to enhance the user experience:

1. **Micro-payments:** Among the most revolutionary changes in the coming months—not years—is the use of micro-payment systems from a variety of financial firms, e.g., Paypal, Visa, WesternUnion, among others, including banks. This trend is facilitated by the W3C working group that approved these protocols and technical standards for the interworking. These systems will change not only how we carry money but how we value money and think about purchases. (Consider how a purchase of $4.99 feels in a mobile app store vs. at Dunkin' Donuts.) Payment systems that make it easier to buy online, coupled with mobile technologies will accelerate the usage of global e-commerce applications.

2. **Mobile technologies:** More people access the Internet on their mobile devices than on any other device. We are rapidly approaching the time (if we are not already there) where designs must be created for the mobile web first, and for the desktop second. Mobile technologies facilitate comparison shopping; with the advent of barcode reader apps and price-comparison databases, a consumer could snap a bar code in Walmart and quickly reference product reviews and prices on walmart.com (or compare prices with Walmart

competitors). Mobile technologies also facilitate impulse buys – especially with the advent of micro-payments tied to the mobile device. Just recently, Starbucks customers can not only place an order with their Smartphone, but also make a purchase.

3. **Social media:** As Facebook has become the most visited site on the Web, the role of social media, including Facebook and its local clones such as Twitter, is increasingly important. Social media sites Page **112** of **112** increasingly act as points of entry to e-commerce sites, and vice versa, as e-commerce sites build rating, loyalty and referral systems tied to social media. Group buying (e.g., Groupon) is also gaining mainstream ground, with many "deal of the day" sites competing for an increasingly savvy consumer base, but improvements lie ahead as the social aspects and user experience are refined.

4. **Fulfillment options:** I believe that users will want to have multiple fulfillments and return options when interacting with a vendor: ship to address, courier, pick-up in store, return to store, etc. Having many fulfillment options is how customers view their overall customer experience. Some companies have made a business proposition online by being exceptional in service to the online channel (e.g., Zappos).

5. **Global availability:** Increasingly, consumers want the availability to buy products from foreign sites and have them delivered locally. Thus, currency and customs will be of growing concern to many online retailers. Along with this, there will be concerns with local privacy laws and restrictions on related data collection and storage.
6. **Localization:** While the trend is to globalize, what_s often more important is to localize. User

Centric_s (now GfK_s User Experience team) research clearly shows that sites that _feel_ local – with proper imagery, language, time/date, weights/measures, currency, etc. – resonate far more than sites that seem culturally distant or sterile.

7. **Customizability:** Consumers want control, and want to be able to design the details of the items they purchase.

8. **Time-based availability:** Some of the hottest and most successful sites are those that have a timecritical response component. Sites like Groupon, Gilt and others capitalize on the perception of limited-time availability. Creating a sense of urgency drives traffic and purchase behavior.

# CHAPTER TEN

# EMERGING TRENDS

***Emerging trends in computer networking***

As bandwidth demands on network continue to grow, companies are placing greater emphasis on higher-performance infrastructure solutions to address performance in various levels of the network.
Today, companies have a wide variety of connectivity options to optimize network performance and management.

i. Software defined Networking(SDN))

Although still in the nascent stage, SDN will slowly gain traction. Cloud computing and mobile internet will place greater demands on the network infrastructure and SDN will go a long way in providing the agile service delivery that people will expect from the networks. Established networking vendors will ramp up on their SDN strategy/execution or look to acquire start-ups to get a leg-up on the competition.

ii. Bring your own Device (BYOD) to work

Companies will have to get onto the BYOD bandwagon. Younger employees who are part of the digital generation and who are used to their own devices will increasingly demand that they use the same devices at work. This will provide increased savings and productivity but companies will need to figure out their network infrastructure to support the plethora of devices and also need to pay more attention to security.

iii. Web Security/ Anti-virus

One of the best secrets is that anti-virus products are often not very good at stopping viruses.

iv. Cloud Computing and Bandwidth of Networks

The data migration from PC to cloud will continue to grow exponentially. The need to store vast volumes of data will drive more innovation in computing and storage architectures. We will also see changes in virtualization, parallel computing, distributed storage and automation. Low-bandwidth networks are a bottleneck in this path of progress. We will see a push towards 10G as the router interface and 100G as the trunk interface.

v. WI-Fi Offloads

With spectrum being a scarce commodity, service providers will figure out a way for largescale adoption of Wi-Fi offloading to increase the efficiency of the wireless network. They will need to do this to meet the increasing demands of Smartphone users to access high bandwidth content

**Backbone considerations**

The link between telecommunication room on each floor and the buildings equipment room is one of the most highly trafficked parts of communication networks. The backbone connects each floor and each building in the enterprise speeding information to the appropriate destination.

**Satisfying large port demands**

In the data center LAN, the horizontal segment is the link between the server and the access or edge switch. In the dense computing environment with redundant connectivity, many ports are

needed for large numbers of ports ultimately drives the importance of total solution cost, giving copper connectivity an advantage.

**Media and management payoff**

No matter what the media choice or management route taken, the broader trend will be adding intelligence and control to the physical layer. Real-time management infrastructure works with media choices, whether its copper or fibre and manages the system with constant updates, helping one reduce network maintenance cost, effectively utilize assets and increase revenue.

***Challenges of emerging trends in networking***

i. One is not able to decide which network gear they need.
Networks can be built with different combinations of hardware and software. The sheer no of choices overwhelm most beginners who too often go for the first solution they find.

ii. Network wont reach certain areas
Stringing network to some rooms within a building can prove impractical.

iii. Computers cant communicate with each other

One may conclude connecting all the network gear but the network fail to communicate with each other.

iv. Network application fail to function

When other aspects of the network may work reliably, this does not guarantee success with the next features that need installation.

***Coping with challenges of emerging trends in networking***

i. Special training should be offered to new network users on how to make good choices over the network they should opt for.
ii. Concessions should be made in network installation plan when the network is to be installed.
iii. Taking a step by step approach to the problem, to see where the failure is and fix it.
iv. The communication links should be perfectly laid to make sure all applications run perfectly well.

**Clouds and grids compared**

**Let's take a look at the main differences between grids and clouds.**

| | **Grid computing** | **Cloud computing** |
|---|---|---|
| What? | Grids enable access to **shared** computing power and storage capacity from your desktop | Clouds enable access to **leased** computing power and storage capacity from your desktop |
| Who provides the service? | Research institutes and universities federate their services around the world through projects such as EGI-InSPIRE and the European Grid Infrastructure. | Large individual companies e.g. Amazon and Microsoft and at a smaller scale, institutes and organizations deploying open source software such as Open Slate, Eucalyptus and Open Nebula. |

| | | |
|---|---|---|
| Who uses the service? | Research collaborations, called "Virtual Organizations", which bring together researchers around the world working in the same field. | Small to medium commercial businesses or researchers with generic IT needs |
| Who pays for the service? | Governments - providers and users are usually publicly funded research organizations, for example through National Grid Initiatives. | The cloud provider pays for the computing resources; the user pays to use them |
| Where are the computing resources? | In computing centres distributed across different sites, countries and continents. | The cloud provider's private data centres which are often centralized in a few locations with excellent network connections and cheap electrical power. |
| Why use them? | - You don`t need to buy or maintain your own large computer centre<br>- You can complete more work more quickly and tackle more difficult problems.<br>- You can share data with your distributed team in a secure way. | - You don`t need to buy or maintain your own personal computer centre - You can quickly access extra resources during peak work periods |
| What are they useful for? | Grids were designed to handle large sets of limited duration jobs that produce or use large quantities of data (e.g. the LHC and life sciences) | Clouds best support long term services and longer running jobs (E.g. facebook.com) |
| How do they work? | Grids are an **open source** technology.<br>Resource users and providers alike can understand and contribute to the management of their grid | Clouds are a **proprietary** technology.<br>Only the resource provider knows exactly how their cloud manages data, job queues, security requirements and so on. |
| Benefits? | - **Collaboration:** grid offers a federated platform for distributed and collective work.<br>- **Ownership :** resource providers maintain ownership of the resources they contribute to the grid<br>- **Transparency:** the technologies used are open source, encouraging trust and transparency.<br>- **Resilience:** grids are located at multiple sites, reducing the risk in case of a failure at one site that removes significant resources from the infrastructure. | - **Flexibility:** users can quickly outsource peaks of activity without long term commitment<br>- **Reliability:** provider has financial incentive to guarantee service availability (Amazon, for example, can provide user rebates if availability drops below 99.9%)<br>- **Ease of use:** relatively quick and easy for non-expert users to get started but setting up sophisticated virtual machines to support complex applications is more difficult. |

| | | |
|---|---|---|
| Drawbacks? | - **Reliability:** grids rely on distributed services maintained by distributed staff, often resulting in inconsistency in reliability across individual sites, although the service itself is always available.<br>- **Complexity:** grids are complicated to build and use, and currently users require some level of expertise.<br>- **Commercial:** grids are generally only available for not-for-profit work, and for proof of concept in the commercial sphere | - **Generality:** clouds do not offer many of the specific high-level services currently provided by grid technology. - **Security:** users with sensitive data may be reluctant to entrust it to external providers or to providers outside their borders.<br>- **Opacity:** the technologies used to guarantee reliability and safety of cloud operations are not made public. - **Rigidity:** the cloud is generally located at a single site, which increases risk of complete cloud failure.<br>- **Provider lock-in:** there's a risk of being locked in to services provided by a very small group of suppliers. |
| When? | The concept of grids was proposed in 1995. The Open science grid (OSG) started in 1995 The EDG (European Data Grid) project began in 2001. | In the late 1990`s Oracle and EMC offered early private cloud solutions . However the term cloud computing didn't gain prominence until 2007. |