Department of Distance Education

Punjabi University, Patiala

Class : B.A. III (Computer Applications) Semester : 6

Paper : (BAP 303) INTRODUCTION TO COMPUTER NETWORK AND INTERNET PROGRAMMING

Medium : English Unit : I

Lesson No.

Department website : www.pbidde.org

Lesson No. 1.1 **Author : Kanwal Preet Singh**

Introduction to Computer Networks

1.1.1 Introduction

In this day and age, networks are everywhere. The Internet has also revolutionized not only the computer world, but the lives of millions in a variety of ways even in the "real world". We tend to take for granted that computers should be connected together. In fact, these days, whenever I have two computers in the same room, I have a difficult time ***not*** connecting them together. In approaching any discussion of networking, it is very useful to take a step back and look at networking from a high level. What is it, exactly, and why is it now considered so important that it is assumed that most PCs and other devices should be networked? In this section, we will have a quick introduction to networking, discussing what it is all about in general terms. I begin by defining networking in the most general terms. I then place

networking in an overall context by describing some of its advantages and benefits, as well as some of its disadvantages and costs.

1.1.2 Objective

After reading the chapter, you will be able to understand

- Basics of Computer networks
- Uses of Computer networks
- Network Hardware
- Network Software

1.1.3 What Is Networking?

A network is simply a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate. Networking is the term that describes the processes involved in designing, implementing, upgrading, managing and otherwise working with networks and network technologies.

Networks are used for an incredible array of different purposes. In fact, the definitions above are so simple for the specific reason that networks can be used so broadly, and can allow such a wide variety of tasks to be accomplished. While most people learning about networking focus on the interconnection of PCs and other “true” computers, you use various types of networks every day. Each time you pick up a phone, use a credit card at a store, get cash from an ATM machine, or even plug in an electrical appliance, you are using some type of network.

In fact, the definition can even be expanded beyond the world of technology altogether: I'm sure you've heard the term “networking” used to describe the process of finding an employer or employee by talking to friends and associates. In this case too, the idea is that independent units are connected together to share information and cooperate.

The widespread networking of personal computers is a relatively new phenomenon. For the first decade or so of their existence, PCs were very much “islands unto themselves”, and were rarely connected together. In the early 1990s, PC networking began to grow in popularity as businesses realized the advantages that networking could provide. By the late 1990s, networking in homes with two or more PCs started to really take off as well.

This interconnection of small devices represents, in a way, a return to the “good old days” of mainframe computers. Before computers were small and personal, they were large and centralized machines that were shared by many users operating remote terminals. While having all of the computer power in one place had many disadvantages, one benefit was that all users were connected because they shared the central computer.

Individualized PCs took away that advantage, in favor of the benefits of independence. Networking attempts to move computing into the middle ground, providing PC users with the best of both worlds: the independence and flexibility of personal computers, and the connectivity and resource sharing of mainframes. in fact, networking is today considered so vital that it's hard to conceive of an organization with two or more computers that would not want to connect them together.

1.1.4 Uses of Computer Network

Here are some of the specific advantages or uses generally associated with networking:

- **Connectivity and Communication:** Networks connect computers and the users of those computers. Individuals within a building or work group can be connected into *local area networks (LANs)*; LANs in distant locations can be interconnected into larger *wide area networks (WANs)*. Once connected, it is possible for network users to communicate with each other using technologies such as electronic mail. This makes the transmission of business (or non-business) information easier, more efficient and less expensive than it would be without the network.
- **Data Sharing:** One of the most important uses of networking is to allow the sharing of data. Before networking was common, an accounting employee who wanted to prepare a report for her manager would have to produce it on his PC, put it on a floppy disk, and then walk it over to the manager, who would transfer the data to her PC's hard disk. (This sort of "shoe-based network" was sometimes sarcastically called a "sneakernet".) True networking allows thousands of employees to share data much more easily and quickly than this. More so, it makes possible applications that rely on the ability of many people to access and share the same data, such as databases, group software development, and much more. Intranets and extranets can be used to distribute corporate information between sites and to business partners.
- **Resource/Hardware Sharing:** Networks facilitate the sharing of hardware devices. For example, instead of giving each of 10 employees in a department an expensive color printer (or resorting to the "sneakernet" again), one printer can be placed on the network for everyone to share.
- **Internet Access:** The Internet is itself an enormous network, so whenever you access the Internet, you are using a network. The significance of the Internet on modern society is hard to exaggerate, especially for those of us in technical fields.
- **Internet Access Sharing:** Small computer networks allow multiple users to share a single Internet connection. Special hardware devices allow the bandwidth of the connection to be easily allocated to various individuals as they

need it, and permit an organization to purchase one high-speed connection instead of many slower ones.

- **Data Security and Management:** In a business environment, a network allows the administrators to much better manage the company's critical data. Instead of having this data spread over dozens or even hundreds of small computers in a haphazard fashion as their users create it, data can be centralized on shared servers. This makes it easy for everyone to find the data, makes it possible for the administrators to ensure that the data is regularly backed up, and also allows for the implementation of security measures to control who can read or change various pieces of critical information.
- **Performance Enhancement and Balancing:** Under some circumstances, a network can be used to enhance the overall performance of some applications by distributing the computation tasks to various computers on the network.
- **Entertainment:** Networks facilitate many types of games and entertainment. The Internet itself offers many sources of entertainment, of course. In addition, many multi-player games exist that operate over a local area network. Many home networks are set up for this reason, and gaming across wide area networks (including the Internet) has also become quite popular. Of course, if you are running a business and have easily-amused employees, you might insist that this is really a ***disadvantage*** of networking and not an advantage!

1.1.4 Disadvantages of Installing a School Network

- **Expensive to Install**. Although a network will generally save money over time, the initial costs of installation can be prohibitive. Cables, network cards, and software are expensive, and the installation may require the services of a technician.
- **Hardware and Software Management and Administration Costs:** In all but the smallest of implementations, ongoing maintenance and management of the network requires the care and attention of an IT professional. In a smaller organization that already has a system administrator, a network may fall within this person's job responsibilities, but it will take time away from other tasks. In more substantial organizations, a network administrator may need to be hired, and in large companies an entire department may be necessary**.**
- **Requires Administrative Time**. Proper maintenance of a network requires considerable time and expertise. Many schools have installed a network, only to find that they did not budget for the necessary administrative support.
- **Data Security Concerns:** If a network is implemented properly, it is possible to greatly improve the security of important data. In contrast, a poorly-secured network puts critical data at risk, exposing it to the potential problems associated with hackers, unauthorized access and even sabotage.

To tackle with such problems, strong data security measures are required like antivirus, fire wall etc.

- **File Server May Fail**. Although a file server is no more susceptible to failure than any other computer, when the files server "goes down," the entire network may come to a halt. When this happens, the entire school may lose access to necessary programs and files.
- **Cables May Break**. The Topology section of this tutorial presents information about the various configurations of cables. Some of the configurations are designed to minimize the inconvenience of a broken cable; with other configurations, one broken cable can stop the entire network.

1.1.5 Network Hardware

Networking hardware includes all computers, peripherals, interface cards and other equipment needed to perform data-processing and communications within the network. This section provides information on the following components:

- File Servers
- Workstations
- Network Interface Cards
- Concentrators/Hubs
- Repeaters
- Bridges
- Routers

1.1.5.1 File Servers

A file server stands at the heart of most networks. It is a very fast computer with a large amount of RAM and storage space, along with a fast network interface card. The network operating system software resides on this computer, along with any software applications and data files that need to be shared.

The file server controls the flow of information between the nodes on a network. For example, it may be asked to send a word processor program to one workstation, receive a database file from another workstation, and store an e-mail message during the same time period. This requires a computer that can store a lot of information and share it very quickly. File servers should have at least the following characteristics:

- 75 megahertz or faster microprocessor (Pentium, PowerPC)
- A fast hard drive with at least four gigabytes of storage
- A RAID (Redundant Array of Inexpensive Disks) to preserve data after a disk casualty
- A tape back-up unit
- Numerous expansion slots
- Fast network interface card
- At least of 512 MB of RAM

1.1.5.2 Workstations

All of the computers connected to the file server on a network are called workstations. A typical workstation is a computer that is configured with a network interface card, networking software, and the appropriate cables. Workstations do not necessarily need floppy disk drives or hard drives because files can be saved on the file server. Almost any computer can serve as a network workstation.

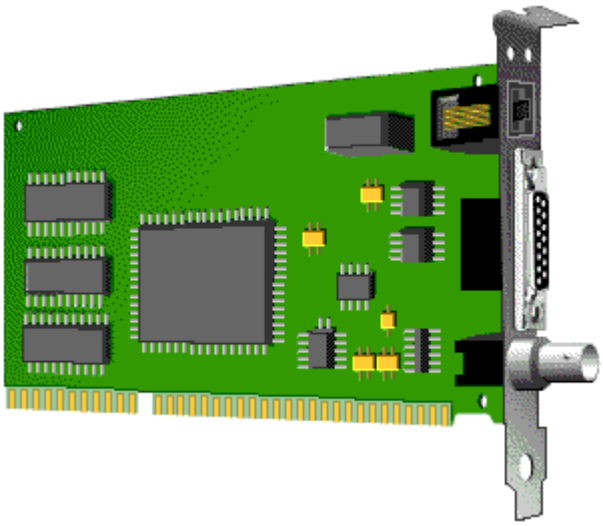
1.1.5.3 Network Interface Cards

The network interface card (NIC) provides the physical connection between the network and the computer workstation. Every NIC have a 48 bit long unique serial number which is referred as the MAC address of the machine. This MAC address can also be referred as the physical address of the machine over the network. Most NICs are internal, with the card fitting into an expansion slot inside the computer. Some computers, such as Mac Classics, use external boxes which are attached to a serial port or a SCSI port. Laptop computers generally use external LAN adapters connected to the parallel port or network cards that slip into a PCMCIA slot. Network interface cards are a major factor in determining the speed and performance of a network. It is a good idea to use the fastest network card available for the type of workstation you are using.

The three most common network interface connections are Ethernet cards, LocalTalk connectors, and Token Ring cards. According to a International Data Corporation study, Ethernet is the most popular, followed by Token Ring and LocalTalk (Sant'Angelo, R. (1995). NetWare Unleashed, Indianapolis, IN: Sams Publishing).

1.1.5.4 Ethernet Cards

Ethernet cards are usually purchased separately from a computer, although many computers (such as the Macintosh) now include an option for a pre-installed Ethernet card. Ethernet cards contain connections for either coaxial or twisted pair cables (or both) (See fig. 1). If it is designed for coaxial cable, the connection will be BNC. If it is designed for twisted pair, it will have a RJ-45 connection. Some Ethernet cards also contain an AUI connector. This can be used to attach coaxial, twisted pair, or fiber optics cable to an Ethernet card. When this method is used there is always an external transceiver attached to the workstation.



1.1.5.5 Token Ring Cards

Token Ring network cards look similar to Ethernet cards. One visible difference is the type of connector on the back end of the card. Token Ring cards generally have a nine pin DIN type connector to attach the card to the network cable.

1.1.5.6 Concentrators/Hubs

A concentrator is a device that provides a central connection point for cables from workstations, servers, and peripherals. In a star topology, twisted-pair wire is run from each workstation to a central concentrator. Hubs are multislot concentrators into which can be plugged a number of multi-port cards to provide additional access as the network grows in size. Some concentrators are passive, that is they allow the signal to pass from one computer to another without any change. Most concentrators are active, that is they electrically amplify the signal as it moves from one device to another. Active concentrators are used like repeaters to extend the length of a network. Concentrators are:

- Usually configured with 8, 12, or 24 RJ-45 ports
- Often used in a star or star-wired ring topology
- Sold with specialized software for port management
- Also called hubs
- Usually installed in a standardized metal rack that also may store netmodems, bridges, or routers

1.1.5.7 Repeaters : Used between similar networks

When a signal travels along a cable, it tends to lose strength and becomes weak. A repeater is a device that boosts a network's signal as it passes through. The repeater does this by electrically amplifying the signal it receives and rebroadcasting it.

Repeaters can be separate devices or they can be incorporated into a concentrator. They are used when the total length of your network cable exceeds the standards set for the type of cable being used.

A good example of the use of repeaters would be in a local area network using a star topology with unshielded twisted-pair cabling. The length limit for unshielded twisted-pair cable is 100 meters. The most common configuration is for each workstation to be connected by twisted-pair cable to a multi-port active concentrator. The concentrator regenerates all the signals that pass through it allowing for the total length of cable on the network to exceed the 100 meter limit.

1.1.5.8 Bridges : Used to connect similar Networks

A bridge is a device that allows you to segment a large network into two smaller, more efficient networks. If you are adding to an older wiring scheme and want the new network to be up-to-date, a bridge can connect the two.

A bridge monitors the information traffic on both sides of the network so that it can pass packets of information to the correct location. Most bridges can "listen" to the network and automatically figure out the address of each computer on both sides of the bridge. The bridge can inspect each message and, if necessary, broadcast it on the other side of the network.

The bridge manages the traffic to maintain optimum performance on both sides of the network. You might say that the bridge is like a traffic cop at a busy intersection during rush hour. It keeps information flowing on both sides of the network, but it does not allow unnecessary traffic through. Bridges can be used to connect different types of cabling, or physical topologies. They must, however, be used between networks with the same protocol.

1.1.5.9 Routers : Used in inter-networking between LANs of different protocols

A router translates information from one network to another; it is similar to a superintelligent bridge. Routers select the best path to route a message, based on the destination address and origin. The router can direct traffic to prevent head-on collisions, and is smart enough to know when to direct traffic along back roads and shortcuts.

While bridges know the addresses of all computers on each side of the network, routers know the addresses of computers, bridges, and other routers on the network. Routers can even "listen" to the entire network to determine which sections are busiest -- they can then redirect data around those sections until they clear up.

If you have a school LAN that you want to connect to the Internet, you will need to purchase a router. In this case, the router serves as the translator between the information on your LAN and the Internet. It also determines the best route to send the data over the Internet. Routers can:

- Direct signal traffic efficiently

- Route messages between any two protocols
- Route messages between linear bus, star, and star-wired ring topologies
- Route messages across fiber optic, coaxial, and twisted-pair cabling

1.1.6 Network Operating Systems

Unlike operating systems, such as DOS and Windows95, that are designed for single users to control one computer, network operating systems (NOS) coordinate the activities of multiple computers across a network. The network operating system acts as a director to keep the network running smoothly.

The two major types of network operating systems are:

- Peer-to-Peer
- Client/Server

Peer-to-Peer

Peer-to-peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. However, they do not have a file server or a centralized management source (See fig. 1). In a peer-to-peer network, all computers are considered equal; they all have the same abilities to use the resources available on the network. Peer-to-peer networks are designed primarily for small to medium local area networks. AppleShare and Windows for Workgroups are examples of programs that can function as peer-to-peer network operating systems.

Fig.1. Peer-to-peer network

Advantages of a peer-to-peer network:

- Less initial expense - No need for a dedicated server.
- Setup - An operating system (such as Windows 95) already in place may only need to be reconfigured for peer-to-peer operations.

Disadvantages of a peer-to-peer network:

- Decentralized - No central repository for files and applications.
- Security - Does not provide the security available on a client/server network.

Client/Server

Client/server network operating systems allow the network to centralize functions and applications in one or more dedicated file servers (See fig. 2). The file servers become the heart of the system, providing access to resources and providing security. Individual workstations (clients) have access to the resources available on the file servers. The network operating system provides the mechanism to integrate all the components of the network and allow multiple users to simultaneously share the same resources irrespective of physical location. Novell Netware and Windows NT Server are examples of client/server network operating systems.

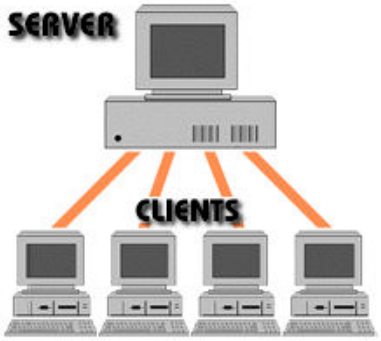


Fig.2. Client/server network

Advantages of a client/server network:

- Centralized - Resources and data security are controlled through the server.
- Scalability - Any or all elements can be replaced individually as needs increase.
- Flexibility - New technology can be easily integrated into system.
- Interoperability - All components (client/network/server) work together.
- Accessibility - Server can be accessed remotely and across multiple platforms.

Disadvantages of a client/server network:

- Expense - Requires initial investment in dedicated server.
- Maintenance - Large networks will require a staff to ensure efficient operation.
- Dependence - When server goes down, operations will cease across the network.

Examples of network operating systems

The following list includes some of the more popular peer-to-peer and client/server network operating systems.

- Microsoft Windows Server 2008
- MAC OSX
- Novell Netware
- Microsoft Windows NT Server
- Microsoft Windows NT Work Station

1.1.7 Summary

A network is simply a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate. Some of the specific advantages or uses generally associated with networking are: data sharing, hardware sharing, internet access, etc. Networking hardware includes all computers, peripherals, interface cards and other equipment needed to perform data-processing and communications within the network. Unlike operating systems, such as DOS and Windows, that are designed for single users to control one computer, network operating systems (NOS) coordinate the activities of multiple computers across a network. The network operating system acts as a director to keep the network running smoothly. The two major types of network operating systems are: Peer-to-Peer and Client/Server.

1.1.8 Review Questions

1. What is a computer network? Why do we need a network?
2. Explain the different types of network hardware.
3. What is a network Operating System? Explain different types of network Operating systems.

1.1.9 Suggested Readings

1. Computer Networks by Andrew S. Tanenbaum
2. Data and Computer Communication by William Stallings
3. Computer networks & internet by D.E. Comer, Pearson Education

Lesson No. 1.2 **Author : Kanwal Preet Singh**

Network Goals and Topologies

1.2.1 Introduction

The main goals of computer network are resource sharing and providing communication. There are some other goals also and are discussed in this chapter. The major applications of networking are in marketing, finance, telecommunication, email, cell phones, etc. Network models provide a standard framework to use when designing complex communication systems. The two types of network models – peer to peer and client server are discussed in the chapter. A topology refers to both the physical and logical layout of a network. The different types of topologies are discussed in the chapter.

1.2.2 Objective

After reading the chapter, you will be able to understand:

- Network Goals
- Network Applications
- Network models
- Network Topologies

1.2.3 Network goals

- The main goal of networking is "**Resource sharing**", and it is to make all programs, data and equipment available to anyone on the network without the regard to the physical location of the resource and the user.
- A second goal is to provide **high reliablity** by having alternative sources of supply. For example, all files could be replicatied on two or three machines, so if one of them is unavailable, the other copies could be available.
- Another goal is **saving money.** Small computers have a much better price/performance ratio than larger ones. Mainframes are roughly a factor of ten times faster than the fastest single chip microprocessors, but they cost thousand times more. This imbalance has caused many system designers to build systems consisting of powerful personal computers, one per user, with data kept on one or more shared **file server** machines. This goal leads to networks with many computers located in the same building. Such a network is called a **LAN(local area network).**
- Another closely related goal is to increase the systems perfomance as the work load increases by just adding more processors. With central mainframes, when the system is full, it must be replaced by a larger one, usually at great expense and with even greater disruption to the users.
- Computer networks provide a powerful communication medium. A file that was updated/modified on a network, can be seen by the other users on the network immediately.

1.2.4 Applications of Networks

Data networks have become an indispensible part of business, industry and entertainment. Some of the applications of networks in different fields are as follows:

- **Marketing and Sales:** Computer networks are used extensively in both marketing and sales organizations. Marketing professionals use them to collect, exchange and analyze data relating to customer needs and product development cycles. Sales applications include teleshopping, which uses order-entry computers or telephones connected to an order-processing network, and on-line reservation services for hotels, airlines, railways, etc.
- **Financial Services:** Now-a-days financial services are totally dependent on computer networks. Applications include credit history searches, foreign exchange and investment services, and electronic funds transfer (EFT), which allows a user to transfer money without going into a bank (e.g. ATMs).
- **Manufacturing:** Computer networks, these days are used in many aspects of manufacturing, including the manufacturing process itself. Two applications

that use networks to provide essential services are computer-assisted design (CAD) and computer-assisted manufacturing (CAM), both of which allow multiple users to work on a project simultaneously.

- **Information Services:** They provide connections to the Internet and other information services which includes bulletin boards and data banks.
- **Electronic Mail (e-mail or Email):** E-mail is the forwarding of electronic files to an electronic post office for the recipient to pick up.
- **Groupware**: It is the latest network application; it allows user groups to share documents, schedules databases, etc.
- **Teleconferencing:** It allows people in different regions to "attend" meetings using telephone lines.
- **Telecommuting:** It allows employees to perform office work at home by "Remote Access" to the network.
- **Videotext**: It is the capability of having a 2 way transmission of picture and sound. Games like Doom, Hearts, distance education lectures, etc use this technology.
- **Cellular Telephones:** In the past, two parties wishing to use the services of the telephone companies had to be linked by a fixed physical connection. Today's cellular networks make it possible to maintain wireless phone connections even while travelling over large distances.
- **Cable Television:** Future services provided by cable television networks may include video on request, as well as financial and communication services currently provided by telephone companies and computer networks.

1.2.5 Network Models

Network models provide a standard framework to use when designing complex communication systems. These models outline standard issues associated with network design and allow the designer to solve each issue separately, modularizing the solution. A network model is a framework to use, not a concrete method. It is up to the implementers to decide which parts of the model are relevant to accomplish their goals. Different wired networks can be described functionally as belonging to one of these two broad categories:

1. Peer-to-peer networks
2. Client/server networks

Let us look into the details of each of these models now.

Peer-to-peer Networks

A peer-to-peer network is a decentralized network model offering no centralized storage of data or centralized control over the sharing of files or resources. All systems on a peer-to-peer network can share the resources on their local computer as well as use resources of other systems.

Peer-to-peer networks are cheaper and easier to implement than client/server networks, making them an ideal solution for environments in which budgets are a concern. The peer-to-peer model does not work well with large numbers of computer systems. As a peer-to-peer network grows, it becomes increasingly complicated to navigate and access files and resources connected to each computer because they are distributed throughout the network. Further, the lack of centralized data storage makes it difficult to locate and back up key files.

Peer-to-peer networks are typically found in small offices or in residential settings where only a limited number of computers will be attached and only a few files and resources shared. A general rule of thumb is to have no more than 10 computers connected to a peer-to-peer network.

Advantages:

- Easy to install and setup costs are relatively low.

Disadvantages:

- They do not expandability and centralized management.
- There is no central repository for files and applications.
- It does not provide the security as available in a client/server network.

Client/Server Networking Model

The client/server networking model is, without question, the most widely implemented model and the one which are most likely to encounter when working in real-world environments. The advantages of the client/server system stem from the fact that it is a centralized model. It allows for centralized network management of all network services, including user management, security, and backup procedures.

A client/server network often requires technically skilled personnel to implement and manage the network. The cost of a dedicated server hardware and software increase the cost of the client/server model. Despite this, the advantages of the centralized management, data storage, administration, and security make it the network model of choice.

Advantages:

- Centralized - Resources and data security can be controlled through the server.
- Interoperability - All components (client/network/server) work together.
- Accessibility - Server can be accessed remotely and across multiple Operating systems, such as Windows XP, Windows NT, and Macintosh.

Disadvantages:

- Maintenance - They can support thousands of clients, hence requires a staff to ensure efficient operation.
- Dependence - When server goes down, operations across the network will be affected.

1.2.6 Network Topologies

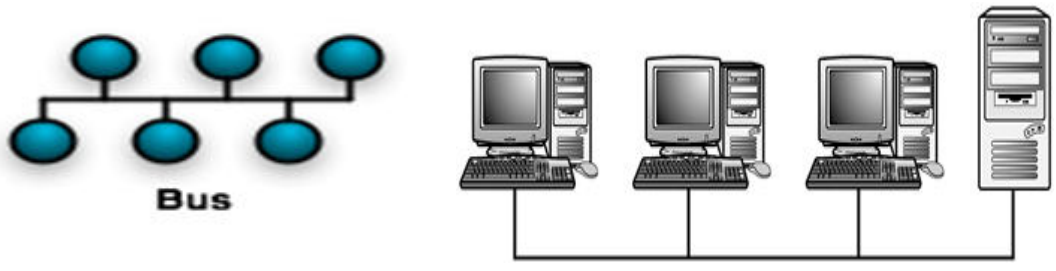
A topology refers to both the physical and logical layout of a network. The physical topology of a network refers to the actual layout of the computer cables and other network devices. The logical topology of a network, on the other hand, refers to the way in which the network appears to the devices that use it. There are five different Networking Topologies :

a) Bus
b) Star
c) Ring
d) Mesh
e) Tree.

When networks are design using multiple topologies it is called Hybrid Networks, this concept is usually utilized in complex networks were larger number of computer clients are required.

1.2.6.1 Bus Topology

Bus topology is one the easiest topologies to install, it does not require lots of cabling. There are two most popular Ethernet cable types which are used in this topology they are 10Base-2 and 10BaseT. Bus topology based networks works with very limited devices. It performs fine as long as computer count remain within 12 – 15, problems occurs when number of computer increases. Bus topology uses one common cable (backbone) to connect all devices in the network in linear shape. Network interface cards of all network devices are attached to single communication medium backbone cable. When any computer sends out message in the network it is broadcasted in the entire network but only intended computer accepts the message and process it. Bus topology provide simplicity to the network, however there is big disadvantage of this topology, if main single network cable somehow gets damaged, it will shut down the entire network no computer will run on network and no communication can be made among computers until backbone cable is replaced.



Bus Topology

Advantages and Disadvantages of the Bus Topology

Advantages

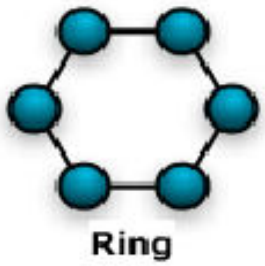
- Compared to other topologies, a bus is cheap and easy to implement.
- Does not use any specialized network equipment.
- Requires less cable than other topologies.

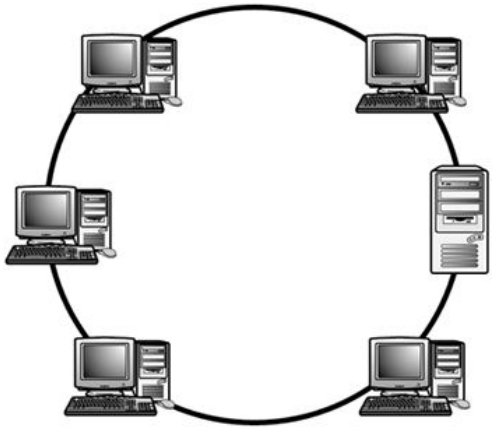
Disadvantages

- Because all systems on the network connect to a single backbone, a break in the cable will prevent all systems from accessing the network.
- There might be network disruption when computers are added or removed.
- Difficult to troubleshoot.

1.2.6.2 Ring Topology

Ring topology is one of the old ways of building computer network design and it is pretty much obsolete. FDDI, SONET or Token Ring technologies are used to build ring technology. It is not widely popular in terms of usability but incase if you find it any where it will mostly be in schools or office buildings. In ring network topology computers and other networking devices are attached to each other in such a way that they have devices adjacent to each other (Left and right side). All messages travel in the same direction either clockwise or anticlockwise. In case of failure of any device or cable the whole network will be down and communication will not be possible.





Ring Topology

Advantages and Disadvantages of the Ring Topology:

Advantages :

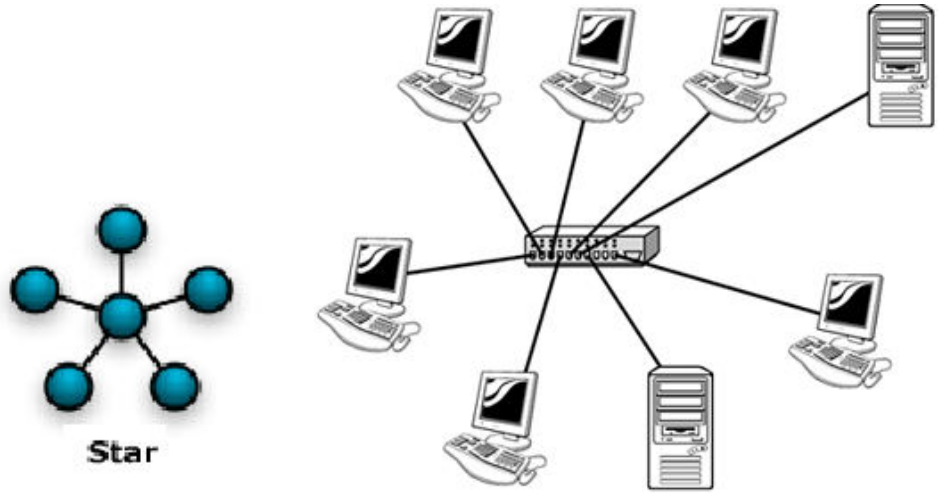
- Cable faults are easily located, making troubleshooting easier.
- Ring networks are moderately easy to install.

Disadvantages :

- Expansion to the network can cause network disruption.
- A single break in the cable can disrupt the entire network.

1.2.6.3 Star Topology

This is the most commonly used network topology design you will come across in LAN computer networks. In Star, all computers are connected to central device called hub, router or switches using Unshielded Twisted Pair (UTP) or Shielded Twisted Pair cables. In star topology, we require more connecting devices like routers, cables unlike in bus topology where entire network is supported by single backbone. All peripheral nodes may thus communicate with all others by transmitting to, and receiving from, the central node only. The most practical point of Star topology success is that the entire network does not go down in case of failure of a computer or cable or device, it will only affect the computer whose wire failed rest of the network will be working fine. However, in case of failure of central communication device such as Hub, Router or Switch the entire network will collapse. Star topology is widely used in homes, offices and in buildings because of its commercial success.



Star Topology

Advantages and Disadvantages of the Star Topology:

Advantages

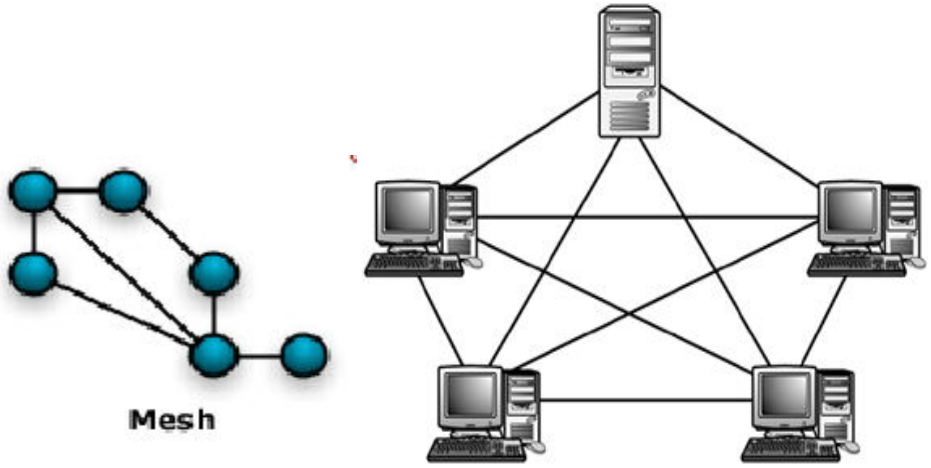
- Star networks are easily expanded without disruption to the network.
- Easy to troubleshoot and isolate problems.
- Cable failure affects only a single user.

Disadvantages

- A central connecting device allows for a single point of failure.
- Requires more cable than most of the other topologies.
- More difficult than other topologies to implement.

1.2.6.4 Mesh Topology

Mesh topology is designed over the concept of routing. Basically it uses router to choose the shortest distance for the destination. In topologies like star, bus etc, message is broadcasted to entire network and only intended computer accepts the message, but in mesh the message is only sent to the destination computer which finds its route it self with the help of router. Internet is based on mesh topology. Routers plays important role in mesh topology, routers are responsible to route the message to its destination address or computer. When every device is connected to every other device it is known as full mesh topology and if every device is connected indirectly to each other then it is called partial mesh topology.



Mesh Topology

Advantages and Disadvantages of the Mesh Topology

Advantages

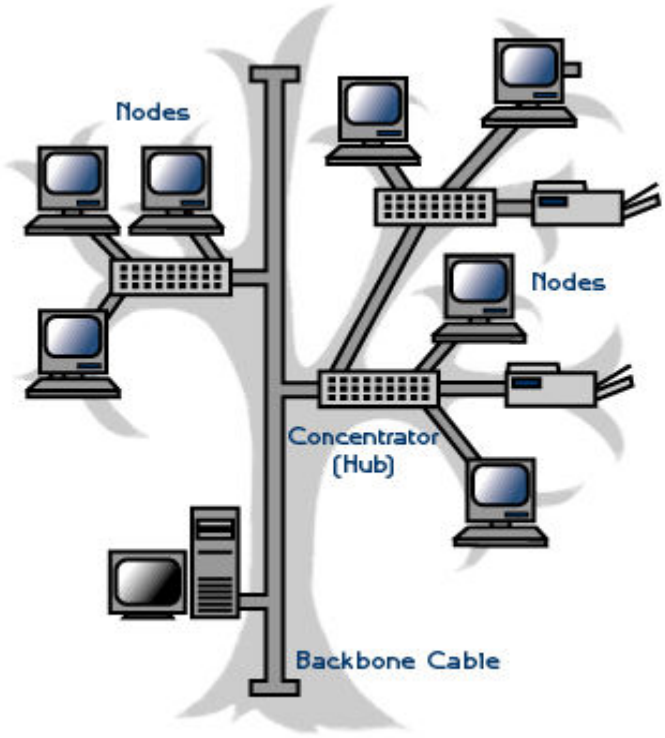
- Provides redundant paths between devices
- The network can be expanded without disruption to current users.

Disadvantages

- Requires more cable than the other LAN topologies.
- Complicated implementation.

1.2.6.5 Tree Topology

Just as name suggest, the network design is little confusing and complex to understand at first but if we have better understanding of Star and Bus topologies then Tree is very simple. Tree topology is basically the mixture of many Star topology designs connected together using bus topology. Devices like Hub can be directly connected to Tree bus and each hub performs as root of a tree of the network devices. Tree topology is very dynamic in nature and it holds potential of expandability of networks far better than other topologies like Bus and Star.



Advantages and Disadvantages of the Mesh Topology

Advantages :

- Potential of expandability of network is far better than other topologies like Bus and Star.
- The network can be expanded without disruption to current users.

Disadvantages :

- Because all systems on the network connect to a single backbone, a break in the cable will prevent all systems from accessing the network.
- Complicated implementation.

1.2.7 Summary

The main goals of computer network are resource sharing, providing communication, increasing reliability, saving money, etc. The major applications of networking are in marketing, finance, telecommunication, email, cell phones, etc. Network models provide a standard framework to use when designing complex communication systems. The two types of network models are peer to peer and client server. A peer-to-peer network is a decentralized network model offering no centralized storage of data or centralized control over the sharing of files or resources. All systems on a peer-to-peer network can share the resources on their local computer as well as use resources of other systems. The client-server model allows for centralized network

management of all network services, including user management, security, and backup procedures. A topology refers to both the physical and logical layout of a network. The physical topology of a network refers to the actual layout of the computer cables and other network devices. The logical topology of a network, on the other hand, refers to the way in which the network appears to the devices that use it. There are five different Networking Topologies: Bus, Star, Ring, Mesh and Tree.

1.2.8 Review Questions

4. What are the goals of computer network?
5. Explain the major applications of Computer network.
6. What is a network Topology? Explain different types of network topologies.

1.2.9 Suggested Readings

4. Computer Networks by Andrew S. Tanenbaum
5. Data and Computer Communication by William Stallings
6. Computer networks & internet by D.E. Comer, Pearson Education

Lesson No. 1.3 **Author : Kanwal Preet Singh**

Transmission Media

1.3.1 Introduction

On any network, the various entities must communicate through some form of media. Human communication requires some sort of media, whether it is technology based (as are telephone wires) or whether it simply involves the use of our senses to detect sound waves propagating through the air. Likewise, computers can communicate through cables, light, and radio waves. Transmission media enable computers to send and receive messages but, as in human communication, do not guarantee that the messages will be understood. This chapter discusses some of the most common network transmission media. One broad classification of this transmission media is known as *bounded media*, or cable media. This includes cable types such as coaxial cable, shielded twisted-pair cable, unshielded twisted-pair cable, and fiber-optic cable. The bounded or guided media is discussed in this chapter. Another type of media is known as *unbounded media*; these media include all forms of wireless communications. These are discussed in the next chapter.

1.3.2 Objective

After reading the chapter, you will be able to understand:

- Characteristics of Transmission Media
- Different types of transmission mesdia

1.3.3 Transmission Media Characteristics

Each type of transmission media has special characteristics that make it suitable for a specific type of service. You should be familiar with these characteristics for each type of media:

- Cost
- Installation requirements
- Bandwidth
- Band usage (baseband or broadband)
- Attenuation
- Immunity from electromagnetic interference

These characteristics are all important. When you design a network for a company, all these factors play a role in the decision concerning what type of transmission media should be used.

Cost

One main factor in the purchase decision of any networking component is the cost. Often the fastest and most robust transmission media is desired, but a network designer must often settle for something that is slower and less robust, because it more than suffices for the business solution at hand. The major deciding factor is almost always price. It is a rare occasion in the field that the sky is the limit for installing a network. As with nearly everything else in the computer field, the fastest technology is the newest, and the newest is the most expensive. Over time, economies of scale bring the price down, but by then, a newer technology comes along.

Installation Requirements

Installation requirements typically involve two factors. One is that some transmission media require skilled labor to install. Bringing in a skilled outside technician to make changes to or replace resources on the network can bring about undue delays and costs. The second has to do with the actual physical layout of the network. Some types of transmission media install more easily over areas where people are spread out, whereas other transmission media are easier to bring to clusters of people or a roaming user.

Bandwidth

In computer networking, the term *bandwidth* refers to the measure of the capacity of a medium to transmit data. A medium that has a high capacity, for example, has a high bandwidth, whereas a medium that has limited capacity has a low bandwidth.

Using the Term Bandwidth: The term "bandwidth" also has another meaning. In the communications industry, bandwidth refers to the range of available frequencies between the lower frequency limit and the upper frequency limit. Frequencies are

measured in Hertz (Hz), or cycles per second. The bandwidth of a voice telephone line is 400-4,000Hz, which means that the line can transmit signals with frequencies ranging from 400 to 4,000 cycles per second.

Bandwidth can be best explained by using water hoses as an analogy. If a half-inch garden hose can carry water flow from a trickle up to two gallons per minute, then that hose can be said to have a bandwidth of two gallons per minute. A four-inch fire hose, however, might have a bandwidth that exceeds 100 gallons per minute.

Data transmission rates are frequently stated in terms of the bits that can be transmitted per second. An Ethernet LAN theoretically can transmit 10 million bits per second and has a bandwidth of 10 megabits per second (Mbps). The bandwidth that a cable can accommodate is determined in part by the cable's length. A short cable generally can accommodate greater bandwidth than a long cable, which is one reason all cable designs specify maximum lengths for cable runs. Beyond those limits, the highest-frequency signals can deteriorate, and errors begin to occur in data signals. You can see this by taking a garden hose and snapping it up and down. You can see the waves traveling down the hose get smaller as they get farther from your hand. This loss of the wave's amplitude represents attenuation, or signaldegradation.

NOTE: As you know, everything in computers is represented with 1s and 0s. We use 1s and 0s to represent the bits in the computer. However, be sure to remember that transmission media is measured in megabits per second (Mbps), not megaBYTES per second (MBps). The difference is eight-fold, as there are 8 bits in a byte.

Band Usage (Baseband or Broadband)

The two ways to allocate the capacity of transmission media are with *baseband* and *broadband* transmissions. Baseband devotes the entire capacity of the medium to one communication channel. Broadband enables two or more communication channels to share the bandwidth of the communications medium.

Baseband is the most common mode of operation. Most LANs function in baseband mode, for example. Baseband signaling can be accomplished with both analog and digital signals. Although you might not realize it, you have a great deal of experience with broadband transmissions. Consider, for example, that the TV cable coming into your house from an antenna or a cable provider is a broadband medium. Many television signals can share the bandwidth of the cable because each signal is modulated using a separately assigned frequency. You can use the television tuner to select the frequency of the channel you want to watch. This technique of dividing bandwidth into frequency bands is called frequency-division multiplexing (FDM) and works only with analog signals. Another technique, called time-division multiplexing (TDM), supports digital signals. Both of these types of multiplexing are discussed in the later chapters.

Attenuation

Attenuation is a measure of how much a signal weakens as it travels through a medium. Attenuation is a contributing factor to why cable designs must specify limits in the lengths of cable runs. When signal strength falls below certain limits, the electronic equipment that receives the signal can experience difficulty isolating the original signal from the noise present in all electronic transmissions. The effect is exactly like trying to tune in distant radio signals. Even if you can lock on to the signal on your radio, the sound generally still contains more noise than the sound for a local radio station. Repeaters are used to regenerate signals; hence one solution to deal with attenuation is to add a repeater.

Electromagnetic Interference

Electromagnetic interference (EMI) consists of outside electromagnetic noise that distorts the signal in a medium. When you listen to an AM radio, for example, you often hear EMI in the form of noise caused by nearby motors or lightning. Some network media are more susceptible to EMI than others. *Crosstalk* is a special kind of interference caused by adjacent wires. Crosstalk occurs when the signal from one wire is picked up by another wire. You may have experienced this when talking on a telephone and hearing another conversation going on in the background. Crosstalk is a particularly significant problem with computer networks because large numbers of cables often are located close together, with minimal attention to exact placement.

1.3.4 Types of Transmission Media

Whatever type of network is used, some type of network media is needed to carry signals between computers. There are 2 basic categories of Transmission Media:

- Guided and
- Unguided

Guided Transmission Media uses a "cabling" system that guides the data signals along a specific path. The data signals are bound by the "cabling" system. Guided Media is also known as Bound Media. Cabling is meant in a generic sense in the previous sentences and is not meant to be interpreted as copper wire cabling only.

Unguided Transmission Media consists of a means for the data signals to travel but nothing to guide them along a specific path. The data signals are not bound to a cabling media and as such are often called Unbound Media.

There 3 basic types of Guided Media:

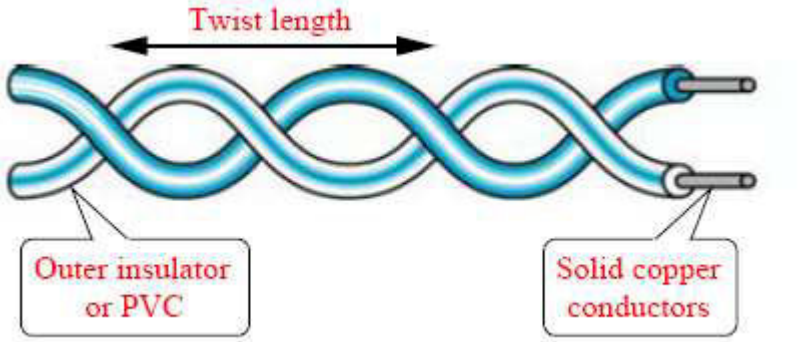
- Twisted Pair
- Coaxial Cable
- Optical Fiber

1.3.5 Twisted-Pair Cable

Twisted-pair cable has become the dominant cable type for all new network designs that employ copper cable. Among the several reasons for the popularity of

twisted-pair cable, the most significant is its low cost. Twisted-pair cable is inexpensive to install and offers the lowest cost per foot of any cable type. Your telephone cable is an example of a twisted-pair type cable.

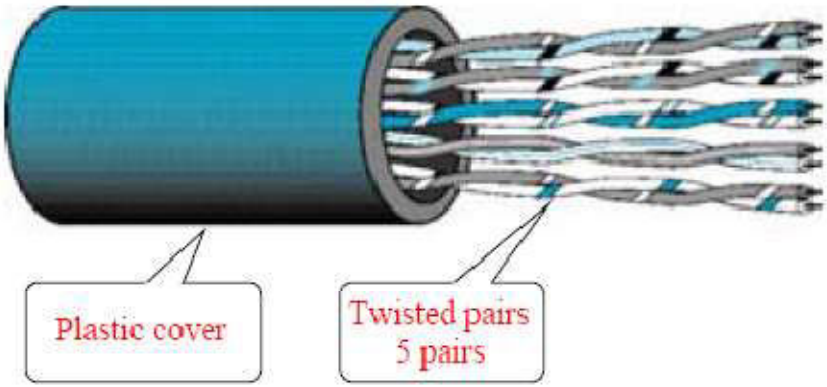
In its simplest form, twisted-pair cable consists of two insulated strands of copper wire twisted around each other.



A number of twisted-pair wires are often grouped together and enclosed in a protective sheath to form a cable. The total number of pairs in a cable varies. The twisting cancels out electrical noise from adjacent pairs and from other sources such as motors, relays, and transformers. The twisting reduces the sensitivity of the cable to EMI and also reduces the tendency of the cable to radiate radio frequency noise that interferes with nearby cables and electronic components, because the radiated signals from the twisted wires tend to cancel each other out. (Antennas, which are purposely designed to radiate radio frequency signals, consist of parallel, non twisted, wires). Twisting of the wires also controls the tendency of the wires in the pair to cause EMI in each other. As noted previously, whenever two wires are in close proximity, the signals in each wire tend to produce crosstalk in the other. Twisting the wires in the pair reduces crosstalk in much the same way that twisting reduces the tendency of the wires to radiate EMI. Two types of twisted-pair cable are used in LANs: unshielded and shielded, as explained in the following section.

Unshielded Twisted-Pair (UTP) Cable

Unshielded twisted-pair cable doesn't incorporate a braided shield into its structure. Traditional UTP cable consists of two insulated copper wires. UTP specifications govern how many twists are permitted per foot of cable; the number of twists allowed depends on the purpose to which the cable will be put. Several twisted pairs can be bundled together in a single cable. These pairs are typically color-coded to distinguish them.



Telephone systems commonly use UTP cabling. Network engineers can sometimes use existing UTP telephone cabling (if it is new enough and of a high enough quality to support network communications) for network cabling. UTP cable is a latecomer to high-performance LANs because engineers only recently solved the problems of managing radiated noise and susceptibility to EMI. Now, however, a clear trend toward UTP is in operation, and all new copper-based cabling schemes are based on UTP.UTP cable is available in the following five grades, or categories:

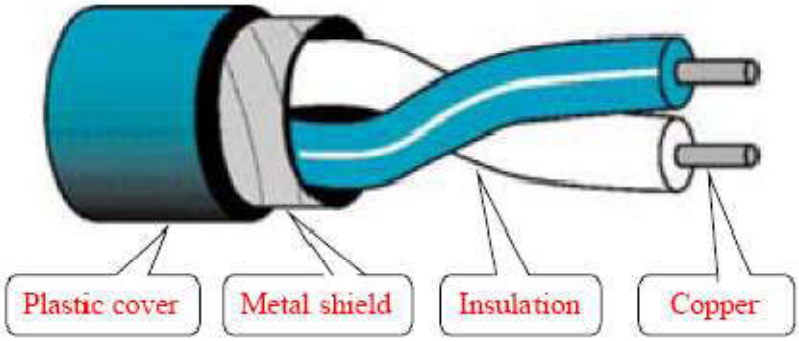
- **Categories 1 and 2:** These voice-grade cables are suitable only for voice and for low data rates (below 4Mbps). Category 1 was once the standard voice-grade cable for telephone systems. The growing need for data-ready cabling systems, however, has caused Categories 1 and 2 cable to be supplanted by Category 3 for new installations.
- **Category 3:** As the lowest data-grade cable, this type of cable generally is suited for data rates up to 10Mbps. Some innovative schemes utilizing new standards and technologies, however, enable the cable to support data rates up to 100Mbps. Category 3, which uses four twisted pairs with three twists per foot, is now the standard cable used for most telephone installations.
- **Category 4:** This data-grade cable, which consists of four twisted-pairs, is suitable for data rates up to 16Mbps.
- **Category 5:** This data-grade cable, which also consists of four twisted-pairs, is suitable for data rates up to 100Mbps. Most new cabling systems for 100Mbps data rates are designed around Category 5 cable.

The prices of the grades of cable increase as you move from Category 1 to Category 5. In a UTP cabling system, the cable is only one component of the system. All connecting devices are also graded, and the overall cabling system supports only the data rates permitted by the lowest-grade component in the system. In other words, if you require a Category 5 cabling system, all connectors and connecting devices must

be designed for Category 5 operation. The installation procedures for Category 5 cable also have more stringent requirements than the lower cable categories. Installers of Category 5 cable require special training and skills to understand these more rigorous requirements. UTP cable offers an excellent balance of cost and performance characteristics

Shielded Twisted-Pair (STP) Cable

Shielded twisted-pair cabling consists of one or more twisted pairs of cables enclosed in a foil wrap and woven copper shielding. Early LAN designers used shielded twisted-pair cable because the shield performed double duty, reducing the tendency of the cable to radiate EMI and reducing the cable's sensitivity to outside interference.



Coaxial and STP cables use shields for the same purpose. The shield is connected to the ground portion of the electronic device to which the cable is connected. A ground is a portion of the device that serves as an electrical reference point, and usually, it is literally connected to a metal stake driven into the ground. A properly grounded shield prevents signals from getting into or out of the cable. Various types of STP cable exist, some that shield each pair individually and others that shield several pairs. The engineers who design a network's cabling system choose the exact configuration.

Applications of Twisted-Pair

The primary applications of twisted-pair are in premises distribution systems, telephony, private branch exchanges (PBXs) between telephone sets and switching cabinets, LANs, and local loops, including both analog telephone lines and broadband DSL.

Advantages and Disadvantages of Twisted-Pair

Twisted-pair has several key advantages:

- **High availability**—More than 1 billion telephone subscriber lines based on twisted-pair have been deployed, and because it's already in the ground, the telephone companies will use it.

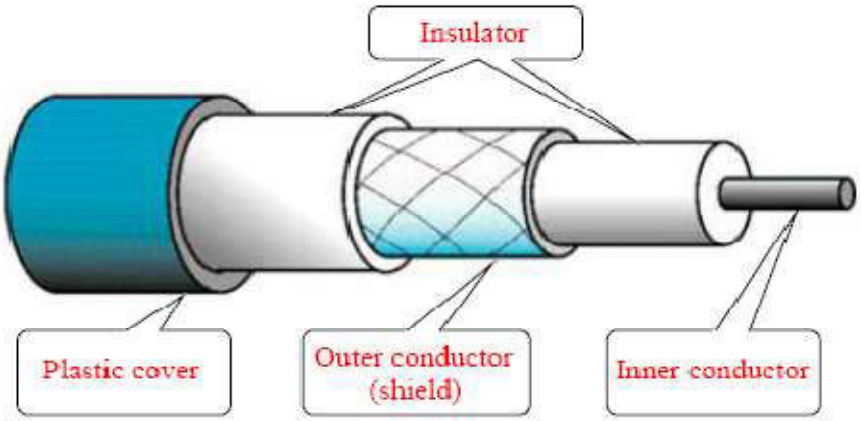
- Less susceptible to electrical interference caused by nearby equipment or cables.
- **Low cost of installation on premises**—The cost of installing twisted-pair on premises is very low.
- **Low cost for local moves, adds, and changes in places**—An individual can simply pull out the twisted-pair terminating on a modular plug and replace it in another jack in the enterprise, without requiring the intervention of a technician. Of course, this assumes that the wiring is already in place; otherwise, there is the additional cost of a new installation.

Twisted-pair has the following disadvantages:

- **Limited frequency spectrum**—The total usable frequency spectrum of twisted-pair copper cable is about 1MHz.
- **Limited data rates**—The longer a signal has to travel over twisted-pair, the lower the data rate. At 30 feet (100 m), twisted-pair can carry 100Mbps, but at 3.5 miles (5.5 km), the data rate drops to 2Mbps or less.
- **Short distances required between repeaters**—More components need to be maintained, and those components are places where trouble can arise, which leads to higher long-term operational costs.
- **High error rate**—Twisted-pair is highly susceptibility to signal interference such as EMI and RFI. Although twisted-pair has been deployed widely and adapted to some new applications, better media are available to meet the demands of the broadband world.

1.3.6 Coaxial Cable

The second transmission medium to be introduced was coaxial cable (often called coax), which began being deployed in telephony networks around the mid-1920s. Coaxial cable gets its name because two conductors share a common axis; the cable is most frequently referred to as a "coax." A type of coaxial cable that you may be familiar with is your television cable.



The components of a coaxial cable are as follows:

- An **inner conductor**, usually solid copper wire.
- An **outer conductor** forms a tube surrounding the inner conductor. This conductor can consist of braided wires, metallic foil, or both. The outer conductor, frequently called the shield, serves as a ground and also protects the inner conductor from EMI.
- An **insulation layer** keeps the outer conductor spaced evenly from the inner conductor.
- A **plastic encasement or cover** (jacket) protects the cable from damage.

The core of a coaxial cable carries the electronic signals that make up the data. This wire core can be either solid or stranded. If the core is solid, it is usually copper. Surrounding the core is a dielectric insulating layer that separates it from the wire mesh. The braided wire mesh acts as a ground and protects the core from electrical noise and crosstalk. (*Crosstalk* is signal overflow from an adjacent wire.) The conducting core and the wire mesh must always be kept separate from each other. If they touch, the cable will experience a *short*, and noise or stray signals on the mesh will flow onto the copper wire. An electrical short occurs when any two conducting wires or a conducting wire and a ground come into contact with each other. This contact causes a direct flow of current (or data) in an unintended path. In the case of household electrical wiring, a short will cause sparking and the blowing of a fuse or circuit breaker. With electronic devices that use low voltages, the result is not as dramatic and is often undetectable. These low-voltage shorts generally cause the failure of a device; and the short, in turn, destroys the data. A nonconducting outer shield—usually made of rubber, Teflon, or plastic—surrounds the entire cable. Coaxial cable is more resistant to interference and attenuation than twisted-pair cabling.

Types of Coaxial Cable

There are two types of coaxial cable:

- Thin (thinnet) cable
- Thick (thicknet) cable

Which type of coaxial cable you select depends on the needs of your particular network.

Thinnet Cable

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

Thicknet Cable

Thicknet cable is a relatively rigid coaxial cable about 1.27 centimeters (0.5 inches) in diameter. Thicknet cable is sometimes referred to as Standard Ethernet because it was the first type of cable used with the popular network architecture Ethernet. Thicknet cable's copper core is thicker than a thinnet cable core. The thicker the copper core, the farther the cable can carry signals. This means that thicknet can carry signals farther than thinnet cable. 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.

Cable manufacturers have agreed upon specific designations for different types of cable. (The following Table lists cable types and descriptions.) Thinnet is included in a group referred to as the *RG-58* family and has 50ohm impedance. (*Impedance* is the resistance, measured in ohms, to the alternating current that flows in a wire.) The principal distinguishing feature of the RG-58 family is the center core of copper. The following figure shows two examples of RG-58 cable, one with a stranded wire core and one with a solid copper core.

RG-58 coaxial cable showing stranded wire and solid copper cores

Table Cable Types

Cable	Description
RG-58/U	Solid copper core
RG-58 A/U	Stranded wire core
RG-58 C/U	Military specification of RG-58 A/U
RG-59	Broadband transmission, such as cable television
RG-6	Larger in diameter and rated for higher frequencies than RG-59, but also used for broadband transmissions
RG-62	ArcNet networks

Applications of Coaxial Cable

In the mid-1920s, coax was applied to telephony networks as interoffice trunks. Rather than having to add more copper cable bundles with 1,500 or 3,000 pairs of copper wires in them, it was possible to replace those big cables (which are very difficult to install cost-effectively) with a much smaller coaxial cable.

The next major use of coax in telecommunications occurred in the 1950s, when it was deployed as submarine cable to carry international traffic. It was then introduced into the data-processing realm in the mid- to late 1960s. Early computer architectures required coax as the media type from the terminal to the host. LANs were predominantly based on coax from 1980 to about 1987. Coax has been used in cable TV and in the local loop, in the form of HFC architectures. HFC brings fiber as close as possible to the neighborhood; then on a neighborhood node, it terminates that fiber, and from that node it fans the coax out to the home service by that particular node.

Advantages and Disadvantages of Coaxial Cable

The advantages of coax include the following:

Broadband system—Coax has a sufficient frequency range to support multiple channels, which allows for much greater throughput.

- **Greater channel capacity**—Each of the multiple channels offers substantial capacity. The capacity depends on where you are in the world. In the North American system, each channel in the cable TV system is 6MHz wide, according to the National Television Systems Committee (NTSC) standard. In Europe, with the Phase Alternate Line (PAL) standard, the channels are 8MHz wide. Within one of these channels, you can provision high-speed Internet access—that's how cable modems operate. But that one channel is now being shared by everyone using that coax from that neighborhood node, which can range from 200 to 2,000 homes.
- **Greater bandwidth**—Compared to twisted-pair, coax provides greater bandwidth systemwide, and it also offers greater bandwidth for each channel. Because it has greater bandwidth per channel, it supports a mixed range of services. Voice, data, and even video and multimedia can benefit from the enhanced capacity.
- **Lower error rates**—Because the inner conductor is in a Faraday shield, noise immunity is improved, and coax has lower error rates and therefore slightly better performance than twisted-pair. The error rate is generally 10–9 (i.e., 1 in 1 billion) bps.
- **Greater spacing between amplifiers**—Coax's cable shielding reduces noise and crosstalk, which means amplifiers can be spaced farther apart than with twisted-pair.

The main disadvantages of coax are as follows:

- **Problems with the deployment architecture**—The bus topology in which coax is deployed is susceptible to congestion, noise, and security risks.
- **Bidirectional upgrade required**—In countries that have a history of cable TV, the cable systems were designed for broadcasting, not for interactive communications. Before they can offer to the subscriber any form of twoway services, those networks have to be upgraded to bidirectional systems.
- **Great noise**—The return path has some noise problems, and the end equipment requires added intelligence to take care of error control.
- **High installation costs**—Installation costs in the local environment are high.
- **Susceptible to damage from lightning strikes**—Coax may be damaged by lightning strikes. People who live in an area with a lot of lightning strikes must

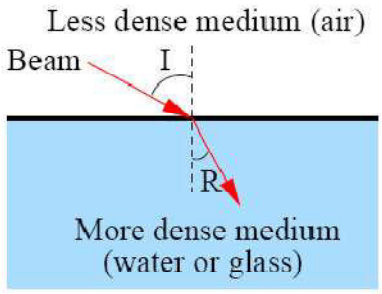
be wary because if that lightning is conducted by a coax, it could very well fry the equipment at the end of it.

1.3.7 Fiber-Optic Cable

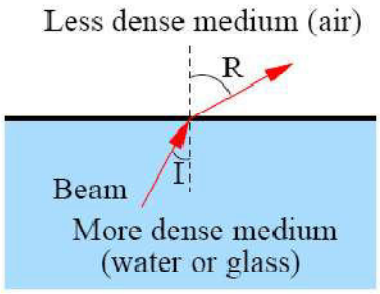
In *fiber-optic cable*, optical fibers carry digital data signals in the form of modulated pulses of light. This is a relatively safe way to send data because, unlike copper-based cables that carry data in the form of electronic signals, no electrical impulses are carried over the fiber-optic cable. This means that fiber optic cable cannot be tapped, and its data cannot be stolen. Fiber-optic cable is good for very high-speed, high-capacity data transmission because of the purity of the signal and lack of signal attenuation.

Refraction

An important characteristic of Fiber Optics is Refraction. Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light travelling through one substance suddenly enters another (more or less denser) substance, its speed abruptly, causing the ray to change direction. This change is called refraction. An example of this is when we look into a pond of water. The direction in which a light ray is refracted depends on the change in density encountered. A beam of light moving from a less dense into a more dense medium is bent towards the vertical axis. The two angles made by the beam of light in relation to the vertical axis are called I, for incident, and R, for refracted. In the following fig. a, the beam travels from a less dense medium into a more dense medium. In this case, angle R is smaller than angle I. in the fig. b, the beam travels from a more dense medium into a less dense medium. In this case, the value of I is smaller than the value of R.



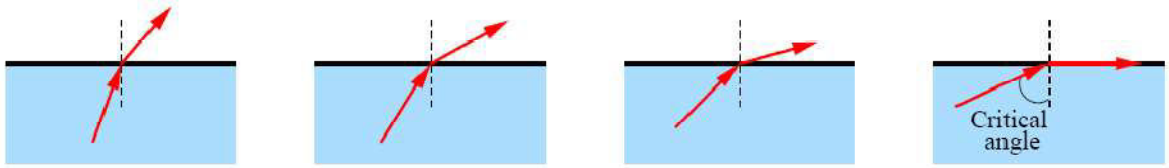
(a) From less dense to more dense medium



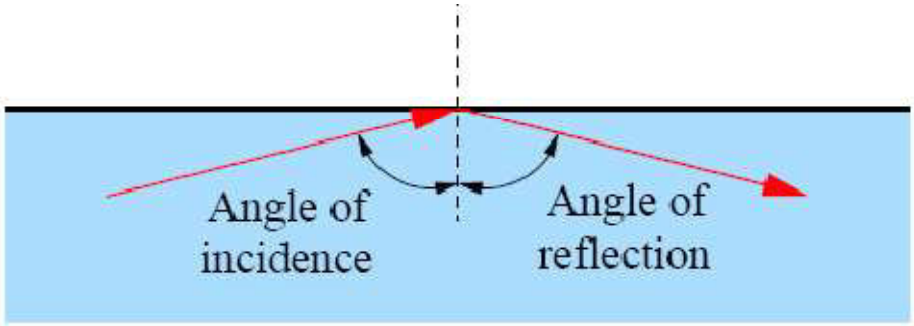
(b) From more dense to less dense medium

Fiber optic technology takes advantage of the property shown in fig. b to control propagation of light through the fiber channel. In the following example, we gradually increase the angle of incidence measured from the vertical. As the angle of incidence increases, so does angle of refraction. It, too, moves away from the vertical and closer and closer to the horizontal. At some point in this process, the change in incident angle

results in refracted angle of 90 degrees, with the refracted beam now lying along the horizontal. The incident angle at this point is known as critical angle.

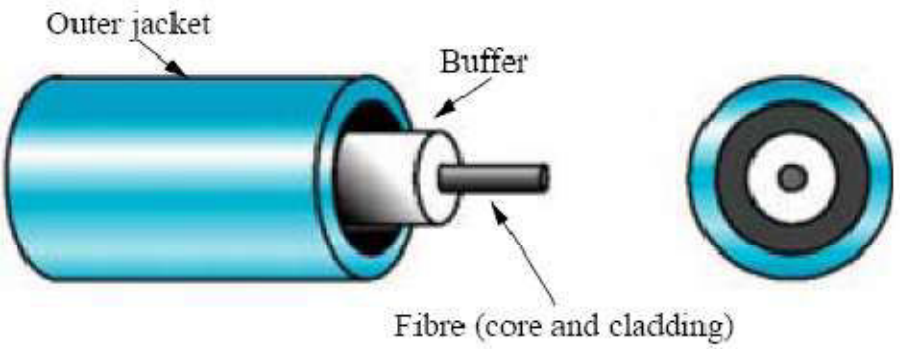


When the angle of incidence becomes greater than the critical angle, light no longer passes into less dense medium al all and is completely reflected into inner medium. Fiber-optics work on this principle.



Working

An optical transmission system has three key components: the light source, the transmission medium, and the detector. Conventionally, a pulse of light indicates a 1 bit and the absence of light indicates a 0 bit. The transmission medium is an ultra-thin fiber of glass or plastic. The detector generates an electrical pulse when light falls on it. By attaching a light source to one end of an optical fiber and a detector to the other, we have a unidirectional data transmission system that accepts an electrical signal, converts and transmits it by light pulses, and then reconverts the output to an electrical signal at the receiving end. Higher bandwidth links can be achieved using optical fibers. One of the best substances used to make optical fibers is ultrapure fused silica. These fibers are more expensive than regular glass fibers. Plastic fibers are normally used for short-distance links where higher losses are tolerable.



The typical optical fiber consists of a very narrow strand of glass called the Core. The core is the light transmission element at the center of the optical fiber. All the light signals travel through the core. A core is typically glass made from a combination of silicon dioxide and other elements. Surrounding the core is the cladding. Cladding is also made of silica but with a lower index of refraction than the core. Light rays traveling through the fiber core reflect off this core-to-cladding interface as they move through the fiber by total reflection. Standard multimode fiber-optic cable is the most common type of fiber-optic cable used in LANs. A standard multimode fiber-optic cable uses an optical fiber with either a 62.5 or a 50µm core and a 125µm diameter cladding. This is commonly designated as 62.5/125 or 50/125 micron optical fiber. Surrounding the cladding is a buffer material that is usually plastic. The buffer material helps shield the core and cladding from damage. The final element is the outer jacket. The outer jacket surrounds the cable to protect the fiber against abrasion, solvents, and other contaminants. The color of the outer jacket of multimode fiber is usually orange. Because each glass strand passes signals in only one direction, a cable includes two strands in separate jackets. One strand transmits and one receives.

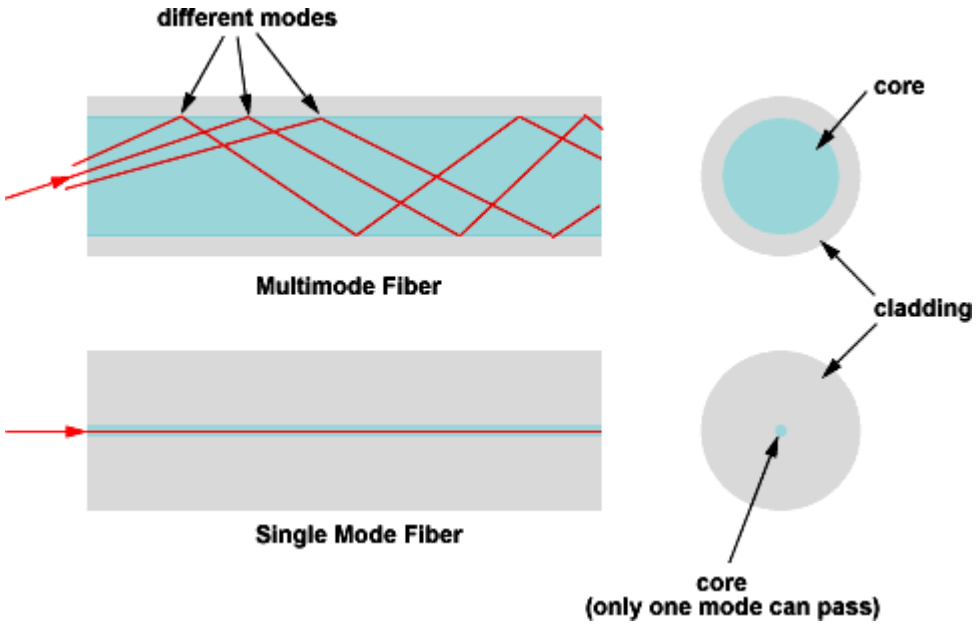
Mode

Light rays can only enter the core if their angle is inside the numerical aperture of the fiber. Once the rays have entered the core of the fiber, there are a limited number of optical paths that a light ray can follow through the fiber. These optical paths are called modes. If the diameter of the core of the fiber is large enough so that there are many paths that light can take through the fiber, the fiber is called "multimode" fiber. Single-mode fiber has a much smaller core that only allows light rays to travel along one mode inside the fiber.

There are 2primary types of transmission modes using optical fiber.

They are

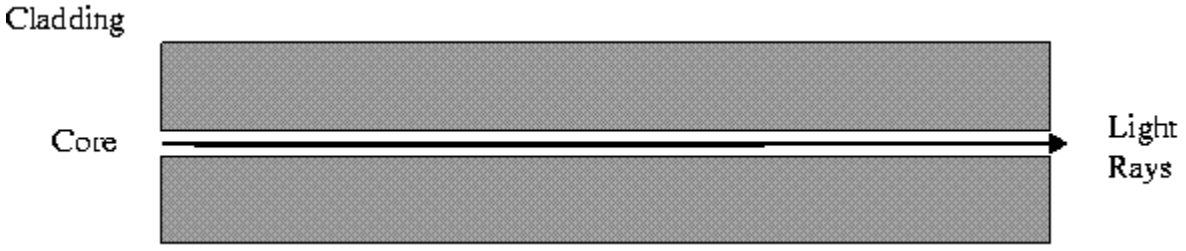
a) Single Mode
b) Multi Mode



The Multi Mode fiber is further of two types:

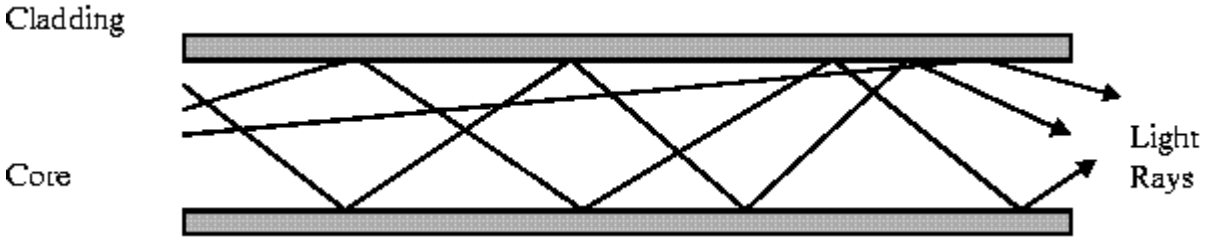
a) Step Index
b) Grade Index

Single-mode fiber is that single-mode allows only one mode of light to propagate through the smaller, fiber-optic core. 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. The single-mode core is eight to ten μm in diameter. Nine-micron cores are the most common. An infrared laser is used as the light source in single-mode fiber. The ray of light it generates enters the core at a 90-degree angle. The data carrying light ray pulses in single-mode fiber are essentially transmitted in a straight line right down the middle of the core. This greatly increases both the speed and the distance that data can be transmitted.



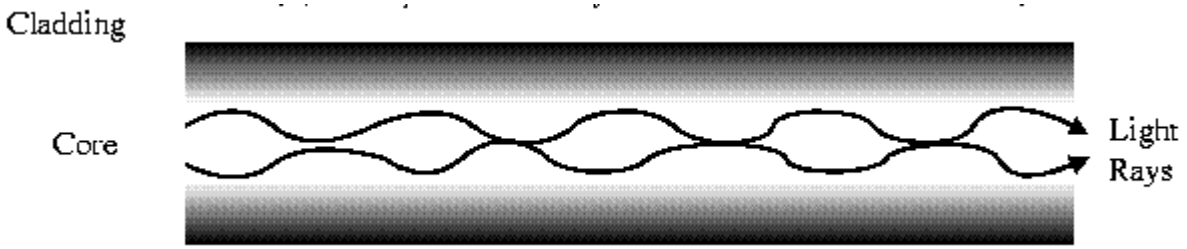
Single Mode

Step Index has a large core. The density of the core remains same from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface, there is an abrupt change to a lower density that alters the angle of beam's motion. The term step-index refers to the suddenness of this change. The light rays tend to bounce around, reflecting off the cladding, inside the core. This causes some rays to take a longer or shorter 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 has 62.5 microns diameter.



Step 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 has 62.5 microns diameter.



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.

Advantages of Optical Fibre:

- Noise immunity: RFI and EMI immune (RFI - Radio Frequency Interference, EMI -Electromagnetic Interference)
- Security: cannot tap into cable.
- Large Capacity due to BW (bandwidth).

- No corrosion.
- Longer distances than copper wire.
- Smaller and lighter than copper wire.
- Faster transmission rate.

Disadvantages of Optical Fibre:

- Physical vibration will show up as signal noise.
- Limited physical arc of cable. Bend it too much & it will break.
- Cost is higher.
- Difficult to install.

The cost of optical fiber is a trade-off between capacity and cost. At higher transmission capacity, it is cheaper than copper. At lower transmission capacity, it is more expensive.

1.3.8 Summary

Transmission media enable computers to send and receive messages. Each type of transmission media has special characteristics that make it suitable for a specific type of service. These characteristics are: Cost, Installation requirements, Bandwidth, Band usage (baseband or broadband), Attenuation and Immunity from electromagnetic interference. There are 2 basic categories of Transmission Media: Guided and Unguided. Guided Transmission Media uses a "cabling" system that guides the data signals along a specific path. Unguided Transmission Media consists of a means for the data signals to travel but nothing to guide them along a specific path. There 3 basic types of Guided Media: Twisted Pair, Coaxial Cable and Optical Fiber. A twisted-pair cable consists of two insulated strands of copper wire twisted around each other. A number of twisted-pair wires are often grouped together and enclosed in a protective sheath to form a cable. A coaxial cable consists of an inner conductor, usually solid copper wire, an outer conductor forms a tube surrounding the inner conductor, an insulation layer keeps the outer conductor spaced evenly from the inner conductor and a plastic encasement or cover (jacket) protects the cable from damage. The core of a coaxial cable carries the electronic signals that make up the data. In *fiber-optic cable*, optical fibers carry digital data signals in the form of modulated pulses of light.

1.3.9 Review Questions

7. What do you mean by Transmission Media?
8. What are the different types of transmission media?
9. Explain different types of transmission media in detail.

1.3.10 Suggested Readings

7. Computer Networks by Andrew S. Tanenbaum
8. Data and Computer Communication by William Stallings
9. Computer networks & internet by D.E. Comer, Pearson Education

Lesson No. 1.4 **Author : Kanwal Preet Singh**

Transmission Media-II

1.4.1 Introduction

The voice communication from one place to another started with the invention of telephone in 1876. Initially, the phones were sold in pairs and communication was

possible only between the specific set of people. With time, the telephone systems became complex and it became possible to set up a connection between any two set of phones. The connection had to be set up physically. When electrons move, they create electromagnetic waves that can propagate through free space. The number of oscillation per second of an electromagnetic wave is called its frequency (f), and measured in hertz (Hz). The distance of two consecutive maxima is called wavelength and universally designated by λ (lambda). By attaching an antenna of the appropriate size to an electrical circuit, the electromagnetic waves can be broadcasted efficiently and received by a receiver some distance away. All wireless communication is based on this principle. In vacuum, all electromagnetic waves travel at the same speed, usually called the speed of light, c, approximately 3×10^8 m/sec.

1.4.2 Objective

After reading the chapter, you will be able to understand:

- Structure of the Telephone System
- Basics principles of working of cellular phones
- Electromagnetic Spectrum
- Wireless Transmission media

1.4.3 The Telephone System

The telephone system is tightly intertwined with (wide area) computer networks. *Public Switched Telephone Network (PSTN)*, that is used today also for computer networking, was designed many years ago with a completely different goal in mind: to transmit the human voice in a more or less recognizable form. Its suitability for use in computer - computer communication is often marginal at best, but the situation is rapidly changing with the introduction of fiber optics and digital technology.

1.4.3.1 Structure of the Telephone System

The telephone was patented by Graham Bell in 1876. Initially, the telephones were sold in pairs and it was up to customer to string a single wire between them. The electrons returned through the earth. Bell formed also the Bell Telephone Company which opened its first switching office in New Haven, Connecticut, in 1878. To make a call, the customer would crank the phone to ring in the telephone company office where the operator manually connected the caller to the callee using a jumper cable (Fig-4-1(a)). Later, the switching offices had to be connected to make long-distance calls possible. Therefore second-level switching offices became necessary (Fig. 4-1(c)) and successively the hierarchy grew to five levels. This scheme remained essentially intact for over 100 years.

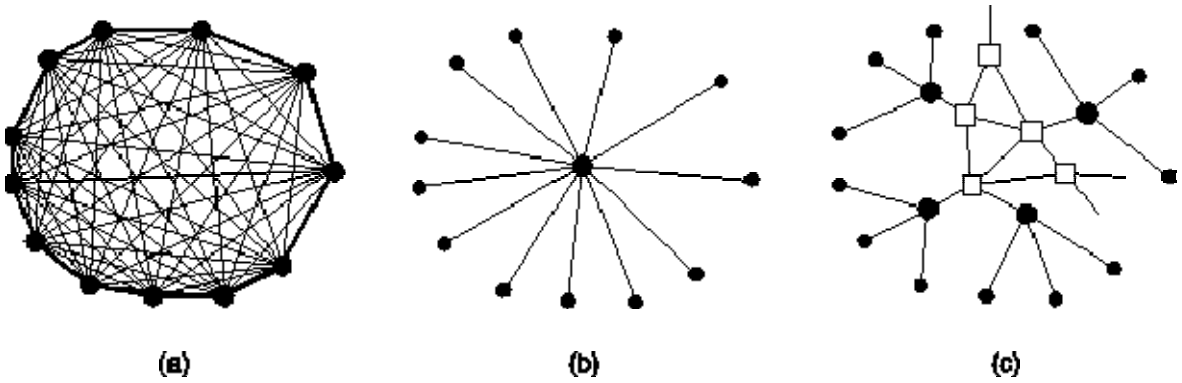


Fig. 4-1. (a) Fully interconnected network. (b) Centralized network. (c) Two level hierarchy.

At present, the telephone system can be, with some simplifications, described as follows: Each telephone has two copper wires coming out of it that go directly to the telephone company's nearest end office. The two wire connection of the telephone and end office is called local loop. If a subscriber attached to a given end office calls another subscriber attached to the same end office, the switching mechanism within the office sets up a direct electrical connection between the two local loops that remains intact for the duration of the call. If a called telephone is attached to another end office, the path will have to be established somewhere higher up in the hierarchy. There are toll offices, primary, sectional, and regional offices that form a network by which the end offices are connected. They communicate with each other via high bandwidth interoffice trunks formed today by coaxial cables, microwaves and especially fiber optics. The number of different kinds of switching centers and their topology varies from country to country depending on its telephone density (Fig. 4-5.)

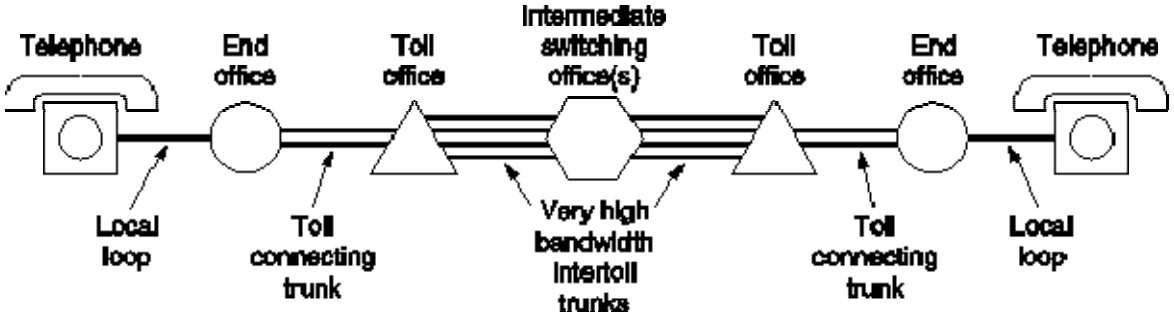


Fig. 4-2. Typical circuit route for a medium-distance call.

In the past, signaling throughout the telephone system was analog. Now, all the long-distance trunks within the telephone system are rapidly being converted to digital using optical fibers. It has the following reasons:

- Digital signal can pass through arbitrary number of regenerators with no information loss. In contrast, analog signals always suffer some information loss when amplified, and this loss is cumulative.
- Voice, data, music, and images can be interspersed to make more efficient use of the circuits and equipment.
- Much higher data rates are possible.
- Digital transmission is much cheaper than analog, since it is not necessary to accurately reproduce an analog waveform through potentially hundreds of amplifiers on a transcontinental call.
- Maintenance of digital system is easier. A transmitted bit is either received correctly or not.

In summary, the telephone system consists of three major components:

1. Local loops (twisted pairs, analog signaling).
2. Trunks (fiber optics or microwave, mostly digital).
3. Switching offices.

1.4.3.2 The Local Loop

The local loops are sill analog. Consequently, when a computer wishes to send digital data over a dial-up line, the data must first be converted to analog form by a modem for transmission over a local loop, then converted to digital form for transmission over the long-haul trunks, then back to analog over the local loop at the receiving end, and finally back to digital by another modem for storage in the destination computer (Fig. 4-3.).

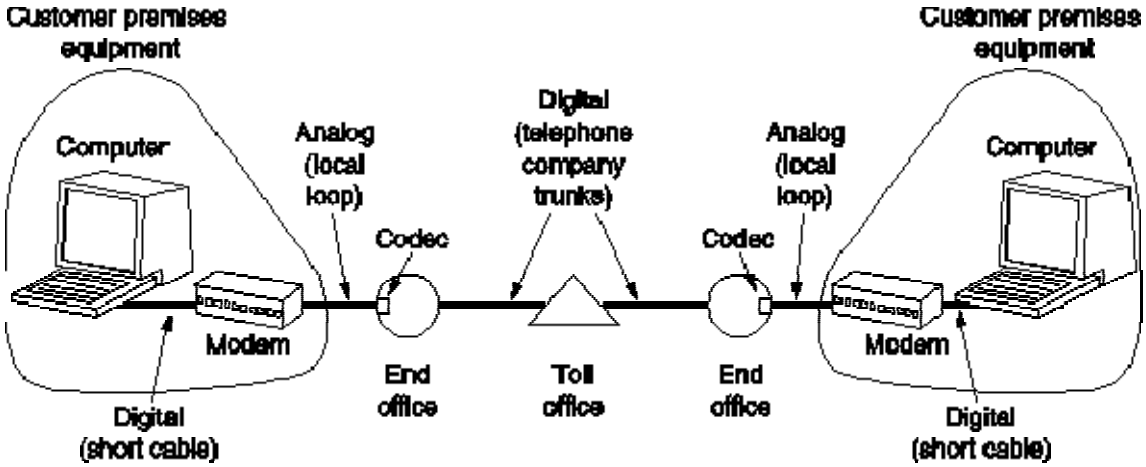


Fig. 4-3. The use of both analog and digital transmission for a computer to computer call. Conversion is done by the modems and codecs.

For leased lines it is possible to go digital from start to finish, but these lines are still expensive.

1.4.3.3 Transmission Impairments

Transmission lines suffer from three major problems:

1. *Attenuation*. It is the loss of energy as the signal propagates outwards. On guided media the signal falls off logarithmically with the distance. The loss is expressed in decibels per km. The amount of energy lost depends of frequency. Amplifiers can be put in to try to compensate for frequency-dependent attenuation. They help but can never restore the signal exactly back to its original shape.
2. *Delay distortion*. It is caused by the fact that different Fourier components travel at different speeds. For digital data, fast components from one bit may catch up and overtake slow components from the bit ahead, mixing the two bits and increasing the probability of incorrect reception.
3. *Noise*. It is unwanted energy from sources other than transmitter (thermal noise, cross talks, impulse noise). (or) It is any type of disturbance that interferences with transmission of information from sender to receiver.

1.4.3.4 Modems

Due to transition impairments dependent on frequency, it is undesirable to have a wide range of frequencies in the signal. Square waves of digital data have a wide spectrum and thus are subject to strong attenuation and delay distortion. So the baseband (DC) signaling is unsuitable except at slow speed and over short distances. To get around the problem, especially on telephone lines, analog (AC) signaling is used. It is based on continuous tone in the 1000 to 2000 Hz range, called sine wave carrier, with amplitude, frequency or phase modulation to transmit information (Fig. 4-18.).

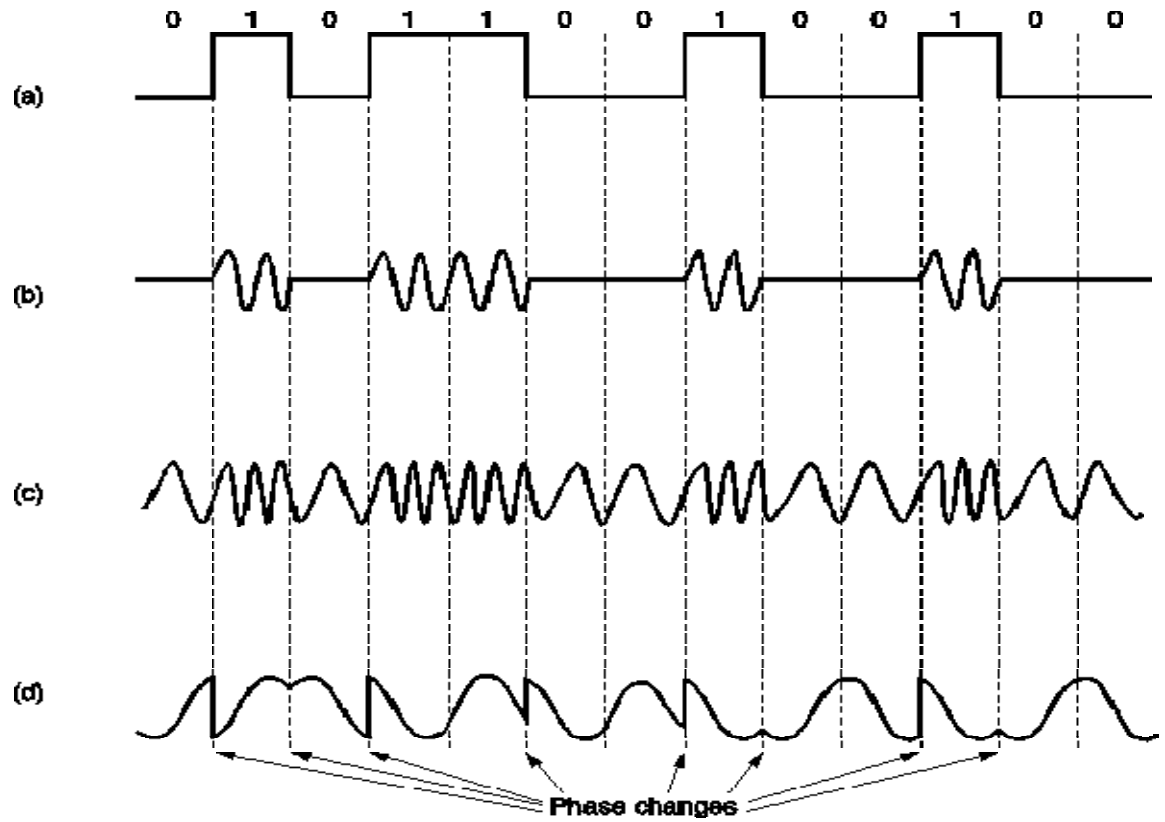


Fig. 4-4. (a) A binary signal. (b) Amplitude modulation. (c) Frequency modulation. (d) Phase modulation.

In amplitude modulation, two different voltage levels are used to represent 0 and 1, respectively.

In frequency modulation (or frequency shift keying), two or more different tones are used.

In phase modulation, the carrier wave is systematically shifted at uniformly spaced intervals. E.g., if 45, 135, 225, or 315 degrees shifts are used, each phase shift transmits 2 bits of information.

A device that accepts a serial stream of bits as input and produces a modulated carrier as output (and vice versa) is called *modem* (for modulator-demodulator).

1.4.4 Cellular Radio

The traditional telephone system (even when broadband ISDN is fully operating) will still not be able to satisfy people on the go. Consequently, there is increasing competition from systems that use wireless technologies for communication. They are already creating a huge market. Many companies in the computer, telephone, satellite, and other industries want a piece of action. The result is a chaotic market, with numerous overlapping and incompatible products and services, all rapidly changing.

1.4.4.1 Paging Systems

The first paging systems used loudspeakers within a single building. Nowadays, people who want to be paged wear small beepers, usually with tiny screens for displaying short incoming messages. A person wanting to page a beeper wearer can call the beeper company and enter a security code, the beeper number, and the number the beeper wearer is to call (or another short message). The request is then broadcasted from a hilltop antenna (for local paging) or from a satellite (for long distance paging). When a beeper detects its unique number in the incoming radio stream, it beeps and displays the number to be called.

Most current paging systems are one-way systems, from a single computer out to a large number of receivers. There is no problem about who will speak next, and no contention among many competing users. Paging systems require little bandwidth since each message requires only a single burst of about 30 bytes. At this rate, a 1 Mbps satellite channel can handle over 240000 pages per minute. The older paging systems run in the 150 - 174 MHz band, the modern ones in the 930 - 932 MHz band. (Fig. 4-5). But the use of pagers have almost become distinct, this form of communication has been replaced by SMS (Short Message Service). The SMS service is provided by the mobile telephone, which performs double task of providing text and voice form of communication.

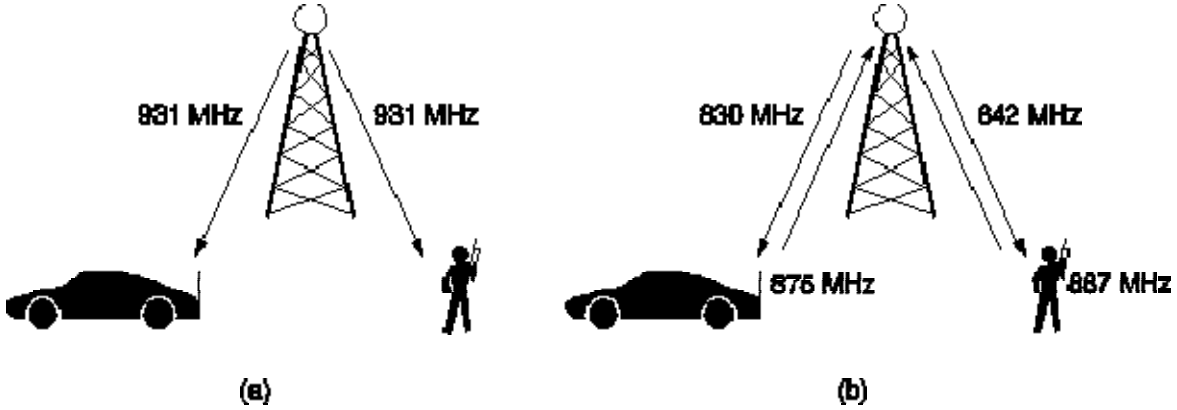


Fig. 4-5. (a) Paging systems are one way. (b) Mobile telephones are two way.

1.4.4.2 Cordless Telephones

A cordless telephone consists of two parts: a base station and a telephone. The base station has a standard phone jack and is connected by a wire to the telephone system. The telephone communicates with the base station by low-power radio. The range is typically 100 - 300 m. Some of cheaper models of cordless telephones used a fixed frequency, selected at the factory. If, by accident, someone in the neighborhood of a user had the telephone with the same frequency, he could listen user's calls. More expensive models avoided this problem by allowing the user to select the transmission frequency.

The generations of cordless telephones:

- CT-1 in the US and CEPT-1 in Europe - entirely analog. They could cause interference with radios and television. Poor reception and lack of security.
- CT-2 - digital standard, originated in England. Each telephone had to be within a few hundred meters of its own base station. Useful around the house or office, useless in cars when walking around the town.
- CT3 or DECT - third generation introduced in 1995. This technology is beginning to approach cellular telephones.

1.4.4.3 Analog Cellular Telephones

Mobile radiotelephones were used sporadically for maritime and military communication during the early decades of the 20th century. Push-to-talk systems (installed in several big cities in the late 1950s) had a single channel used for both sending and receiving. They used a large transmitter on top of a tall building. To talk, the user had to push a button that enabled the transmitter and disabled the receiver. The users could hear each other.

IMTS (Improved Mobile Telephone System - in the 1960s) also used a high-powered (200 watt) transmitter, on top of a hill, but it used different frequencies for sending and for receiving, so no push-to-talk button was necessary. IMTS supported 23 channels spread out from 150 MHz to 450 MHz. Due to the small number of channels, users often had to wait a long time before getting a dial tone. The adjacent systems had to be several hundred km apart. So the system was impractical due to limited capacity.

1.4.4.4 Advanced Mobile Phone System

AMPS (Advanced Mobile Phone System) was invented by Bell Labs, first installed in US in 1985. It is also used in England, where it is called TACS, and in Japan, where it is called MCS-L1. In AMPS, a geographic region is divided up into cells, typically 10 to 20 km across, each using some set of frequencies. The key idea that gives AMPS far more capacity than all previous systems, is using relatively small cells, and reusing transmission frequencies in nearby (but not adjacent) cells. The idea of frequency reuse is illustrated in Fig. 4-6(a). The cells are normally roughly circular, but they are easier to model as hexagon. In Fig. 4-6(a), the cells are all the same size. They are grouped in units of seven cells. Each letter indicates a group of frequencies.

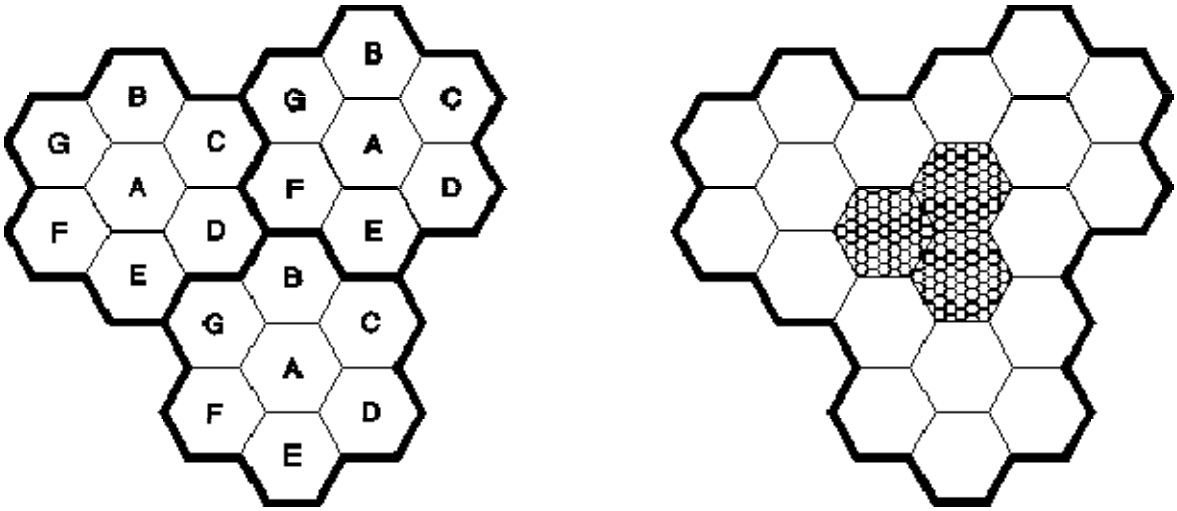


Fig. 4-6. (a) Frequencies are not reused in adjacent cells. (b) To add more users, smaler cells can be used.

In an area where the number of users has grown to the point where the system is overloaded, the power is reduced and the overloaded cells are split into smaller ones to permit more frequency reuse (Fig. 4-6(b)).

At the center of each cell, there is a *base station* to which all the telephones in the cell transmit. The base station consists of a computer and transmitter/receiver connected to an antenna. The base stations are connected to *MTSO* (Mobile Telephone Switching Office). In larger areas, several MTSOs may be needed, all of which are connected to a second-level MTSO, and so on. The MTSO system is connected to at least one telephone system end office. The MTSOs communicate with the base stations, each other, and the PSTN using a packet switching network.

At any instant, each mobile telephone is logically in one specific cell and under the control of that cell's base station. When a mobile telephone leaves a cell, its ownership is transferred to the cell getting the strongest signal from it. If a call is in progress, it will be asked to switch to a new channel. This process is called handoff and takes about 300 msec. The channel assignment is done by MTSO.

1.4.4.5 Channels

The AMPS system uses 832 full-duplex channels, each consisting of a pair of simplex channels. There are 832 simplex transmission channels from 824 to 849 MHz, and 832 simplex receive channels from 869 to 894 MHz. Each of these simplex channels is 30 kHz wide. AMPS uses FDM to separate the channels.

In the 800 MHz band, radio waves travel in straight lines. They are absorbed by trees and plants and bounce off the ground and buildings. This may lead to an echo effects or signal distortion. The 832 channels are divided into four categories:

1. Control (base to mobile) to manage the system. 21 channels are reserved for control, and these are wired into a PROM in each telephone.
2. Paging (base to mobile) to alert mobile users to call for them.
3. Access (bi-directional) for call setup and channel assignment.
4. Data (bi-directional) for voice, fax, and data.

Since the same frequencies cannot be reused in nearby cells, the actual number of voice channels per cell is much smaller than 832, typically about 45.

1.4.4.6 Call Management

Each mobile phone in AMPS has a 32 bit serial number and 10 digit telephone number in its PROM. When a phone is switched on, it scans a preprogrammed list of 21 control channels to find the most powerful signal. From the control channel, it learns the number of paging and access channels.

The phone then broadcasts its serial number and telephone number several times. When the base station hears the announcement, it tells the MTSO, which records the existence of its new customer and also inform the customer's home MTSO of his current location. During the normal operation, the mobile telephone reregisters about once every 15 minutes.

To make a call, the user enters the number to be called, and hits the send button. The phone sends the number and its own identity on the access channel. When the base station gets the request, it informs the MTSO. The MTSO looks for idle channel for the call. If one is found, the channel number is sent back on the control channel. The mobile phone then automatically switches to the selected voice channels and waits until the called party picks up the phone.

As for incoming calls, all idle phones continuously listen to the paging channel to detect messages directed at them. When a call is placed to a mobile phone, a packet is sent to the callee's home MTSO to find out where it is. A packet is then sent to the base station in its current cell, which then sends a broadcast on the paging channel of the form: "Unit 4, are you here?" The called phone then responds with "Yes" on the control channel. The base then says something like: "Unit 4, call for you on channel 3." The called phone switches to channel 3 and starts making ringing sounds.

1.4.4.7 Security Issues

Analog cellular phones are totally insecure. Anyone with an all-band radio receiver (scanner) can tune in and hear everything going in a cell. Another major problem is theft of air time, again based on the possibility of monitoring the transmitted information. Some of these problems could be solved by encryption, but then the police could not easily perform "wiretaps" on wireless criminals.

1.4.4.8. Digital Cellular Telephones

First generation cellular systems were analog. The second generation is digital. In Europe, an agreement on a common digital system, call *GSM* (Global System for Mobile communication) was achieved.

GSM operates in a new frequency band (1.8 GHz) and uses both FDM and TDM. The available spectrum is broken up into 50 200 kHz bands. With each band TDM is used to multiplex multiple users.

Some GSM telephones use smart cards (credit card sized devices containing a CPU). The serial number and telephone number are contained there, not in telephone, making for better security. Encryption is also used.

1.4.5 Wireless Transmission

Modern wireless digital communication began in the Hawaiian Islands, where large chunks of Pacific Ocean separated the users and the telephone system was inadequate.

1.4.5.1 The Electromagnetic Spectrum

When electrons move, they create electromagnetic waves that can propagate through free space. The number of oscillation per second of an electromagnetic wave is called its frequency, f, and measured in hertz (Hz). The distance of two consecutive maxima is called wavelength and universally designated by l (lambda). By attaching an antenna of the appropriate size to an electrical circuit, the electromagnetic waves can be broadcasted efficiently and received by a receiver some distance away. All wireless communication is based on this principle. In vacuum, all electromagnetic waves travel at the same speed, usually called the speed of light, c, approximately 3×10^8 m/sec. In copper or fiber the speed slows to about 2/3 of this value and becomes slightly frequency dependent. The fundamental relation between f, l, and c (in vacuum) is

$$lf = c$$

For example: 1-MHz waves are about 300 m long and 1-cm waves have a frequency of 30 GHz.

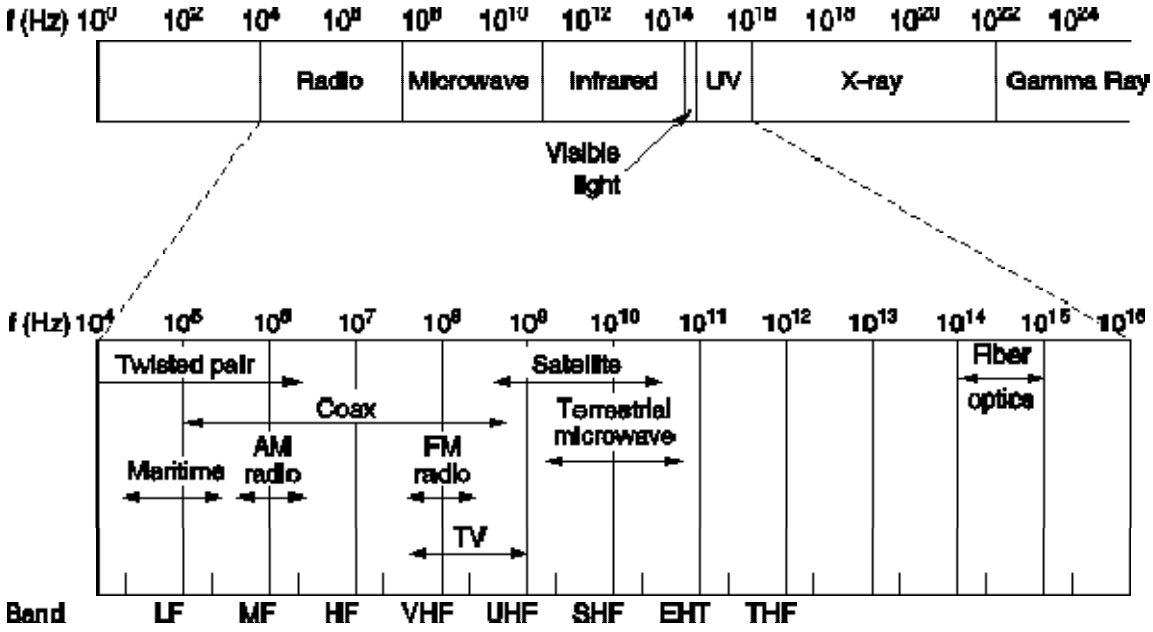


Fig. 4-7. The electromagnetic spectrum and its uses for communication.

The electromagnetic spectrum is shown in Fig. 4-7. The radio, microwave, infrared, and visible light portions of the spectrum can all be used for transmitting information by modulating the amplitude, frequency, or phase of the wave. Ultraviolet light, X-rays, and gamma rays would be even better, due to their higher frequencies, but they are hard to produce and modulate, do not propagate well through buildings, and are dangerous to living things. LF, MF, ... are official ITU (International Telecommunication Union) names and are based on wavelengths. The amount of information that an electromagnetic wave can carry is related to its bandwidth. With current technology, it is possible to encode a few bits per Hertz at low frequencies, but often as many as 40 under certain conditions at high frequencies, so a cable with 500 MHz bandwidth can carry several gigabits/sec. There are national and international agreement about who gets to use which frequencies. World-wide, it is an agency of ITU-R (WARC), in US the work is done by FCC (Federal Communication Commission). Most transmissions use a narrow frequency band ((f/f<<1)to get the best reception (many watts/Hz). However, there are some exception from this rule (i.e. spread spectrum popular in military communications).

1.4.5.2 Radio Transmission

Radio Waves are easy to generate, can travel long distances, and penetrate building easily, so they are widely used for communications, both indoors and outdoors. They are also omnidirectional, so the transmitter and receiver do not have to be aligned physically. This feature is sometimes good, but sometimes bad. The properties of radio waves are frequency dependent. At low frequencies they pass

through obstacles well, but the power falls off sharply with distance from the source. At high frequencies, radio waves tend to travel in straight lines and bounce off obstacles. They are also absorbed by rain. At all frequencies, they are subject to interference from motors and other electrical equipment. Due to radio's ability to travel long distances, interference between users is a problem. For this reasons, all governments license the use user of radio transmitters.

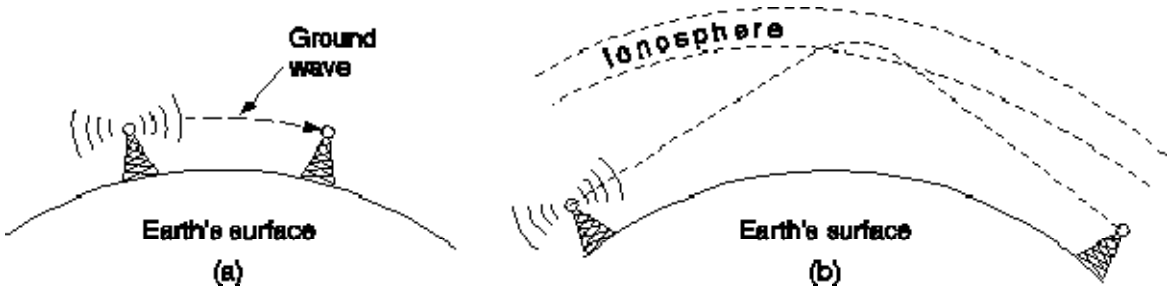


Fig. 4-8. (a) In the VLF, VF, and MF bands, radio waves follow the curvature of the earth. (b) In the HF they bounce off the ionosphere.

In the VLF, LF, and MF bands, radio waves follow the ground (Fig. 4-8(a)) and can be detected for about 1000 km at the lower frequencies, less at the higher ones. The main problem with using these bands for data communication is relatively low bandwidth they offer. In the HF and VHF bands, the ground waves tend to be absorbed by the earth, but if they reach the ionosphere (a layer of charged particles circling the earth at a height of 100 to 500 km) are refracted (Fig. 4-8(b)) by it and sent back to earth. Amateur radio operators use these bands to talk long distance.

1.4.5.3 Microwave Transmission

Above 100 MHz, the waves travel in straight lines and can therefore be narrowly focused. Concentrating all the energy into a small beam using parabolic antenna gives a much higher signal to noise ratio, but the transmitting and receiving antennas must be accurately aligned with each other. Before fiber optics, for decades, these microwaves formed the heart of the long-distance telephone transmission system. Microwaves do not pass through buildings well. In addition, even though the beam is well focused, there is still some divergence in space. Some waves may be refracted off low lying atmospheric layers and may take slightly longer to arrive than direct waves. Being out of phase they can cancel the signal. This effect is called multipath fading and is often a serious problem. It is weather and frequency dependent.

Bands up to 10 GHz are now in routine use, but at about 8 GHz a new problem sets in: absorption by water (rain). The only solution is to shut off links that are being rained on and route around them. Microwave is also relatively inexpensive. Putting up two simple towers (maybe just big poles with four guy wires) and putting antennas on each one may be cheaper than burying 50 km of fiber through a congested urban area, and it may also be cheaper than leasing the telephone company fiber. Microwaves have

also another important use. We are speaking about cordless telephones, garage door openers, wireless hi-fi speakers, security gates etc. These devices use so called Industrial/Scientific/Medical bands forming an exception to the licensing rule: transmitters using these bands do not require government licensing. One band is allocated world-wide: 5.400-5.484 GHz. These bands are popular also for various forms of short-range wireless networking.

1.4.5.4 Infrared and Millimeter Waves

Unguided infrared and millimeter waves are widely used for short-range communication (remote control of televisions and stereos). They are relatively directional, cheap and easy to build, but they do not pass through the solid objects. For this reason, no government license is needed to operate an infrared system. These properties have made infrared an interesting candidate for indoor wireless LANs (i.e. portable computers with infrared capability can be on local LAN without having to physically connect to it. Infrared communication cannot be used outdoors because the sun shines as brightly in the infrared as in visible spectrum.

1.4.5.5 Lightwave Transmission

Unguided optical signaling has been in use for centuries. A modern application is to connect the LANs in two building via lasers mounted on their rooftops. Optical signaling using lasers is unidirectional, so each building needs its own laser and its own photodetector. This scheme offers very high bandwidth and very low cost. It is also relatively easy to install and does not require license. The laser's strength, a very narrow beam, is also a weakness here. Aiming a laser beam 1 mm wide at a target 1 mm wide 500 m away could be a problem. Usually, lenses are put into the system to defocus the beam slightly. A disadvantage is that laser beams cannot penetrate rain or thick fog. Some other phenomena in the atmosphere can also influence the communication using laser (Fig. 4-9.).

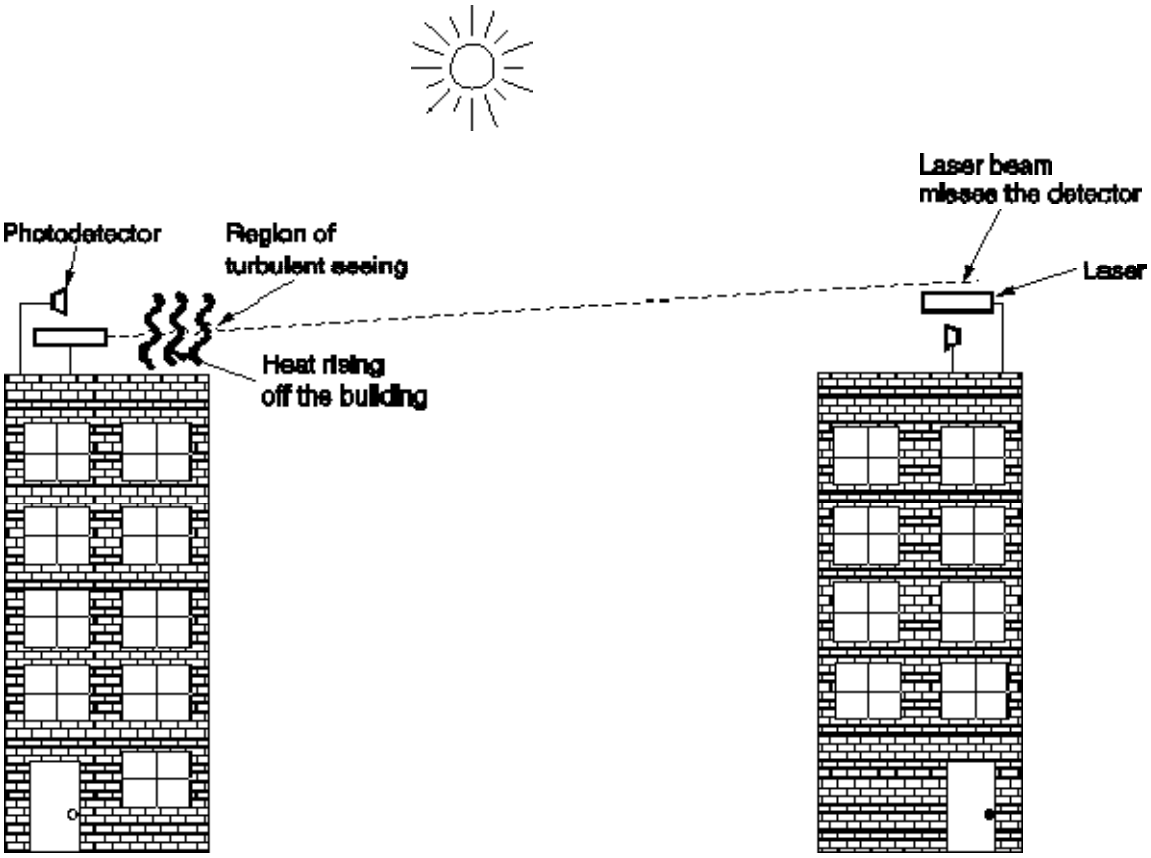


Fig. 4-9. Convection currents can interfere with laser communication systems. A bidirectional system, with two lasers, is pictured here.

1.4.6 Communication Satellites

In the 1950s and early 1960s people tried to set up communication systems by bouncing signals off metalized balloons. Unfortunately, the received signals were too week to be of any practical use. The US Navy built an operational system for ship-to-shore communication by bouncing signal off the moon. Further progress in the celestial communication came with the first communication satellite launched in 1965. The artificial satellites can amplify the signal before sending them back and can be thought as a big microwave repeaters in the sky. Communication satellites contain several transpoders, each of which listens to some portion of the spectrum, amplifies the incoming signal, and then rebroadcasts it at another frequency, to avoid interference with the incoming signal. The downward beams can be broad, covering a substantial fraction of the earth's surface, or narrow, covering an area only hundreds of kilometers in diameter.

1.4.6.1 Geosynchronous Satellites

According to Kepler's law, the orbital period of a satellite varies as the orbital radius to the 3/2 power. Near the surface of the earth, the period is about 90 minutes that use useless for communication satellites. However, at an altitude approximately 36000 km above the equator, the satellite period is 24 hours, so it revolves at the same rate as the earth under it. It is very desirable for communication purposes.

With current technology, it is in general unwise to have satellites spaced much closer than 2 degrees in the 360 degree equatorial plane, to avoid interference. So we have just 180 slots for geosynchronous satellites. Fortunately, satellites using different parts of spectrum do not compete, so each of the 180 possible satellites could have several data streams going up and down simultaneously. Alternatively, two or more satellites could occupy one orbit slot if they operate at different frequencies. There have been international agreement about who may use which orbit slots and frequencies. The main commercial bands are the following (Fig. 4-10):

Band	Frequencies	Downlink (GHz)	Uplink (GHz)	Problems
C	4/6	3.7–4.2	5.925–6.425	Terrestrial interference
Ku	11/14	11.7–12.2	14.0–14.5	Rain
Ka	20/30	17.7–21.7	27.5–30.5	Rain; equipment cost

Fig. 4-10 The principal satellite bands.

1. C band - the frequency ranges assigned to this band are already overcrowded because they are also used by the common carriers for terrestrial microwave links.
2. Ku band - this band is not (yet) congested, and at these frequencies satellites can be spaces as close as 1 degree. But another problem exists: absorption by rain. This problem can be circumvented by using several widely separated ground stations.
3. Ka band - the problem with this band is still expensive equipment.

In addition to these commercial bands, many government and military bands also exist. A typical satellite has 15-20 transpoders, each with 36-50 MHz bandwidth (e.g., a 50 Mbps transpoder can handle 800 64 kbps digital voice channels). The first satellites had a single spatial beam that illuminated the entire earth. Nowadays, each downward beam can be focused on a small geographical area, typically elliptically shaped, and as small as a few hundreds km in diameter (so called spot beams). A new development in the communication satellite world is the development of low-cost microstations, sometimes called VSATs (Very Small Aperture Terminals). These tiny terminals can put out only small power (1 watt) and the communication among them is

ensured by using a special ground station, the hub, with a large antenna and amplifier (Fig. 4-56). The trade off is a longer delay.

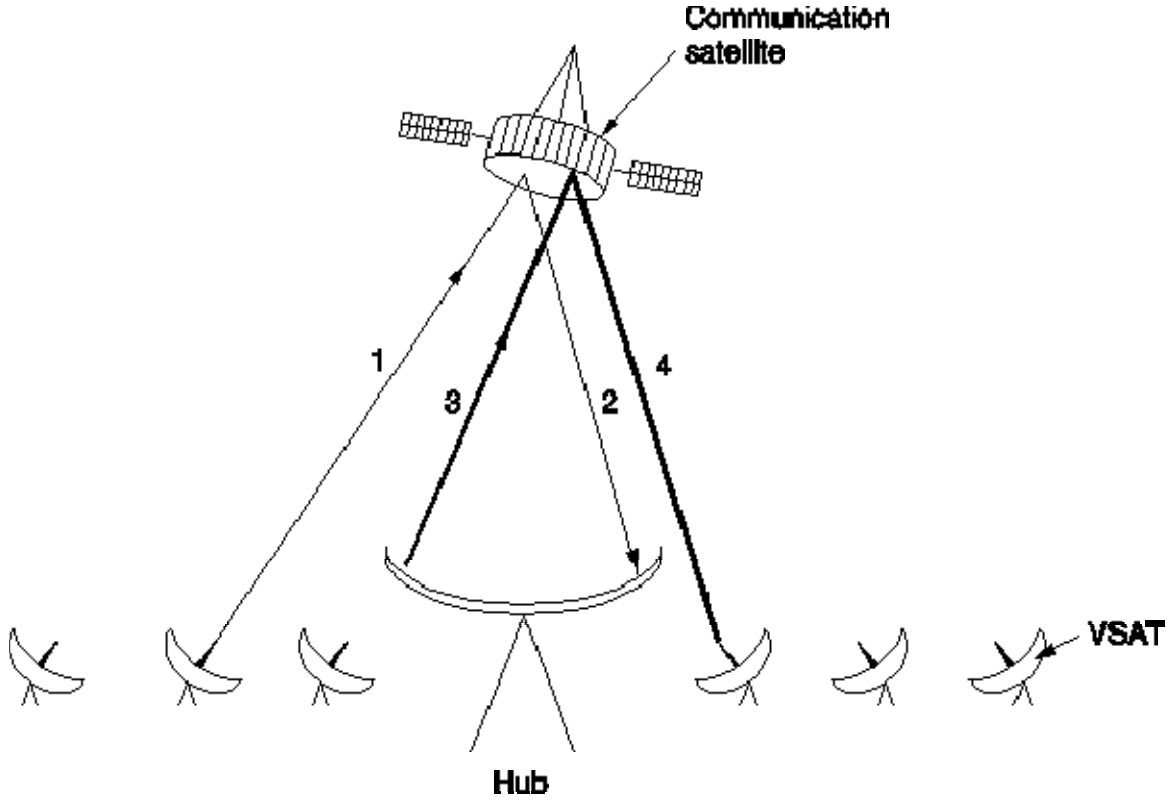


Fig. 4.11. VSATs using a hub.

Differences between communication satellites communication and terrestrial microwave links communication:

- Average end-to-end transmit time 270 msec at satellites (540 at VSATs), much longer than at terrestrial communication).
- Satellites are inherently broadcast media, the satellite broadcasting is much cheaper that terrestrial one.
- If security is required, encryption must be used at satellite transmission.
- At satellite communication, the cost for transmitting of a message is independent of the distance of the source and destination. A call across the ocean costs no more to service than a call across the street.
- Satellites have excellent error rates.

1.4.6.2 Low-Orbit Satellites

For the first 30 years of satellite era, low-orbit satellites were rarely used for communication because they zip into and out of view so quickly. In 1990, Motorola started a new activity called Iridium project, aimed to communication based on low orbit satellites. The basic goal of Iridium is to provide worldwide telecommunication

service using hand-held devices that communicate directly with Iridium satellites. This service competes with PCS/PCN activities. The project uses ideas from cellular radio, but with moving cells. The satellites beams scan the earth as the satellites move. The handover techniques used in cellular radio are applicable also in this case. The satellites (66 in total) are to be positioned at an altitude of 750 km, in circular polar orbits (Fig 4-12(a)). With 6 satellite necklaces, the entire earth would be covered (Fig. 4-12(b)).

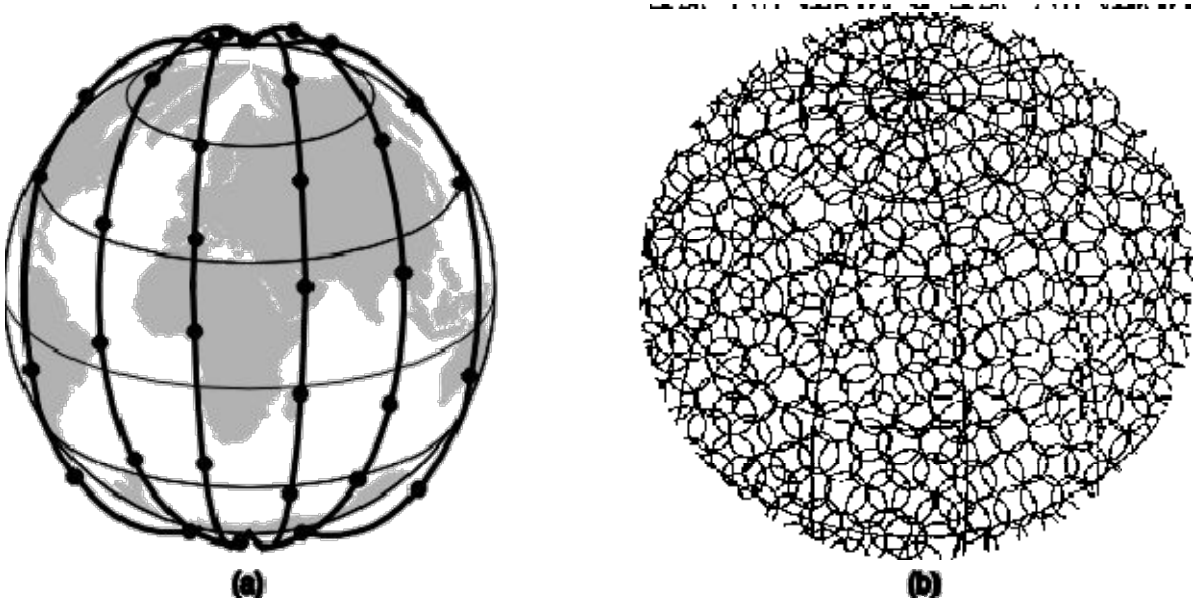


Fig. 4-12. (a) The Iridium satellites from six necklaces around the earth. (b) 1628 moving cells cover the earth.

1.4.7 Summary

Initially, the telephones were sold in pairs and it was up to customer to string a single wire between them. At present, each telephone has two copper wires coming out of it that go directly to the telephone company's nearest end office. The two wire connection of the telephone and end office is called local loop. If a subscriber attached to a given end office calls another subscriber attached to the same end office, the switching mechanism within the office sets up a direct electrical connection between the two local loops that remains intact for the duration of the call. If a called telephone is attached to another end office, the path will have to be established somewhere higher up in the hierarchy. A cordless telephone consists of two parts: a base station and a telephone. The base station has a standard phone jack and is connected by a wire to the telephone system. The telephone communicates with the base station by low-power radio. *AMPS* (Advanced Mobile Phone System) was invented by Bell Labs, first installed in US in 1985. In AMPS, a geographic region is divided up into cells, typically 10 to 20 km across, each using some set of frequencies. The key idea that

gives AMPS far more capacity than all previous systems, is using relatively small cells, and reusing transmission frequencies in nearby (but not adjacent) cells. When electrons move, they create electromagnetic waves that can propagate through free space. The number of oscillation per second of an electromagnetic wave is called its frequency, f, and measured in hertz (Hz). The distance of two consecutive maxima is called wavelength and universally designated by l (lambda). By attaching an antenna of the appropriate size to an electrical circuit, the electromagnetic waves can be broadcasted efficiently and received by a receiver some distance away. All wireless communication is based on this principle. The radio, microwave, infrared, and visible light portions of the spectrum can all be used for transmitting information by modulating the amplitude, frequency, or phase of the wave.

1.4.8 Review Questions

1. Explain the structure of telephone system.
2. What is a modem?
3. What is an electromagnetic spectrum?
4. Explain different types of wireless media.

1.4.9 Suggested Readings

10. Computer Networks by Andrew S. Tanenbaum
11. Data and Computer Communication by William Stallings
12. Computer network & internets by D.E. Comer, Pearson Education

B.A. Part-III **Paper : BAP-303**
Semester-VI **Introduction to Computer Network and Internet Programming**

Lesson No. 1.5 **Author : Vishal Singh**

The Internet

Objective:

In this lesson, we will discuss the Internet, its working, protocols and the various services provided by the Internet. We will also discuss the concept of Electronic mail in detail.

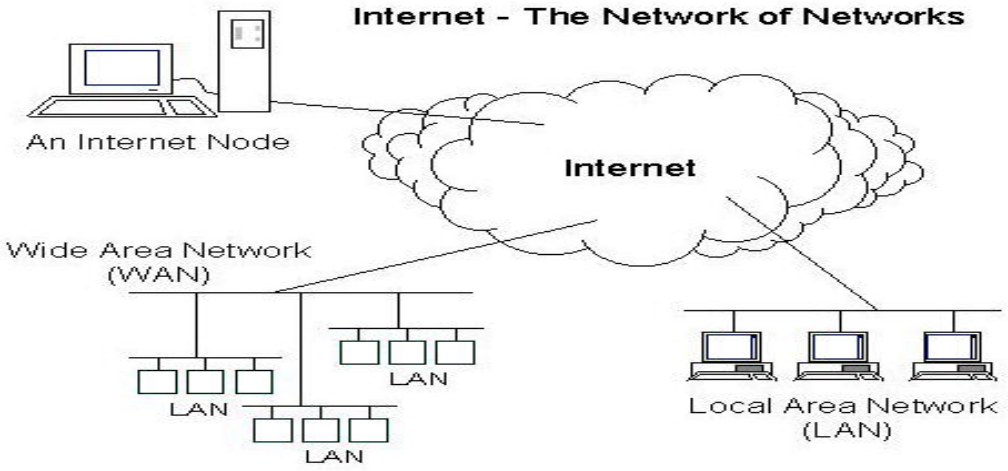
1.0 Introduction: Internet

The Internet, sometimes called simply "the net", is a computer network made up of thousands of networks worldwide. No one knows exactly how many computers are connected to the Internet. It is certain, however, that these number in the millions and are growing.

No one is in charge of the Internet. There are organizations which develop technical aspects of this network and set standards for creating applications on it, but no governing body is in control. The Internet backbone, through which Internet traffic flows, is owned by private companies.

All computers on the Internet communicate with one another using the Transmission Control Protocol/Internet Protocol suite, abbreviated to TCP/IP. Computers on the Internet use client/server architecture. This means that the remote server machine provides files and services to the user's local client machine. Software can be installed on a client computer to take advantage of the latest access technology.

An Internet user has access to a wide variety of services: electronic mail, file transfer, vast information resources, interest group membership, interactive collaboration, multimedia displays, real-time broadcasting, breaking news, shopping opportunities and much more.



1.1 How does the internet work?

The internet is defined as a “network of networks”. The formal definition of the network is: “An interconnection of two or more autonomous computers”. Interconnection means that the computers are able to exchange messages and data. Autonomous means that no computer can forcefully start, stop or control another computer. At its most complexes, as in the internet, a network is a globe spanning, heterogeneous mix of technologies and operating systems.

The internet mostly connects network of computers. Think of a corporate wide network: each department has a LAN that allows it to share files and may be a printer

or two. Several departments, working together, interconnects their networks so that information may be shared more easily among the departments. These "regional" networks are interconnected based on geography (same city, same state, same group of states) or function (accounts-receivable grouped with accounts payable into an accounting network, for example).

Then the regional networks are connected together onto a corporate network, sometime called a "backbone". So, there is a user connected to a Local Net; a Local Net connected into a regional Net; and regional Nets connected to a backbone. This is the Global Internet.

Unlike commercial networks such as CompuServe or Prodigy, the internet is not run by one central computer or computers. This is both its greatest strength and greatest weakness. The approach means it is virtually impossible for the entire Net to crash at once even if one computer shutdown, the rest of the network stays up. The design also reduces the cost for an individual or organization to get onto the network. But thousand of connected computers can also make it difficult to navigate the Net and find what you want especially as different computer may have different commands for plumbing their resources. It is only recently that Net users have begun to develop the sorts of navigational tools and "maps" that will let neophytes get around without getting lost.

Nobody really knows how many computes and networks actually make up this Net. Some estimates say there are now Thousands of networks connecting more than 2 millions computers and more than 3 billion people around the world. Whatever the actual numbers, however, it is clear they are only increasing.

1.2 Data flow across the Net

Consider the transfer of message from one computer to another. Each message has an address on it. The e-mail handling system on the sender's computer packages the message and perhaps for "shipping". The message is broken up into small pieces called "packets". Packets are one of the basic units of measurement on the internet. Packets have different sizes, depending on what application "packed" them. You can think of them as envelopes or suitcase full of information. The packets are all addressed to the final destination. In fact the packets that contains the message may not all travel the same path. Along the possible path are special purpose computers called "routers". These computers do nothing but look at network addresses and figure out from the address what is the current best route to the destination address.

Routers make their decisions based on information that is constantly reaching them from all over the Net. They hear from other routers about links that are down, about others that may be congested and slow or about routers that are no longer accepting packets from certain destinations. Each packet's destination and proposed route is evaluated individually, in the blink of eye and sent off along the best route for that particular packet at that particular moment.

The same sort of decision making is made for all packets that traverse to internet. Each time a packet is forwarded either to another to another route near its ultimate destination or to that destination if the router is the final router on the path. The destination computer is the one that unpacks the packets, throw away "envelopes" and hands of the e-mail message.

1.3 Internet Addressing

There are two kinds of addresses in the internet**:** Domain Names & IP Addresses.

1. **Domain Name System (DNS):** Every computer on the internet has a domain name. The names of the domain describe organizational or geographic realities. They indicate what country the network is in, what kind of organization owns it and in some cases, the names are defined in even more detail. Domains can be Non-geographic or Geographic.
2. **IP Addresses:** Every node on the internet, every end point (which might be a computer or a dial-in modem), has a unique identifying address. These unique identifiers are called **Internet Protocol Addresses**. The computer or server is known as a host and the IP address, its physical network connection is known as the host address. The IP address can be difficult to remember, is easy to enter incorrectly and will not necessary remains same if someone need to reorganize his or her network. The difficulty with these addresses is what led to the creation of DNS names, which map IP addresses to a set of more easily remembered words.

The IP address is a set of numbers that express the exact physical connection between a computer and the network on the internet. In some senses you can think of them in the same way you think about the telephone numbers**:** a phone number uniquely describes your connection to the telephone network.

1.4 Internet Protocols

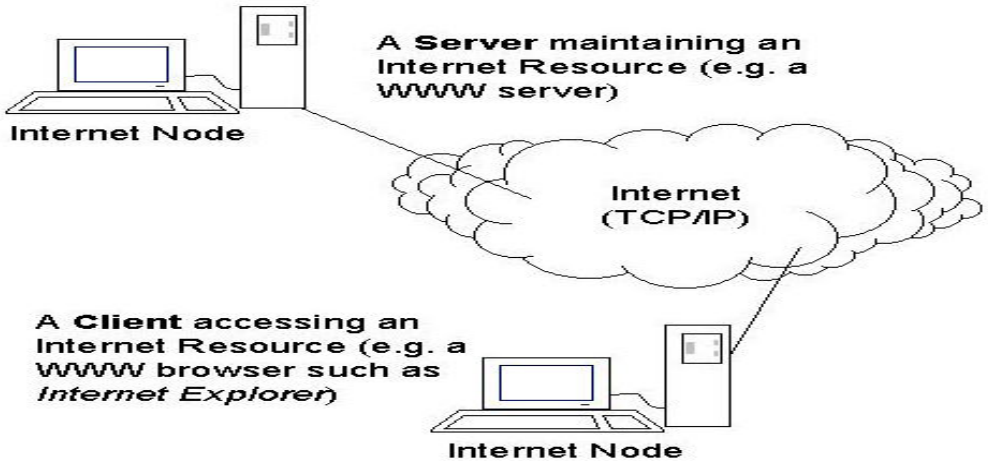
Protocols are the rules that all the networks use to understand each other. The various protocols are set of technical specifications that let computer exchange

information, no matter what kind of computer they are or what kind of technology hooks them together. Vendors of software and hardware want their products to be useful on the internet and so make sure those products understand and operate with the internet protocols. The term interoperability has been coined to describe this ability of disparate types of hardware and software to work together under a common set of rules.

TCP/IP is a set of protocols developed to allow cooperating computers to share resources across a network. It was developed by a community of researchers centered around the ARPAnet (Advanced Research Prospects Agency Networks). Certainly the ARPAnet is the best known TCP/IP (Transmission Control Protocol/Internet Protocol) network. However as of June, 87, at last 130 different vendors had products that support TCP/IP and thousand of networks of all kinds use it.

Whatever it is called, TCP/IP is a family of protocols. A few provide "low-level"

Functions needed for its applications. These include IP, TCP and UDP. Others are protocols for doing specific tasks, e.g. transferring files between computers, sending mail or finding out who is logged in on another computer. Initially TCP/IP was used mostly between minicomputers and mainframes. These machines had their own disks, and generally were self-contained.



1.5 Internet Services

As we have already discussed the Internet along with its working and protocols. So now we are discussing the various services provided by the internet.

There is a big list of things we can do on the internet. Like:

1. Communication
2. Document or file transfer
3. Interactive browsing
4. Bulletin boards

These are the tools for doing these activities.

1. **FTP**-(file transfer protocol)-moving electronic documents, images, sounds etc.
2. **TELNET**-accessing another computer system's database or archives and
3. **WAIS**- a powerful tool for searching some large database.
4. **Gopher**- an information browser that lets us retrieves what we find.
5. **WWW** (World Wide Web) - a hypertext interface to information on the internet.
6. **USENET**-global bulletin board service.
7. **Archie**- a simple but effective mechanism for searching FTP archives.
8. **Veronica**-an enhancement to gopher that searches many gopher databases.
9. **Email**-Electronic message exchange.
10. **Chat & Instant Messaging -** Real time talk.

The details of theses services are:

1. FTP-Ftp is a protocol or set of rules, that enables the file to be transferred from one computer to another. It is part of the TCP/IP protocol suite. Files that are available are stored on the computers called FTP servers. An FTP client program is an interface that allows the user to locate the files to be transferred and initiate the transfer process.

2. Telnet- Telnet is the protocol that enables one computer to establish connection to another computer. The computer establishes the connection is referred to as the local computer; the computer accepting the connection is referred to as remote, or host computer. Telnet can provide access to many resources around the world, such as library catalogs, databases, and other internet tools and applications.

3. WAIS- WAIS is an internet search tool that has the capability of searching many databases at one time. WAIS can be accessed via telnet; gopher or a WAIS client program and increasingly, WAIS indexed databases are accessible through the WWW.

4. Gopher- Gopher is a protocol designed to search, retrieve and display documents from remote sites on the internet. In addition to document display and document retrieval, it is possible to initiate online connections with other systems via Gopher.

5. WWW- The World Wide Web is a system, based on hypertext and HTTP, for providing, organizing and accessing a wide variety of resources (text, images and sounds) that are available via the internet.

6. Usenet- Usenet is conceptually a huge bulletin board system. This allows us to send messages to a specific person or group. Network news lets one to send messages on an electronic bulletin board for any one to see. Both email and news groups are extremely useful internet tools.

7. Archie- Archie is a companion software tool to FTP. The Archie program searches a constantly updated index of FTP sites, file names and descriptions. Archie system help us to find information located anywhere on the internet.

8. Veronica-Veronica ("Very common rodent-oriented network index to computerized archives") is the companion tool to gopher. It is a search tool that allows one to quickly scan gopher for particular files and directories. It is program that one can access through gopher.

9. Email-It is the most commonly used application on the internet. The main attraction of email lies in its speed, it is much more powerful than paper mail. With the email we can send and receive anything we use or create on computer words, documents, Programmes, photos, images and sounds. It is much cheaper than other modes of communication services.

10. Chat & Instant Messaging

Chat programs allow users on the Internet to communicate with each other by typing in real time. They are sometimes included as a feature of a Web site, where users can log into the "chat room" to exchange comments and information about the topics addressed on the site. Chat may take other, more wide-ranging forms. For example, America Online is well known for sponsoring a number of topical chat rooms.

A variation of chat is the phenomenon of instant messaging. With instant messaging, a user on the Web can contact another user currently logged in and type a

conversation. Most famous is America Online's Instant Messenger. ICQ, MSN and Yahoo also offer chat programs.

2.0 Electronic Mail

Electronic mail or e-mail allows information to be sent between people and computers on the internet. It is the most widely used internet resource. Just as written letter can be sent to multiple recipients, an electronic mail message can be sent to one or more e-mail address. An e-mail address identifies a person and the computer for purpose of exchanging electronic mail messages. The basic structure of an e-mail address is:

Username@host.subdomain.second-level-domain.first-level-domain

Two examples based on the above structure are given below:

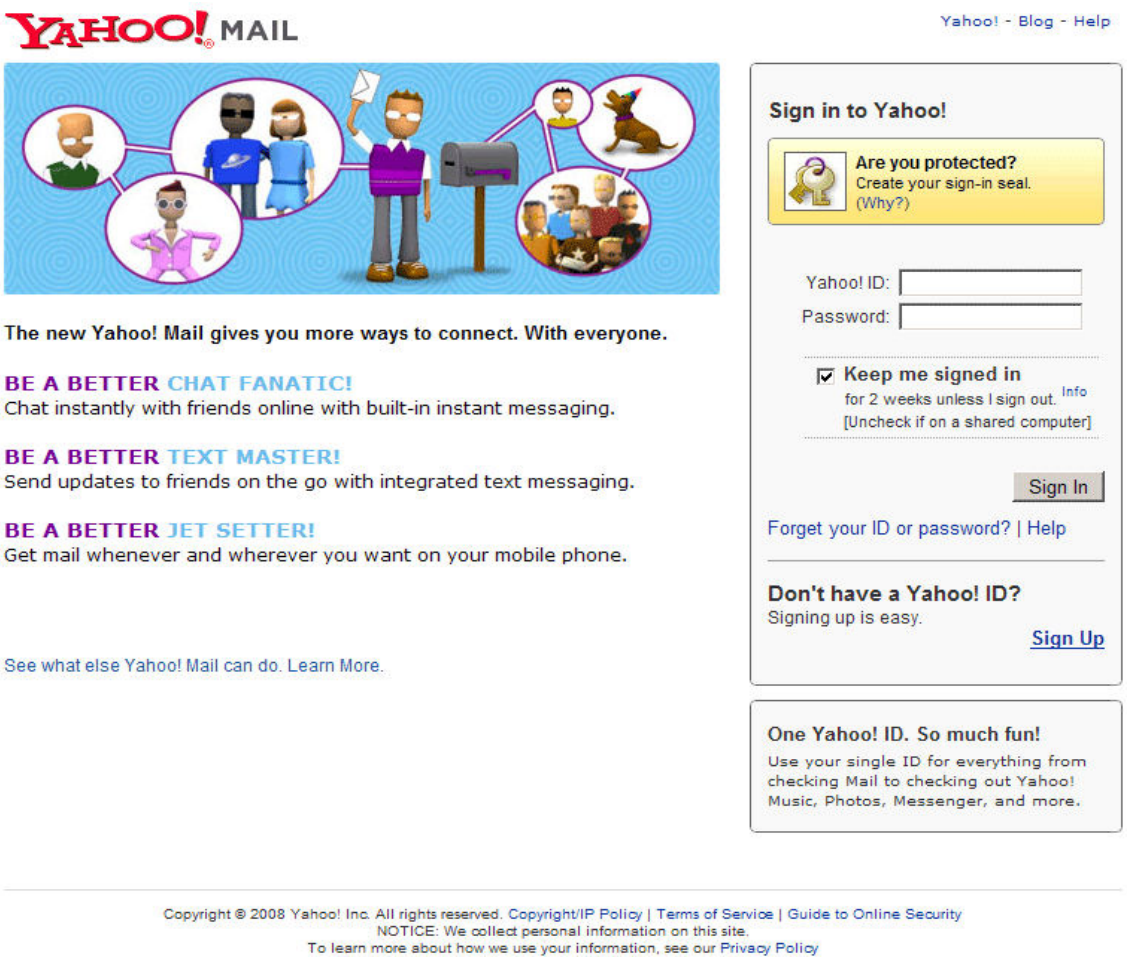
1. amit@giasmd01.vsnl.net.in
2. vishal11@yahoo.com

An e-mail address is read from left to right. For example vishal11@yahoo.com is read as vishal11at the yahoo dot com, where

- "Vishal" is the name of the person sending or receiving the message; this is referred to as the username.
- "Yahoo" is part of the domain name of the organization.
- "Com" is also part of the domain name and indicates that "yahoo" is a commercial organization.

The internet mail system works because of SMTP, Simple mail transfer protocol. SMTP is a part of the TCP/IP suite of protocols. SMTP is a protocol or set of rules that enable electronic mail to move smoothly through the internet. Because of SMTP, a Unix machine can send mail to a PC or Macintosh computer and Vice-Versa.

Electronic mail works on the client/server principle. A client program enables the user to interact with the server in order to access information and services on the server computer. To read and send mail user need to access the computer where their mail resides (the server). The client application is the interface which lets the user read, reply to, forward, compose and send new messages.



Yahoo Mail

2.1 Generic definition:

Email is an ambiguous term. Strictly speaking, email includes all technologies that support electronic transmission of text and graphics. Here is how the American Electronic Mail Association (EMA) defines it:

"Electronic Mail is the generic name for non-interactive communication of text, data, image or voice messages between a senders designated recipients by systems utilizing telecommunications links. Thus, telegraph, telex, voice-mail and computer based messaging systems (CBMS) fall within the preview of email."

1. **Non-interactive:-** There is no synchronous communication with each other. Other person may not be "on-line".
2. **Text, data, image or voice messages: -** All these can be transferred via email in case of voice mail; recorded voice messages take the place documents or letters.
3. Between senders & designated recipients: email messages are from machine to machine.

2.2 How does it work?

In a typical e-mail network, there is transfer of information between three computer systems your very own, the service provides and the receivers system. Imagine the first computer you have. You want to send, message to Bombay. You type out the message on your computer and into the computer belonging to the mail provider by dialing up. As soon as you have logged in, to the e mail provider he starts charging you. This is not be confused with the STD bill. As long as you plugged, you continually charged. The e-mail service provider you with identification number. This infact includes address of your mail box located at the vendor's machine. The message is transmitted and deposited into the mailbox of the recipient. As a user you are given a password by the vendor. You can access your mailbox and retrieve mail only after you given the password. Total secrecy is assured.

As a user, all you need is a modem, a computer terminal and a telephone line. This set up, called the front-end is connected to a location where e mail provider has installed computer capable of handling large amount of data. These computers have predestinated memory spices which are allotted to each local subscriber. These spices are called Mail Boxes. "Something at in to P .O. Box or a P .O. Bag".

Now let's see what a typical e mail message looks like. An e-mail is made up of two-parts, the header and the body.

1. The Header: The header consists of information about the sender and the recipient, the date and the subject. In addition Cc: option allows you to specify if you want carbon copies 'to be sent to one or more addresses.

2. The Body: It contains the text of the message. It is separated from the header by exactly one bland line. The message is normally ASCII mode. Binary data in data in raw form as also accepted by some systems. The maximum message size varies from 64 kb to 100 kb in most systems.

2.3 Functions of Email

There are only few basic functions in an e-mail and almost all mailers handle them. They are:

1. Read
2. Compose (new message)
3. Reply (to message you have received)
4. Forward (message you have received)
5. Refile (save the message away)
6. Delete

2.4 Advantages of using Email:

1. Managing Email is Easy:

You can manage all your correspondence on screen and so can your customers. Your proposal can be answered, revised, stored and sent to others, all without reams of paper involved.

2. Email is Fast:

Email is delivered instantly…from your office to anywhere in the world. No other method of delivery can provide this service. Timely buying and selling decisions can be made in a heartbeat.

3. Email is Inexpensive:

Compared to telephone calls, faxes or over night courier service, Email is less expensive.

4. Email is Easy to Filter:

The subject line on an Email makes it easy to prioritize messages. The reader can identify correspondence quickly and dealt with it immediately. Unlike regular mail which needs to be opened and reviewed or voice mail which requires you to either listen to or scan all your messages for those that require immediate attention.

5. Transmission is Secure and Reliable:

The level of security in transmitting Email messages is very high, and the industry continues to strive to develop even tighter security levels. Email is private. Often telephone and fax messages are not. If the address information is correct, rarely does an Email go astray. Fax machines can be out of order or out of paper and this prevents an important message from being delivered in a timely manner.

6. It's easy to send your message to more than one person.

You just type in several e-mail addresses. You can also keep mailing lists on your computer, which allows quick distribution to many people, thousands even.

7. Most e-mail systems have a reply button that enables you to include all or part of the original message when you are writing a reply. This feature is a small one, but it really speeds replying to messages. In composing a letter or even when making a phone call, people spend a lot of time establishing a context for your reply.

8. You can send letters, notes, files, data, or reports all use the same techniques. Once you learn how to use your email program, everything is sent the same way.

9. You don't have to worry about interrupting someone when you send email. The email is sent and delivered by one computer system communicating with the Internet. Although it is put into someone's mailbox, the recipient isn't interrupted by the arrival of email.

10. The cost to you for email has nothing to do with distance, and in many cases, the cost doesn't depend on the size of the message. Most Internet access charges are based on the number of hours per month you access the Internet, or you pay a flat monthly fee.

2.5 Limitations of email

1. Email isn't necessarily secure. Since messages are passed from one system to another, and sometimes through several systems or networks, there are many opportunities for someone to intercept or read email. Many types of computer systems have protections built in to stop users from reading others' email, but it's still possible for a system administrator to read the email on a system or for someone to bypass the security of a computer system.

2. Some email systems can send or receive text files only. Even though you can send and receive images, programs, files produced by word processing programs or multimedia messages, some folks may not be able to properly view your message.

3. it's difficult to express emotion using email. The recipient doesn't have the benefit of seeing your facial expressions or hearing your voice. You have to be careful with humor or sarcasm, since it's easy for someone to take your message the wrong way.

4. You can receive too much or unwanted email. You can receive "junk" email in the same way you receive other types of junk mail. On the Internet, junk mail is called ***spam.*** You may have to take active steps to delete the email you receive and try to stop it from being sent to you in the first place

5. You may not know about the person with whom you are communicating. The communication is often al in text and it's possible for us to get an incorrect impression of the person sending us email. Also, some people misrepresent themselves.

2.6 Email - Attachments

A powerful feature of electronic mail is the ability to attach text or graphics files created by other programs. Attachments are separate computer files attached to the e-mail message. The recipient can display, print or save the attachment as a separate document. You can use this feature to send draft documents to a co-author. They can read the document on their own computer, make changes, and return the edited version to you.

Text files - A basic text file **- .TXT**
Hypertext Markup Language (HTML) files - HTML is the language used to create Internet pages. Some email programs send messages in this format. **- .HTML** **- .HTM**
Word Processor files - Word processor programs are usually able to read each other's file format - They can also read the basic TXT, RTF and HTML files **- .DOC (MS Word)** **- .WPF (Word Perfect)** **- .PDF (Adobe Acrobat)** **- . RTF (Rich Text Format)**
Graphics (picture)files These are the most common graphics file formats **- .JPG**

- .MPG **- .GIF**
Executable Files (Programs) - May contain viruses - download at your peril - .EXE
Multiple File Extensions - Beware of files with multiple file name extensions. These are often virus-infected!

2.7 How to join an Email service

To join a public e mail network in India, you don't have to be a multinational company or an eccentric millionaire. Nor do you have to be a computer whiz.

1. **Special equipment:** All you need is PC, a telephone, a modem with its software and a healthy interest in the acquisition of information.
2. **Computer expert:** One has to be a computer expert in dealing the matter.
3. **MODEMS:** A device for connecting the PC to internet through telephone lines. Modem can be internal, which is fixed inside the computer itself, or it can be external which can be separately places outside the computer.
4. **Service provider:** The connection can be bought from any of the service provider Operating in the region. E.g. Glide, Bsnl etc

2.8 Email ETIQUETTE

Because email is so new, we have no hard and fast rules about what may be said in a message. These rules are evolving because of our increased use of email, as well as the advent of new technology that continually affects how we apply it. However, since this correspondence is owned by the business, some general rules of etiquette should be observed.

1. Be brief and to the point: A long email message, just like a long letter, is hard to wade through. Most email messages are short. One line may be enough; two pages are usually too much.

Some people write long messages in an effort to avoid being misunderstood. However, this may produce exactly the opposite effect: people will skim the message and pick whatever point catches their attention.

2. Organize the message: Facilitate the reading of the message by stating its main point early (in the first sentence or paragraph) and placing details in the middle. For those rare messages that are quite lengthy, include an overview, headers and a summary.

3. Use a descriptive subject line: If you use a descriptive subject line to tell the readers what the email is about, you will get the interested readers to open and read the rest of the email. Try to give the readers enough information in the subject line for them to act upon it. However, don't write too long a subject line, as most email programs limit what will show up in the inbox window.

4. Format text for professional appearance: Fonts and colors are a nonverbal component of an email. For most business email, use a simple font and black text. Colored text and script fonts create a less formal feeling, so use them wisely with careful consideration of the reader and of the message you want to **send**.

5. Be friendly and courteous: Because email developed as a casual form of communication, we tend to be less careful about what we write. We actually need to be extra careful because email lacks body language and speech inflection, which provide valuable communication clues in a face-to-face conversation.

Extra care should be taken to make email friendly and courteous. A seemingly neutral message may be received more negatively than you would like. Therefore, you should use common courtesies, such as please and thank you

As a receiver of email, always be sure to give correspondents the benefit of the doubt when unsure about their mood. If a message's meaning is ambiguous, ask for clarification before jumping to conclusions.

6. Restrict messages to those who "need to know": Limit the recipients of an email message. Define and narrow your audience to those who truly need the information you are sending.

7. Keep it Simple: don't use exotic features of your word processing software like bold, italics etc. resist the temptation. They may not travel well across protocol of different networks and may show up terribly on the recipient terminal.

8. Identify yourself: Make up a signature block that contains appropriate contact information and append it to your emails. The signature block should include your full name and may include your organization, title, telephone number, fax number or postal address.

9. Attach wisely and sparingly: Attachments can be a source of frustration and even destruction when not used properly. When sending an attachment, try to use a platform that allows your recipient to open the attachment the first time. Don't send a large file without warning the recipient first.

10. Be careful with icons and graphics: Icons and graphics can also be sources of frustration because they can trip up servers. If you use them, be sure they are clean, simple, and well-designed. If your message is professional, your icons and graphics should look the part.

11. Use the reply function: Automatic quoting is a unique capability within email that enables maintaining a record of conversations without retyping anything. This

feature allows you to include the context from previous messages to facilitate picking up the thread of the conversation.

Sometimes, typing your response after each quoted question is helpful. Other times, confining all of your responses to a single paragraph is a more appropriate strategy. You may want to preview your strategy to a reader so they don't miss any important information.

However, remember to quote only those elements of that message that will facilitate the understanding of the reply. Delete any portions that are not relevant.

Also, use the reply function only when you are actually replying to the message you have received. Don't use it as an easy way to enter an email address when you intend to discuss a completely different topic.

12. Don't use emoticons: Emoticons are symbols put together to look like sideways smiley faces, sad faces, etc. In business communication, use emoticons only when you know the correspondent well enough to be informal.

3.0 Summary

In this lesson, we have discussed the Internet, its working, protocols and the various services provided by the Internet. We have also discussed the concept of Electronic mail in detail.

4.0 Keywords

Internet, DNS, IP address, TCP/IP, Email, Attachments

5.0 Self Check Exercise

Q.1 What is Internet? Discuss the various services provided by the internet.

Q.2 What is an Email? What are its function and advantages?

Q.3 Write short notes on the following:

TCP/IP

Email ETIQUETTE

6.0 Suggested Readings

- “Internet for everyone” by Leon & Leon, APH publishing corporation, New Delhi
- "The ABCs of Internet" by Christian Crumlish, Sybex
- "The Internet Book" by Douglas Comer, Prentice Hall.
- Computer network & internets by D.E. Comer, Pearson Education