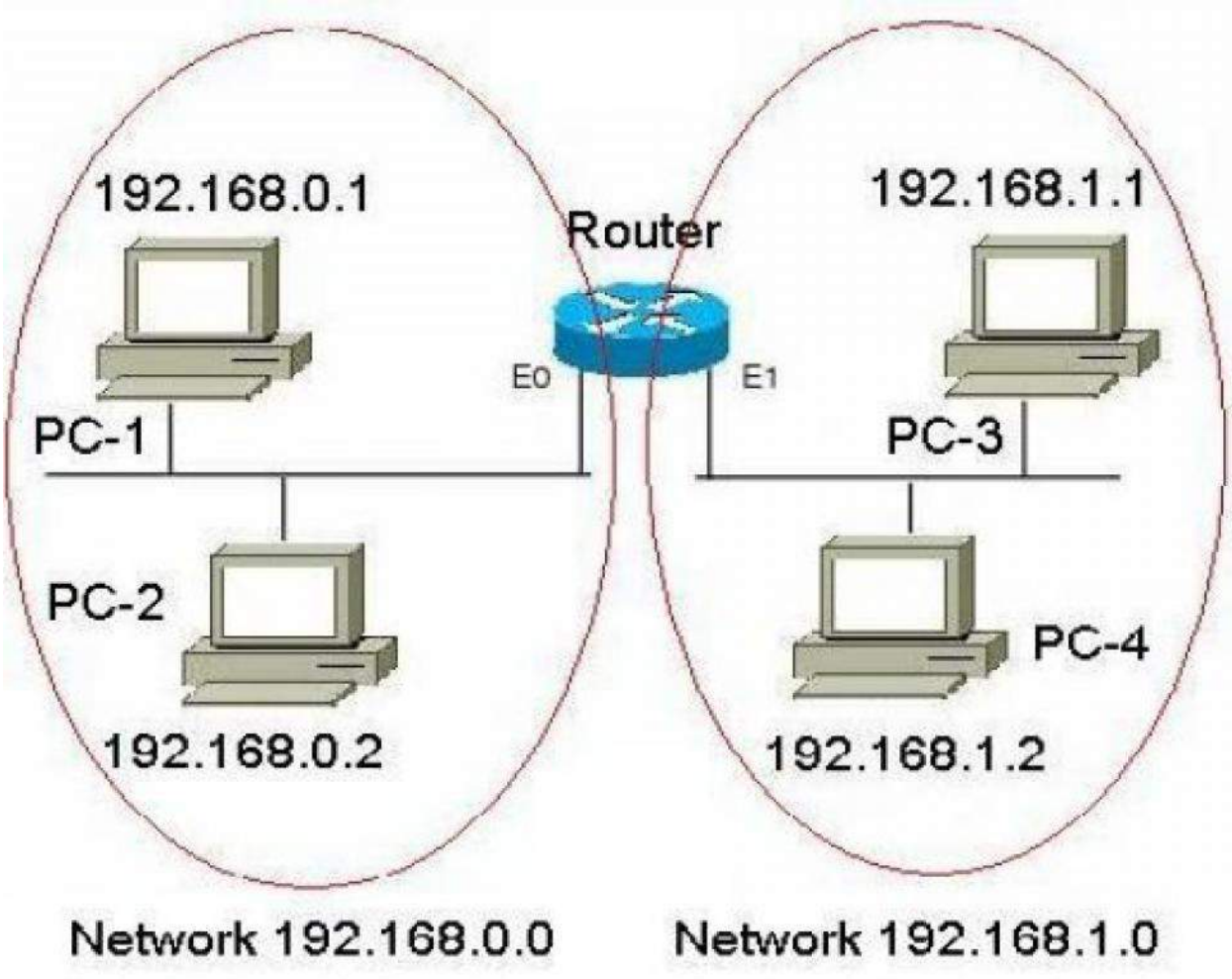
CHAPTER 15

Networking concepts

OBJECTIVES

- **To understand uses of networking.**
- **Various types of networking.**
- **To understand various devices used in networking.**
- **Applications used for networking**
- **How and methods of networking security.**



15.1 Introduction

A Network is an inter-connection of autonomous computers. Two computers are said to be interconnected if they are capable of exchanging the information. Central to this definition is the fact that the computers are autonomous. This means that no computers on the network can start, stop or control another.

15.1.1 Network Goals:

The network goals are as listed below.

(i) Resource Sharing: The aim is to make all the programs, data and peripherals available to anyone on the network irrespective of the physical location of the resources and the user.

(ii) Reliability: A file can have copies on two or three different machines, so if one of them is unavailable, the other copies could be used. For military, banking and many other applications it is great of importance.

(iii) Cost Factor: Personal computers have better price/performance ratio than micro computers. So it is better to have PC's, one per user with data stored on one shared file server machine.

(iv) Communication Medium: Using a network, it is possible for managers, working far apart, to prepare financial report of the company. The changes at one end can be immediately noticed at another and hence it speeds up co-operation among them.

15.1.2 Need of Networking:

1. File sharing provides sharing and grouping of data files over the network.
2.Print sharing of computer resources such as hard disk and printers etc.
3. email tools for communication with the e-mail address.
4. Remote access able to access data and information, around the globe.
5.Sharing database to multiple users at the same time by ensuring the intergrity.

15.2.1 ARPANET

The Advanced Research Projects Agency Network (ARPANET) was one of the world's first operational packet switching networks, the first network to implement TCP/IP, and the progenitor of what was to become the global Internet. The network was initially funded by the Advanced Research Projects Agency (ARPA, later DARPA) within the U.S. Department of Defense for use by its projects at universities and research laboratories in the US. The packet switching of the

ARPANET, together with TCP/IP, would form the backbone of how the Internet works.

15.2.2 OSI Reference Model

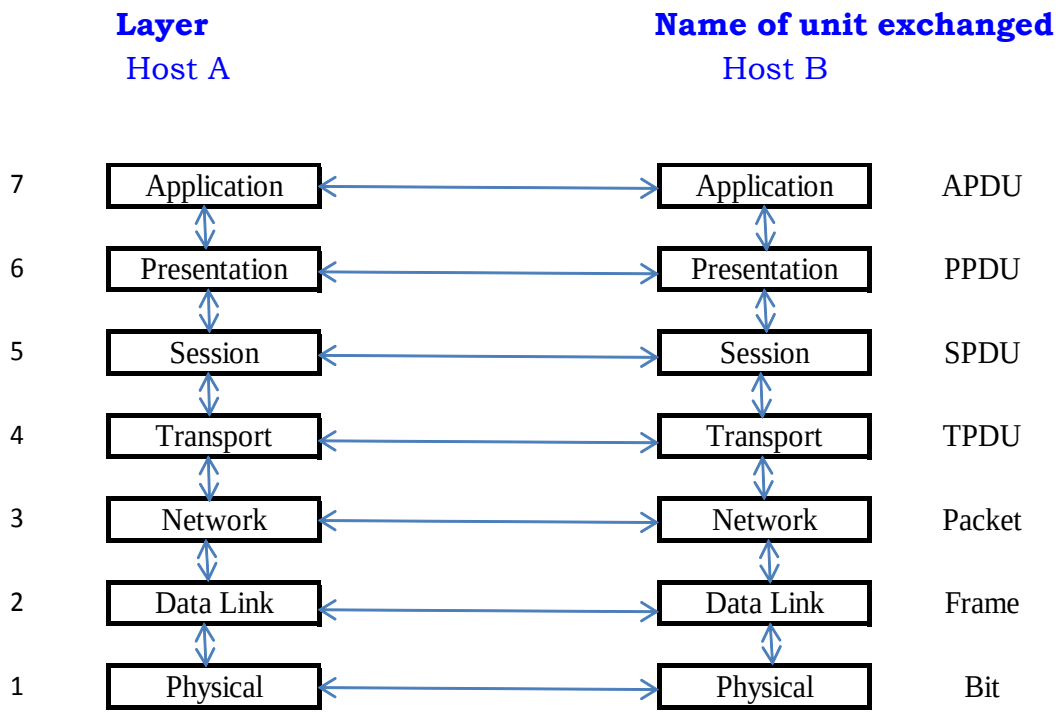


Figure 15.1 OSI Layers

The Physical Layer

The physical layer is concerned with transmitting raw bits over a communication channel. It also deals with mechanical, electrical and timing interfaces.

The Data Link Layer

The main function of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer.

The Network Layer

The network layer controls the operation of the subnet. The main function is to determine how packets are routed from source to destination.

The Transport Layer

The basic function of transport layer is to accept data from above layer and split it up into smaller units if needed, and pass these to the network layer and ensure that the pieces all arrive correctly at the other end. It also determines type of services to provide to the session layer.

The Session Layer

The session layer allows users on different machines to establish sessions between them. It includes dialog control, token management and synchronization.

The Presentation Layer

The presentation layer concerned with the syntax and semantics of the information transmitted concerned with moving bits around the layer.

The Application Layer

The application layer contains a variety of protocols that are commonly needed by the user. For example, HTTP (Hyper Text Transfer Protocol) which is the bases for the World Wide Web (WWW) to access web pages.

15.2.3 TCP/IP (Transmission Control Protocol/Internet Protocol)

TCP/IP is a layered set of protocols. This protocol assumes that there is a way to communicate reliably between the two computers. Mail, like other application protocols, simply defines a set of commands and messages to be sent. TCP is responsible for making sure that the commands get through to the other end. It keeps track of what is sent, and retransmits anything that did not get through.

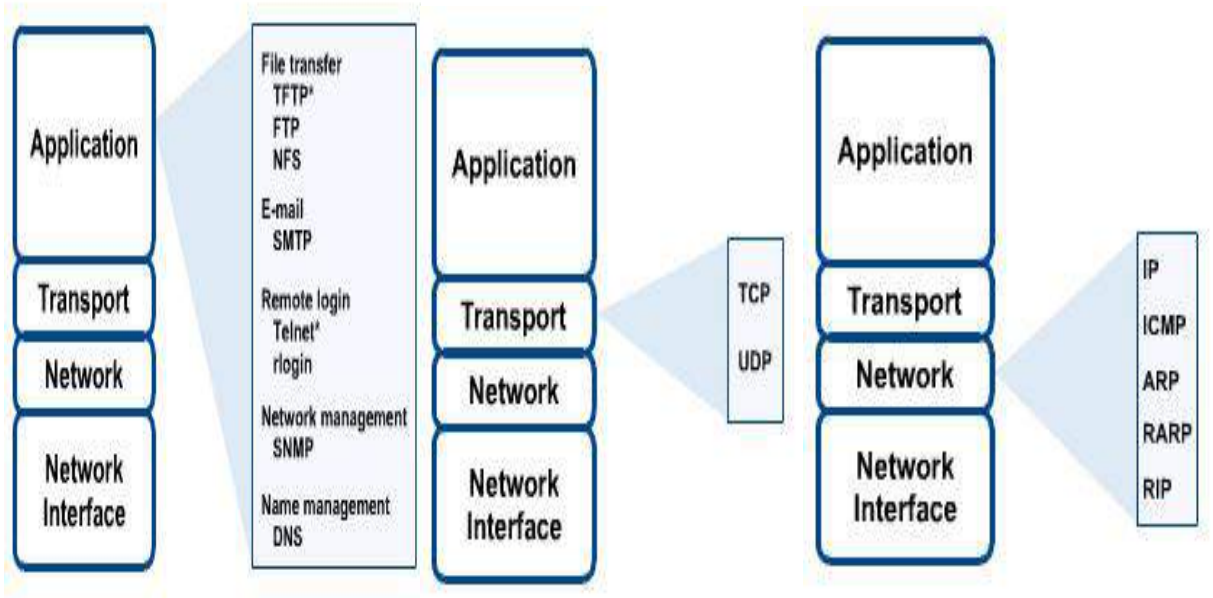


Figure 15.2 TCP/IP Layers

TCP/IP is the base communication protocol of the internet. The part of TCP/IP uses numeric IP addresses to join network segments and TCP part of TCP/IP provides reliable delivery messages between networked computers. It is based on the “catenet model”. This model assumes that there are a large number of independent networks connected together by gateways. The user should be able to access computers or other resources on any of these networks. Datagram will often pass through a dozen different networks before getting their final destination. The routing needed to accomplish this should be completely invisible to the user. As far as the user is concerned, all he need to know is "Internet address", in order to access another system. This is an address that looks like 128.64.194.1. It is actually a 32 bit number. However it is normally written as 4 decimal numbers, each representing 8 bits of the address. (The term “octet” is used by Internet documentation for such 8 bit chunks. The term “byte” is not used, because TCP/IP is supported by some computers that have byte sizes other than 8 bits).

Generally the structure of the address gives you some information about how to get to the system. We normally refer to systems by name, rather than by Internet address. When we specify a name, the network software looks it up in a database, and comes up with the corresponding Internet address. Most of the network software deals strictly in terms of the address. TCP/IP is built on “connection less” technology. Information is transferred as a sequence of “data grams”.

Each of these datagrams is sent through the network individually. There are provisions to open connections (i.e., to start a conversation that will continue for sometime). However at some level, information from those connections is broken up into datagrams, and those datagrams are treated by the network a completely separate. For example, suppose you want to transfer a 15000 octet file. Most networks can’t handle a 15000 octet datagram. So the protocols will break this up into something like thirty 500 octet datagrams each. Each of these datagrams will be sent to the other end. At that point, they will be put back together into the 15000 octet file. However while those datagrams are in transmit, the network doesn’t know that there is any connection between them. It is perfectly possible that datagram 14 will actually arrive before datagram 13. It is also possible that somewhere in the network, an error will occur, and some datagram won’t get through at all. In that case, that datagram has to be sent again. Note by the way that the terms datagram and packet often seem to be nearly interchangeable. Technically, data gram is the right word to use when describing TCP/IP.

A data gram is a unit of data, which is what the protocols deal with.

A packet is a physical thing, appearing on an Ethernet or some wire.

In most cases a packet simply contains a data gram, so there is very little difference. However they can differ at times.

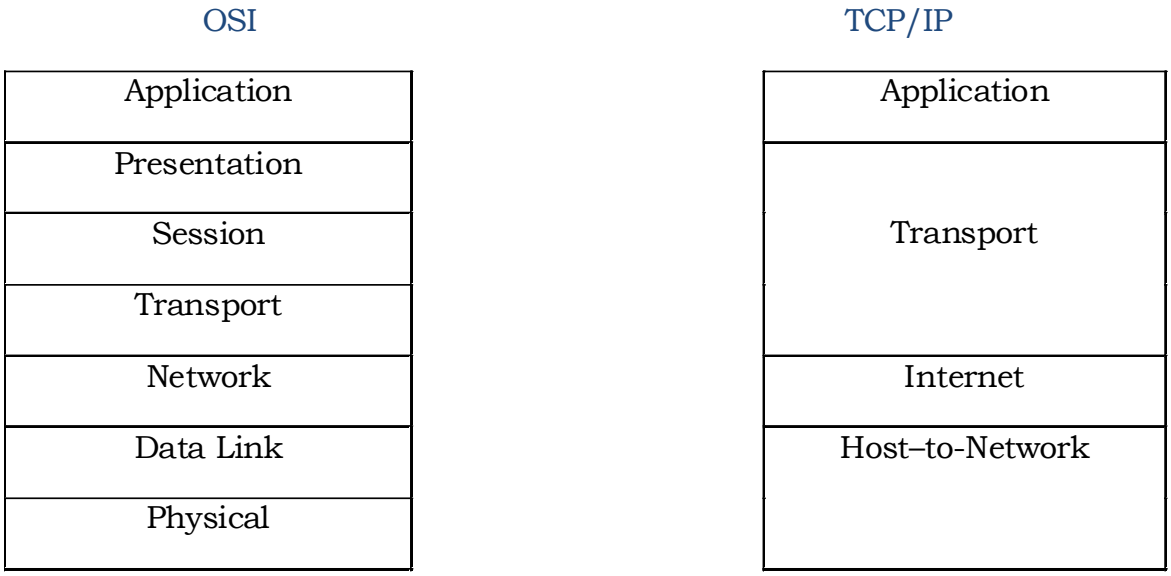


Figure 15.3 OSI and TCP comparetive layers

15.3.1 HTTP (Hypertext Transfer Protocol)

The Hypertext Transfer Protocol (HTTP) is an application-level protocol with the lightness and speed necessary for distributed, collaborative, hypermedia information systems. HTTP allows an open-ended set of methods to be used to indicate the purpose of a request. It builds on the discipline of reference provided by the Uniform Resource Identifier (URI), as a location URL or name (URN) for indicating the resource on which a method is to be applied. Messages are passed to HTTP in a format similar to that used by internet mail and Multipurpose Internet Mail Extensions (MIME).

The HTTP has various built-in request methods which allow users to read a web page, or to read a web page's header, or to store a web page, or to append to a named resource or to remove the web page or to connect two existing resources or to break an existing connection between two resources.

15.3.2 FTP (File Transfer Protocol)

One of the original services on the internet was designed to allow for transferring files from one system to another. It goes by the name *ftp* which stands for file transfer protocol. Files of any type can be transferred, although you may have to specify whether the file is an ASCII or Binary file. They can be transferred to any system on the internet provided that the permissions are set accordingly.

Advantages of FTP

(i) It is very useful to transfer the files from one network to another.

(ii) It is an effective way to get a geographically dispersed group to co-operate on a project.

(iii) It is popular way to share information over the internet. FTP works as a client/server process.

15.3.3 SLIP/PPP (Serial Line Internet Protocol)

Serial line IP (SLIP) was the first protocol for relaying the IP packets over dial-up lines. It defines an encapsulation mechanism, with little ease. There is no support for dynamic address assignment, link testing or multiplexing different protocols over a single link. SLIP has been largely supplanted by PPP.

PPP (Point to Point Protocols)

PPP is the internet standard for transmission of IP packets over serial lines. The PPP is currently the best solution for dial-up internet connections, including ISDN. PPP is a layered protocol, starting with a link control protocol (LCP) for link establishment, configuration and testing. Once the LCP is initialized, one or many of several network control protocols (NCPs) can be used to transport traffic for a particular protocol suite. The IP Control Protocol (IPCT), permits the transport of IP packets over a PPP link. PPP supports both synchronized and unsynchronized lines.

15.4.1 THE INTERNET

The Internet is a worldwide network of computer networks that evolved from the first network ARPAnet (Advanced Research Projects Agency network). The internet is made up of many networks each run by a different company and interconnected at peering points. It is an interconnection of large and small

networks around the globe. The common use of Internet standards allows users connected to one network to communicate with users on another network.

15.4.2 THE INTERSPACE

InterSpace is a client/server software program that allows multiple users to communicate online with real-time audio, video and text chat in dynamic 3D environments. InterSpace provides the most advanced form of communication available on the Internet today.

15.4.3 Elementary Terminology of Networks

Let us have a look at some typical hardware components of network.

(i) Nodes (Workstations)

The term nodes refer to the computer that are attached to a network and are seeking to share the resources of the network. Of course, if there were no nodes, there would be no network at all.

(ii) Server

Servers can be of two types: (1) non-dedicated servers and (2) dedicated servers

15.4.4 Types of Servers

Non-dedicated Servers

On small networks, a workstation that can double as a server is known as non-dedicated server since it is not completely dedicated to the cause of serving. Such servers can facilitate the resource-sharing among the work stations on a proportionately smaller scale. Since one computer works as a work station and as well as server, it is slower and requires more memory. The networks using such a server are known as **PEER-TO-PEER** networks.

Dedicated Servers

On bigger network installations, there is a computer reserved for server's job and its only job is to help workstations access data, software and hardware resources. It does not double-up as a workstations and such a server is known as dedicated server. The networks using such server are known as MASTER-SLAVE networks.

On a network, there may be several servers that allow the workstations to share specific resources. For example, there may be a server exclusively for serving files related request like storing files, deciding about their access privileges and regulating the amount of space allowed for each user. This server is known as **file server**. Similarly there may be **printer server** and **modem server**. The

printer server takes care of the printing requirements of a number of **workstations and the modem server** helps a group of network users use a modem to transmit long distance messages.

15.4.5 TYPES OF NETWORKS

A computer network means a group of networked components, i.e., computers that are linked by means of a communication system. A network can mean a small group of linked computers to a chain of a few hundred computers of different types (e.g., PCs, minis, mainframes, etc) spread around the world. Thus, networks vary in size, complexity and geographical spread. Mostly, computers are classified on the basis of geographical spread and on this basis, there can be 3 types of networks:

- Local Area Networks (LANs)
- Wide Area Networks (WANs)
- Metropolitan Area Networks (MANs)

Local Area Networks (LANs)

Small computer networks that are confined to a localized area (e.g., an office, a building or a factory) are known as Local Area Networks (LANs). The key purpose of a LAN is to serve its users in resource sharing. The hardware as well as software resources are shared through LANs. For instance, LAN users can share data, information, programs, printer, hard disks, modems, etc.

In a typical Lan configuration, one computer is designated as the file server. It stores all of the software that controls the network, as well as the software that can be shared by the computers attached to the network. Computers connected to the file server are called workstations. The workstations can be less powerful than the file server and they may have additional software on their hard drives. On most LANs, cables are used to connect the network interface cards in each computer.

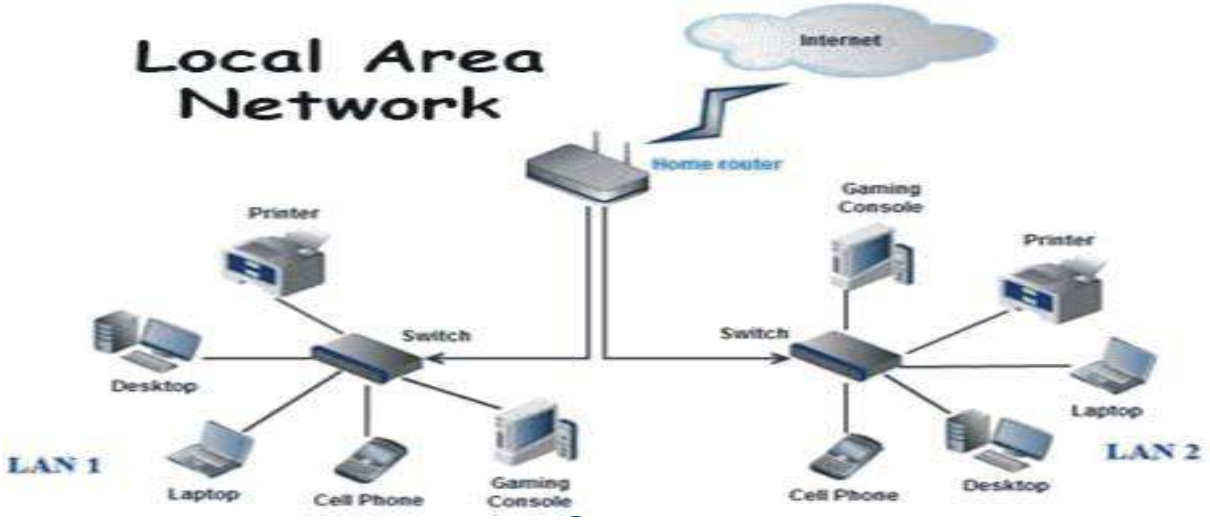


Figure 15.4 LAN topology

Metropolitan Area Networks (MANs)

Metropolitan Area Networks (MANs) are the networks spread over a city. For example, cable TV networks that are spread over a city can be termed as Metropolitan Area Networks (MANs). The purpose of a MAN is also the sharing of the hardware and the software resources among its users.

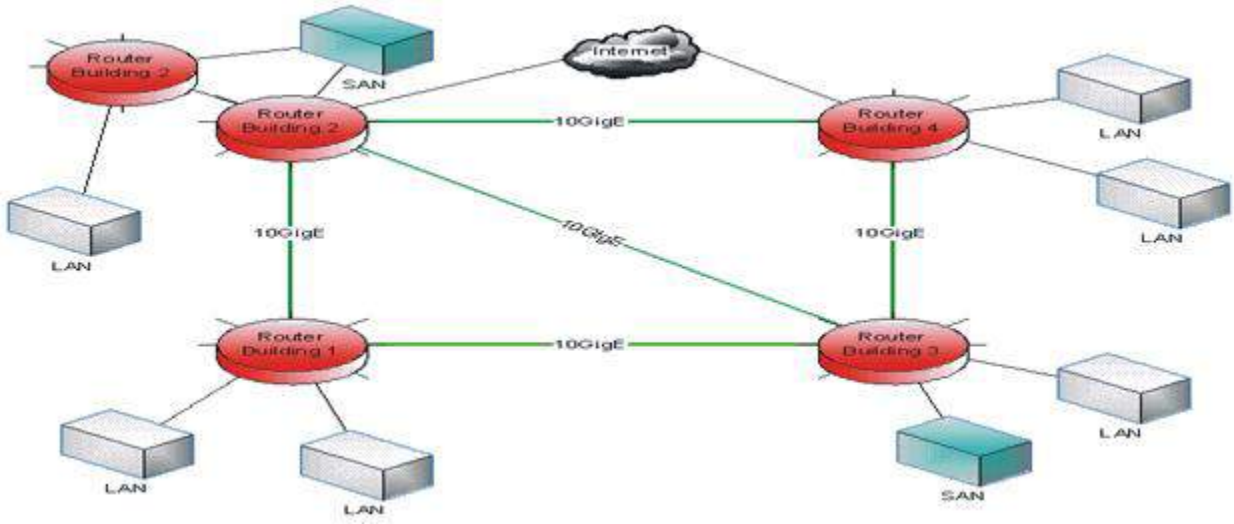


Figure 15.5 MAN topology

Wide Area Networks (WANs)

The networks spread across the countries are known as WANs. A Wide Area Networks (WANs) is a group of computers that are separated by large distances and tied together. It can even be a group of LANs that are spread across several locations and connected together to look like one big LAN. The

WANs link computers to facilitate fast and efficient exchange of information at lesser cost and higher speeds.

Computers connected to a Wide Area Networks (WANs) are often connected through public networks, such as the telephone system. Sometimes they can be connected through leased lines or satellites. The largest WAN in existence is the internet.

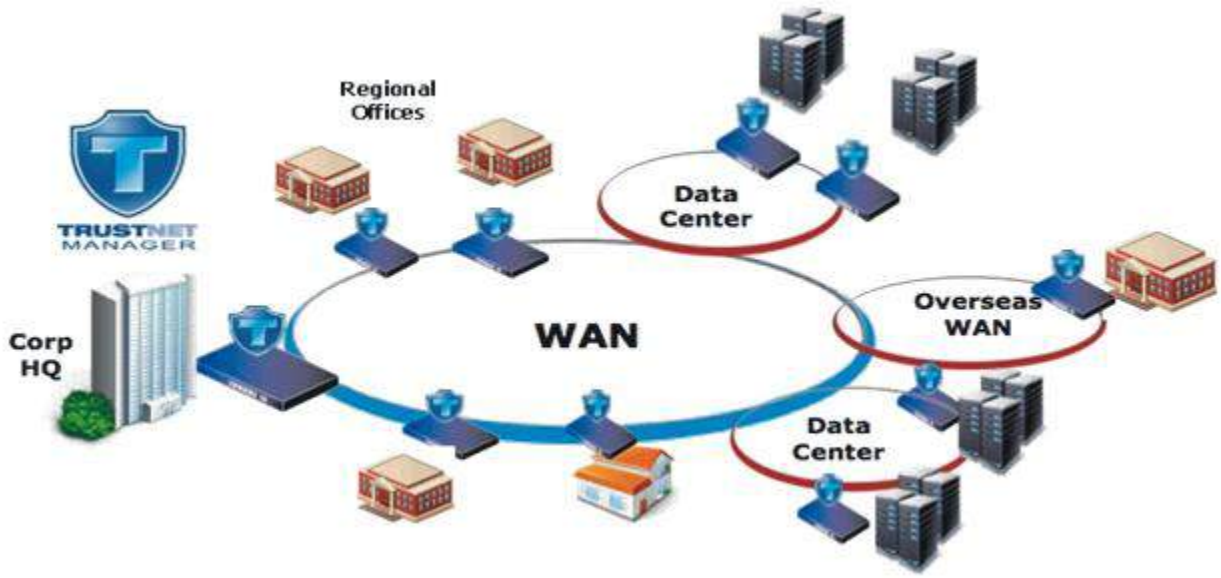


Figure 15.6 WAN topology

Difference between a LAN and a WAN

The next task is to distinguish between LANs and WANs. LANs are different in the following important respects.

1. The distance between the nodes is limited. There is an upper limit of approximately 10Kms and a lower limit of 1 meter.

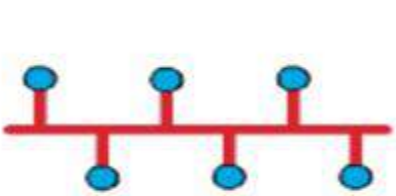
2. While WANs usually operate at speeds of less than 1 mbps (one mega bits per second), LANs normally operate at between 1 and 10 mbps. Using optical fiber technology, it is possible to achieve space of the order of hundreds of mbps.

3. Because of the short distances involved, the error rates in LANs are much lower than in WANs. LANs error rate is thousand times lower than in WANs, so are normal.

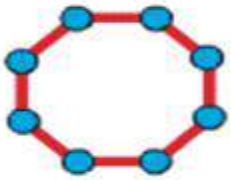
4. The distance limitations involved in LANs normally mean that the entire network is under the ownership and control of a single organization. This is in sharp contrast to WANs, where the network is normally operated by the countries post and telecommunications authorities rather than by its users.

	LAN	WAN
1	Diameter of not more than a few kilometers.	Span entire countries.
2	A total data rate of at least several mbps.	Data rate less than one mbps.
3	Complete ownership by a single organization.	Owned by multiple organizations.
4	Very low error rates.	Comparatively higher error rates.

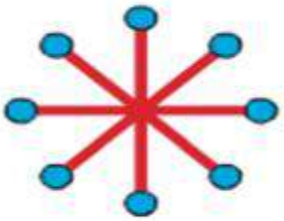
15.4.6 NETWORK TOPOLOGIES: The actual appearence or layout of networking



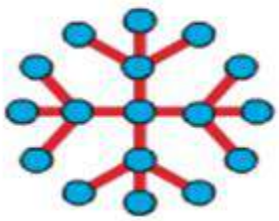
Bus Topology



Ring Topology



Star Topology



Extended Star Topology

Mesh Topology

The Star Topology

This topology consists of a central node to which all other nodes are connected by a single path. It is the topology used in most existing information networks involving data processing or voice communications.

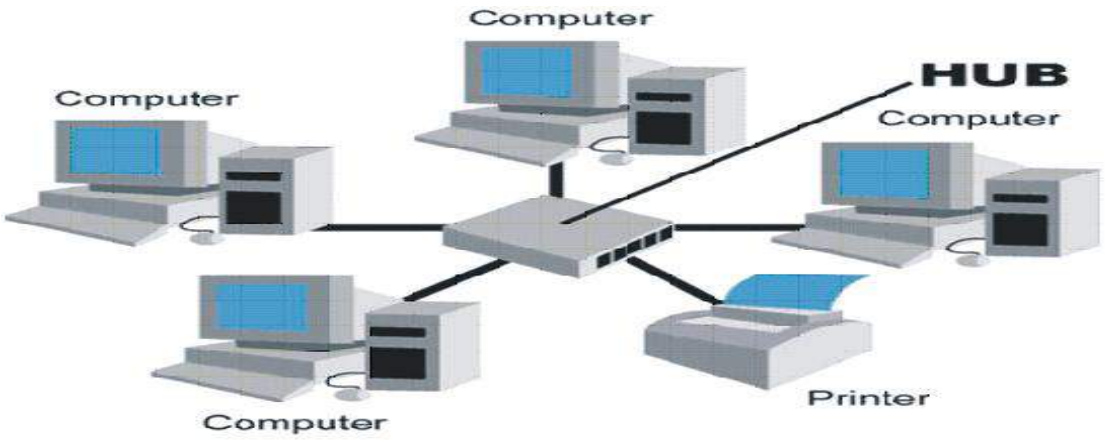


Figure 15.7 STAR topology with hub

Advantages of the Star topology

1. Ease of service. The star topology has a number of concentration points (where connections are joined). These provide easy access for service or reconfiguration of the network.
2. One device per connection. Connection points in any network are inherently prone to failure. In the star topology, failure of a single connection typically involves disconnecting one node from an otherwise fully functional network.

The Bus or Linear Topology

Another popular topology for data networks is the linear. This consists of a single length of the transmission medium (normally coaxial cable) onto which the various nodes are attached. The topology is used in traditional data communication network where the host at one end of the bus communicates with several terminals attached along its length.

The transmission from any station travels the length of the bus, in both directions, and can be received by all other stations. The bus has terminators at either end which absorb the signal, removing it from the bus.

Data is transmitted in small blocks, known as packets. Each packet has some data bits, plus a header containing its destination address. A station wanting to transmit some data sends it in packets along the bus. The destination device, on identifying the address on the packets, copies the data on to its disk.

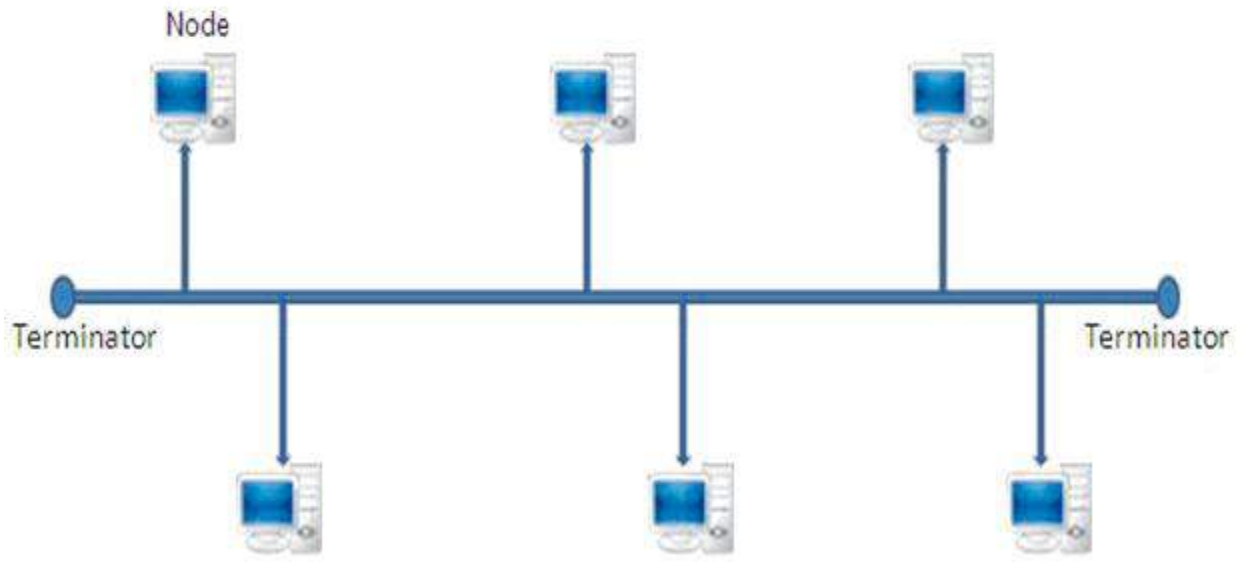


Figure 15.8 Linear topology

Advantages of the linear topology

1. Short cable length and simple wiring layout. Because there is a single common data path connecting all nodes, the linear topology allows a very short cable length to be used. This decreases the installation cost, and also leads to a simple, easy to maintain wiring layout.

2. Resilient Architecture. The LINEAR architecture has an inherent simplicity that makes it very reliable from a hardware point of view. There is a single cable through which all the data propagates and to which all nodes are connected.

3. Easy to extend. Additional nodes can be connected to an existing bus network at any point along its length. More extensive additions can be achieved by adding extra segments connected by a type of signal amplifier known as repeater.

Disadvantages of the linear topology

1. Fault diagnosis is difficult. Although simplicity of the bus topology means that there is very little to go wrong, fault detection is not a simple matter. Control of the network is not centralized in any particular node. This means that detection of a fault may have to be performed from many points in the network.

2. Fault isolation is difficult. In the star topology, a defective node can easily be isolated from the network by removing its connection at the center. If a node is faulty on the bus, it must be rectified at the point where the node is connected to the network.

3. Repeater configuration. When BUS type network has its backbone extended using repeaters, configuration may be necessary.

4. Nodes must be intelligent. Each node on the network is directly connected to the central bus. This means that some way of deciding who can use the network at any given time must be performed in each node.

The Ring or Circular topology

The third topology that we will consider is the ring or the circular. In this case, each node is connected to two and only two neighboring nodes and is transmitted onwards to another. Thus data travels in one direction only, from node to node around the ring. After passing through each node, it returns to the sending node, which removes it.

It is important to note that data gets through rather than travels past each node. This means that the signal may be amplified before being repeated on the outward channel. node to node around the ring. After passing through each node, it returns to the sending node, which removes it.

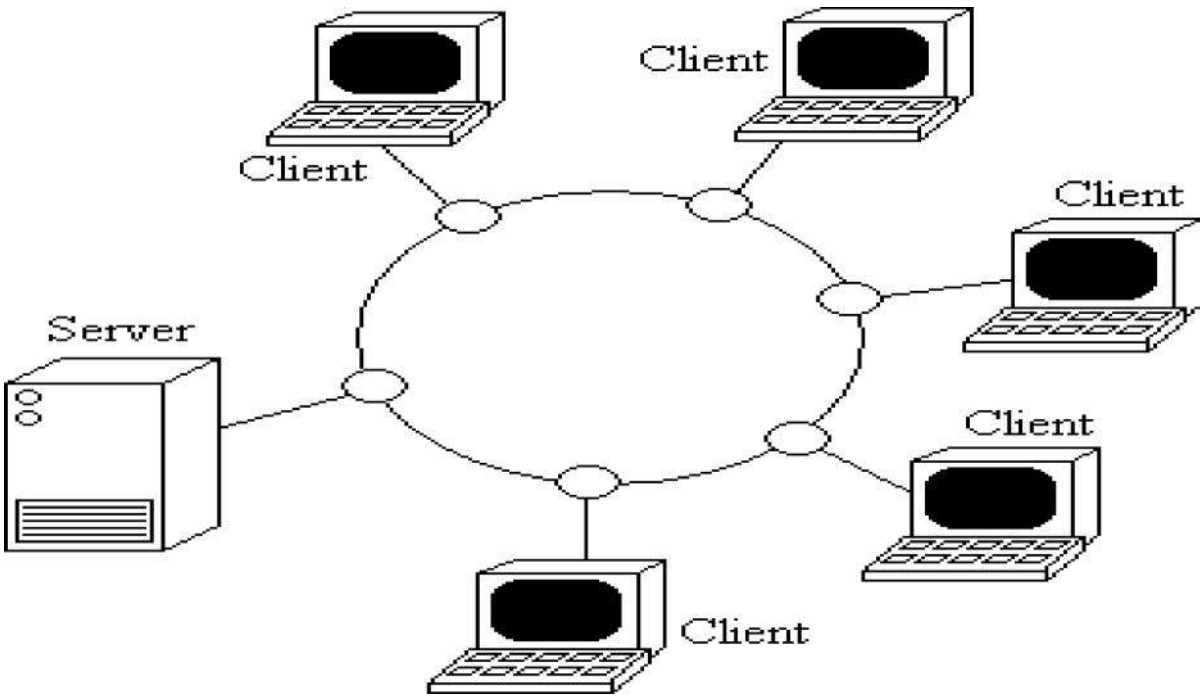


Figure 15.9 Ring topology

Figure 15.10 Ring topology

Advantages of the Ring topology

1. Short cable length. The amount of cabling involved in a ring topology is comparable to that of a bus and is small relative to that of a star. This means that less connections will be needed, which will in turn increase network reliability.

2. No wiring closet space required. Since there is only one cable connecting each node to its immediate neighbors, it is not necessary to allocate space in the building for wiring closet.

3. Suitable for optical fibers. Using optical fibers offers the possibility of very high speed transmission. Because traffic on a ring travels in one direction, it is easy to use optical fibers as a medium of transmission.

Disadvantages of the Ring topology

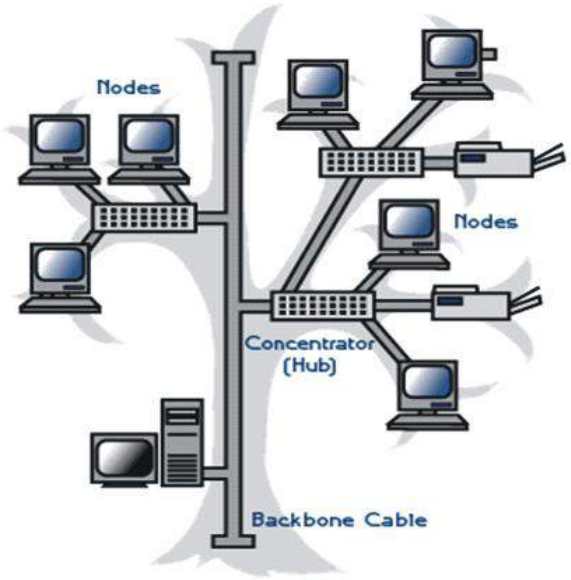
1. Node failure causes network failure. The transmission of data on a ring goes through every connected node on the ring before returning to the sender. If one node fails to pass data though itself, the entire network has failed and no traffic can flow until the defective node has been removed from the ring.

2. Difficult to diagnose faults. The fact that failure of one node will affect all others has serious imprecations for fault diagnosis. It may be necessary to examine a series of adjacent nodes to determine the faulty one. This operation may also require diagnostic facilities to be built into each node.

3. Network reconfiguration is difficult. It is not possible to shut a small section of the ring while keeping the majority of it working normally.

The Tree Topology

A variation of bus topology is the tree topology. The shape of the network is that of an inverted tree with the central root branching and sub branching to the extremities of the network.



Transmission in this topology takes place in the same way as in the bus topology. In both cases, there is no need to remove packets from the medium because when a signal reaches the end of the medium, it is absorbed by the terminators. Tree topology is best suited for the applications which have a hierarchical flow of date and control. Since the tree topology is a modification of a pure network topology, bus topology, it is a hybrid topology.

Figure 15.11 Tree topology

Graph Topology

In this topology, nodes are connected together in an arbitrary fashion. A link may or may not connect two or more nodes. There may be multiple links also. It is not necessary that all the nodes are connected. But if a path can be established in two nodes via one or more links is called a connected graph.

Mesh Topology

In this topology, each node is connected to more than one node to provide an alternative root in the case the host is either down or too busy. It is an extension to P-P network.

The mesh topology is excellent for long distance networking because it provides extensive backup, rerouting and pass through capabilities. Communication is possible between any two nodes on the network either directly or by passing through. This function is needed in the event of a line or node failure anywhere in the network. The mesh topology is commonly used in large internetworking environments with stars, rings and buses attached to each node. This is also idle for distributed networks.

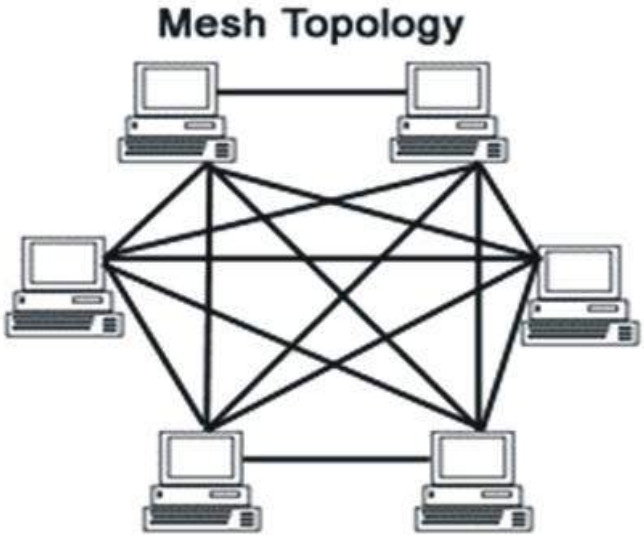


Figure 15.12 Mesh topology

When in a network each host is connected to other directly i.e., there is a direct link between each host, then the network is said to be fully connected. This characteristic is termed as full connectivity.

15.4.8 TRANSMISSION MEDIUM

By transmission media or communication channels of network, it is meant that the connecting cables or connecting media are being talked about. The cables that connect two or more workstations are the communication channels.

TWISTED PAIR CABLE

The most common form of wiring in data communication application is the twisted pair cable. As a **Voice Grade Medium** (VGM), it is the basis for most internal office telephone wiring. It consists of two identical wires wrapped together in a double helix.

Problems can occur due to differences in the electrical characteristics between the pair (e.g., length, resistance, and capacitance). For this reason, LAN applications will tend to use a higher quality cable known as D**ata Grade Medium** (DGM).

Different types and categories of twisted-pair cable exist, but they all have two things in common:

a. The wires come in pairs

b. The pairs of wires are twisted around each other

ADVANTAGES:

1. It is simple and physically flexible.
2. It can be easily connected.
3. It is easy to install and maintain.
4. It has a low weight.
5. It is inexpensive.

DISADVANTAGES:

1. Its low bandwidth capabilities make it unsuitable for broadband applications.
2. Because of high attenuation, it is incapable of carrying a signal over long distances without the use of repeaters.
3. It supports maximum data rates 1 Mbps without conditioning and 10 Mbps with conditioning.

Types of Twisted Pair Cables

There are two types of twisted pair cables available. These are

(i) **Unshielded Twisted Pair (UTP) Cable:** UTP cabling is used for variety of electronic communications. It is available in the following five categories:

Type	Description
CAT1	Voice-grade communications only; No data transmission
CAT2	Data-grade transmission up to 4 Mbps
CAT3	Data-grade transmission up to 10 Mbps
CAT4	Data-grade transmission up to 16 Mbps
CAT5	Data-grade transmission up to 1000 Mbps

The UTP cables can have maximum segment length of 100 meters.

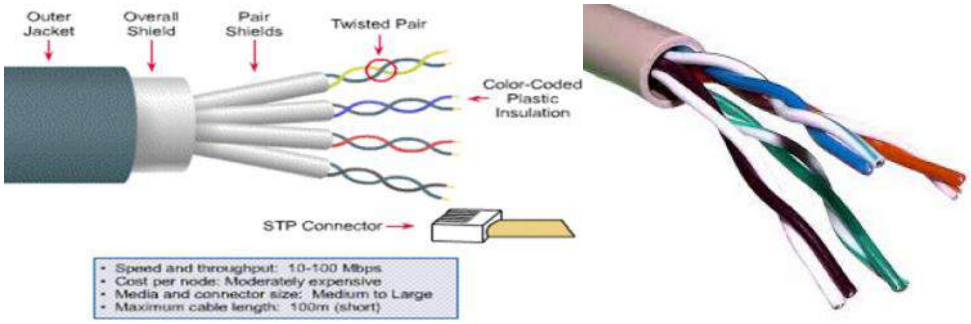


Figure 15.13 UTP cables

Figure 17.13 UTP cables

(ii) **Shielded Twisted Pair (STP) Cable:** This type of cables comes with shielding of the individual pairs of wires, which further protects it from external interference. But these also, like UTP, can have maximum segment length of 100 meters. The advantage of STP over UTP is that it offers greater protection from interference and crosstalk due to shielding. But it is definitely heavier and costlier than UTP and requires proper grounding at both the ends.

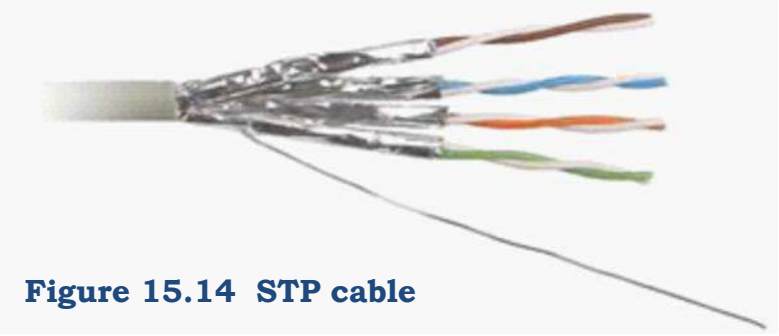


Figure 15.14 STP cable

Types of Coaxial Cables

The two most commonly used types of coaxial cables are **Thicknet** and **Thinnet.**

(i) **Thicknet:** This form of coaxial cable is thicker than thinet. The thicknet coaxial cable segments can be upto 500 meters long.

(ii) **Thinnet:** This form of coaxial cable is thinner and it can have maximum segment length of 185 meters i.e, using this cable, nodes having maximum distance of 185 meters can be joined.

Optical Fibers

Optical Fibers consist of thin strands of glass or glass like material which are so constructed that they carry light from source at one end of the fiber to a detector at the other end. The light sources used are either light emitting diodes (LEDs) or laser diodes (LDs). The data to be transmitted is modulated onto the light beam using frequency modulation techniques. The signals can then be picked up at the receiving end and demodulated. The bandwidth of the medium is potentially very high. For LEDs, this range between 20 and 150 mbps and higher rates are possible using LDs.

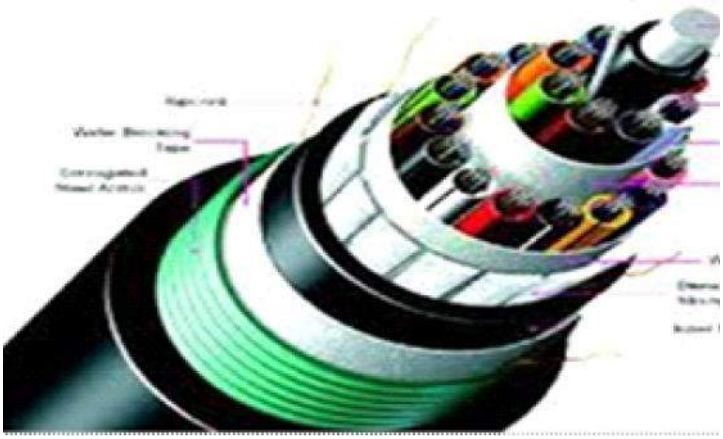


Figure 15.15 OPTICAL Fibers

Advantages:

1. It is immune to electrical and magnetic interference i.e., noise in any form because the information is travelling on a modulated light beam.
2. It is highly suitable for harsh industrial environments.
3. It guarantees source transmission and has a very high transmission capacity.
4. Fiber optic cables can be used for broadband transmission where several channels (i.e., bands of frequency) are handled in parallel and where it is

2. Signals from one signal antenna may split up and propagate by slightly different paths to the receiving antenna. When these out of phase signals recombine, they interfere, reducing the signal strength.
3. Microwave propagation is susceptible to weather effects like rains, thunder storms, etc.
4. Bandwidth allocation is extremely limited.
5. The cost of design, implementation and maintenance of microwave links is high.

Radio Wave

The transmission making use of radio frequencies is termed as radio-wave transmission.

Any radio setup has two parts:

- The **transmitter**
- The **receiver**

The transmitter takes some sort of message (it could be the sound of someone's voice, pictures for a TV set, data for a radio modem or whatever), encodes it onto a sine wave and transmits it with radio waves. The receiver receives the radio waves and decodes the message from the sine wave it receives. Both the transmitter and receiver use antennas to radiate and capture the radio signal.

ADVANTAGES:

1. Radio-wave transmission offers mobility.
2. It proves cheaper than digging trenches for laying cables and maintaining repeaters and cables if cables get broken by a variety of causes.
3. It offers freedom from land acquisition rights that are required for laying, repairing the cables.
4. It offers case of communication over difficult terrain.

DISADVANTAGES:

1. Radio-wave communication is an insecure communication.
2. Radio-wave propagation is susceptible to weather effects like rains, thunder storms, etc.

Security of such communication links is almost nonexistent. Even so, the equipment has many advantages and is widely used by taxi repair, courier and delivery services.

Satellite (Satellite Microwave)

Radio wave can be classified by frequency and wave length. When the frequency is higher than 3 GHz, it is named microwave. Satellite communication is special case of microwave relay system. Satellite communication use the synchronous satellite to relay the radio signal transmitted from ground station. In recently, the use of wireless communication has gained more popularity. Compared to the traditional fixed wire terrestrial networks, satellite and microwave communications network features the time saving, fast implementation and broad coverage characteristics. It provides voice, fax, data and video services as well as email, file transfer, WWW internet applications. When fixed wire terrestrial communication networks are crushed by a disaster, the satellite and microwave system as a emergency backup facility will be stressed.

In satellite communication the earth station consists of a satellite dish that functions as an antenna and communication equipment to transmit and receive data from satellites passing overhead.

A number of communication satellites, owned by both government and private organizations, have been placed in stationary orbits about 22,300 miles above the earth's surface. These satellites act as relay stations for communication signals. The satellites accept data/ signals transmitted from an earth station, amplify them, and retransmit them to the other side of the earth in only one step.

Most communication satellites have multiple, independent reception and transmission devices known as transponders. In a commercial communication satellite, a single transponder is usually capable of handling a full-colour, commercial television transmission, complete with audio. Transponders for data transmission may be even larger. Some firms that market satellite communication service own a satellite. Others lease a portion of a satellite and provide transmission facilities in smaller units to ultimate users. The security in satellite transmission is usually provided by the coding and decoding equipment. Satellite communication has a number of advantages.

ADVANTAGES:

1. The area coverage through satellite transmission is quite large.
2. The laying and maintenance of intercontinental cable is difficult and expensive and this is where the satellite proves to be the best alternative.
3. The heavy usage of intercontinental traffic makes the satellite commercial attractive.

4. Satellites can cover large areas of the earth. This is particularly useful for sparsely populated areas.

DISADVANTAGES:

1. Technological limitations preventing the deployment of large, high gain antennas on the satellite platform.
2. Over-crowding of available bandwidths due to low antenna gains.
3. The high investment cost and insurance cost associated with significant probability of failure.
4. High atmospheric losses above 30 GHz limit carries frequencies.

Other Unguided Media

Apart from microwaves, radio waves and satellites, two other unguided media are also very popular. These are **infrared** and **laser** waves.

1. Infrared

This type of transmission uses infrared light to send the data. The infrared light transmits data through the air and can propagate throughout a room (bouncing off surfaces), but will not penetrate walls. The infrared transmission has become common in PDAs (Personal Digital Assistants) e.g., hand held devices like palm pilots etc. The infrared transmission is considered to be secure one.

2. Laser

The Laser transmission requires direct line-of-sight. It is unidirectional like microwave, but has much higher speed than microwaves. The laser transmission requires the use of a laser transmitter and a photo-sensitive receiver at each end. The laser transmission is point-to-point transmission, typically between buildings. But lasers have a certain disadvantage, which is: it can be adversely affected by weather.

15.4.9 SWITICHING TECHNIQUES

Different types of switching techniques are employed to provide communication between two computers. These are **circuit switching, message switching** and **packet switching**.

Circuit Switching

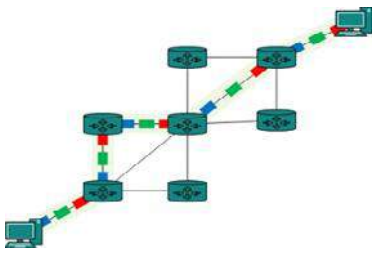


Figure 15.16 Circuit

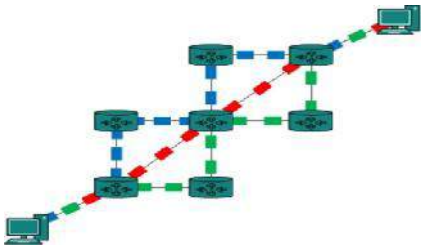
In this technique, first the complete physical connection between two computers is established and then data are transmitted from the source computer to the destination computer. That is, when a computer places a telephone call, the switching equipment within the telephone system seeks out a physical copper path all the way from sender telephone to the receiver's telephone. The important property of this

switching technique is to setup an end to end path (connection) between computers before any data can be sent.

Message Switching

In this technique, the source computer sends the data or the message to the switching office first, which stores the data in the buffer. It then looks for a free link to another switching office and then sends the data to this office. This process is continued until the data is delivered to the destination computers. Owing to its working principle, it is also known as **store and forward**. That is, store first (in switching office), forward later, one jump at a time.

Figure 15.17 Message



Packet Switching

With message switching, there is no limit on block size, in contrast, packet switching places a tight upper limit on block size. A fixed size of packet which can be transmitted across the network is specified.

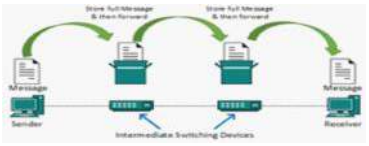


Figure 15.18 Packet

15.4.10 Communication Modes

The communication mode defines in which data can flow depending upon the type media used. They are Simplex, Half Duplex and Full Duplex.

Simplex

On this panel there is only one interface that is a transmitter and all other interfaces is a receiver. The full bandwidth is completely for signals travelling across transmitter to receiver or receivers. On this channel transmitting interface cannot receive and receiving interface cannot transmit. For example Radio, TV, etc uses Simplex channels.

Half Duplex

On this channel each interface works as transmitter and receiver, but only one interface can transmit at a time. The full bandwidth of a channel is available to the transmitting interface which will not receive while transmitting. Generally it is used in Walkie-Talkies, Marine/Aviation, etc use Half Duplex channel.

Full Duplex

This channel has two ends, each serving as transmitter and receiver. Each interface can transmit and receive at the same time. The modern telephone system use Full Duplex channels. It is more expensive due to hardware for increased number of channels and bandwidth.

15.4.11 NETWORK DEVICES

In functioning of networks, many devices play important roles. Here, in this section we are going to discuss a few of them.

Modem (Modulator and Demodulator)

Modems allow you to combine the power of your computer with the global reach of the telephone system.

Because ordinary telephone lines cannot carry digital information, a modem changes the digital data from your computer into analog data, a format that can be carried by telephone lines. In a similar manner, the modem receiving the call then changes the analog signal back into digital data to the computer. This shift of digital data into analog data back again, allows two computers to communicate with one another, called modulation or demodulation.

With a modem you can send faxes to the office or important customers without leaving your computer. And with an online or internet connection, you can share recipes with fellow gourmets catch up on the latest news, view a weather map from Singapore, keep in touch with distant friends by electronic mail, the World Wide Web and much more.

Working on Modem

Modem converts digital signals to A/F (audio frequency) tones which are in the frequency range that the telephone lines can transmit and also it can convert transmitted tones back to digital information.

After the power is turned On in DTE (Data Terminal Equipment) and DCE (Data Communication Equipment), the terminal runs for self check, it asserts the Data Terminal Ready (DTR) signal to tell the modem that it is ready.

When modem is powered up and ready to transmit data, the modem will assert the Data Set Ready (DSR) signal to the terminal. Under the manual or terminal control the modem dials up the computer on the other end. If the computer is available it will send back a specified tone.

Now when the terminal has a character ready to send, it will assert the Request-To-Send (RTS) signal to the modem. The modem assert its Carrier Detect (CD) signal to the terminal to indicate that it has established contact with the computer. When the modem is fully ready to transmit the data it asserts Clear-To-Send (CTS) signal back to the terminal. The terminal then sends serial data characters to the modem. When the terminal has sent all the characters, it needs to make its RTS signal high. This causes the MODEM to unasserted its CTS signal and stop transmitting. Similar handshakes occur between modem and computers on other side also.

Modems are of two types :

1.Internal modems: The modems that are fixed within the computer.

2.External modems: The modems that are connected externally to a computer as other peripherals are connected.

Ethernet Card

As mentioned earlier, Ethernet is a LAN architecture developed by Xerox Corp in association with DEC and Intel. Ethernet uses bus or star topologies and can support data transfer rates of up to 10 Mbps.

The computers that are part of Ethernet have to install a special card called Ethernet card.

An Ethernet card contains connections for either Coaxial or Twisted pair cables (or both). 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 optic cables to an Ethernet card. When this connection is used, there is always an external transceiver attached to the workstation. These days many computers include an option for a pre-installed Ethernet Card.

Hub

A hub is a hardware device used to connect several computers together. A hub that contains multiple independent but connected modules of network and internetworked equipment. A similar term is concentrator. 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.

Basically, hubs are multi slot concentrators into which a number multi port cards can be plugged to provide additional access as the network grows in size.

Hubs can be either passive or active.

1. **Active Hubs:** Electrically amplify the signal as it moves from one connected device to another. Active concentrators are used like repeaters to extent the length of a network.
2. **Passive Hubs:** Allow the signals to pass from one computer to another without any change.

Hubs usually can support 8, 12 or 24 RJ-45 ports. These are often used in a star or star wired ring topology and requires specialized software for port management.

Switch

A switch is a device that is used to segment networks into different sub networks called subnets or LAN segments. Segmenting the network into smaller subnets prevents traffic overloading in a network.

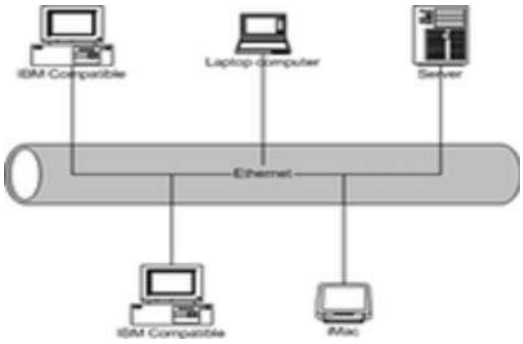


Figure 15.19 Modem with systems

A switch is responsible for filtering i.e., transforming data in a specific way and for forwarding packets (a piece of message being transmitted) between LAN segments. Switch support any packets protocol.

LANs that are segmented through switches are called switched LANs. In the case of Ethernet LANs, they are called switched Ethernet LANs.

How a switch functions

To insulate the transmission from the other ports, the switch establishes a temporary connection between the source and destination and then terminates the connection once the conversation is done.

Repeater

A repeater is a device that amplifies a signal being transmitted on the network. It is used in long network lines, which exceed the maximum rated distance for a single run.

Over distance, the cables connecting a network lose the signal transmitted. If the signal degrades too much, it fails to reach the destination. Or if it does arrive, the degradation of the message makes it useless. Repeaters can be installed along the way to ensure that data packets reach their destination. Repeaters are of two kinds: **amplifier and signal repeater**. The first merely amplifies all incoming signals over the network. However, it amplifies both the signal and any concurrent noise. The second type collects the inbound packet and then retransmits the packet as if it were starting from the source station.

Bridge

A bridge is a device that lets you link two networks together. Bridges are smart enough to know which computers are on which side of the bridge, so they allow only those messages that need to get to the other side of the bridge. As a packet arrives at the bridge, the bridge examines the physical destination address of the packet. The bridge then decides whether or not to let the packet cross.

Router

A device that works like a bridge but can handle different protocols is known as a router. For example, a router can link Ethernet to a mainframe.

If the destination is unknown to a router it sends the traffic (bound to unknown destination) to another router (using logical addresses) which knows the destination. A router differs from a bridge in a way that former uses logical addresses and the latter uses physical addresses.

How a Router functions

Compared to the hubs and switches, routers are smarter. Routers use a more complete packet address to determine which router or workstation should receive each packet next. Based on a network road map called a routing table, routers can help ensure that packets are travelling the most efficient paths to their destinations. If a link between two routers fails, the sending router can determine an alternate route to keep traffic moving.

15.5.1 Gateway

A Gateway is a device that connects dissimilar networks. A gateway operates at the highest layer of network abstraction. It expands the functionality of routers by performing data translation and protocol conversion. It is needed to convert Ethernet traffic from the LAN, to SNA (Systems Network Architecture) traffic on a legacy system. It then routes the SNA traffic to the mainframe. When the mainframe answers, the reverse process occurs.

A gateway is actually a node on a network that serves as an entrance to another network. In enterprises, the gateway is the computer that routes the traffic from a workstation to the outside network that is serving the web pages. In homes, the gateway is the ISP that connects the user to the internet.

In enterprises, the gateway node often acts as a proxy server (a machine that is not actually a server but appears as a server) and a firewall (a system designed to prevent unauthorized access to or from a private network). The gateway is also associated with both a router, which use headers and forwarding tables to determine where packets are sent, and a switch, which provides the actual path for the packet in and out of the gateway.

Wireless Vs Mobile Computing

Wireless refers to the method of transferring information between a computing device, such as Personal Data Assistant (PDA) and a data source, such as an agency data base server, without a physical connection. Wireless communication is simply data communication without the use of the physical connectivity. Not all wireless communications technologies are mobile.

Mobile simply describing a computing device that is not restricted to a desktop. A mobile device may be a PDA, a small cell phone or web phone, a laptop computer or any other of numerous other devices that allow the user to complete the computing task without being tethered, or connected to a network.

Mobile computing does not necessarily require wireless communication. Infact, it may not require communication between devices at all.

Wireless communication is simply data communication without the use of landlines. This may involve cellular telephone, two way radio, fixed wireless, LASER or satellite communications. Here the computing device is continuously connected to the base network.

Mobile or untethered, computing means that the computing device is not continuously connected to the base or central network. Mobile devices include PDAs, Laptop computers and many of today's cell phones. These products may communicate with a base location with or without a wireless connection.

GSM

GSM is short for Global System for Mobile communications, which is one of the leading digital cellular systems. The GSM standard for digital cell phones was established in Europe in the mid 1980s.

In covered areas, cell phone users can buy one phone that will work anywhere where the standard is supported. To connect to the specific service providers in these different countries, GSM uses simply switch Subscriber Identification Module (SIM) cards. SIM cards are small removable disks that slip in and out of GSM cell phones. They store all the connection data and identification numbers you need to access a particular wireless service provider.

GSM uses narrow band (TDMA), which allows eight simultaneous calls on the same radio frequency. TDMA is short for (Time Division Multiple Access), a technology for delivering digital wireless service using Time Division Multiplexing. TDMA works by dividing a radio frequency into time slots and then allocating slots to multiple calls. In this way, a single frequency can support multiple, simultaneous data channels. GSM operates in the 900 MHz and 1800 MHz bands.

15.6.1 What is a SIM card?

The SIM – Subscriber Identity Module – is a chip card, the size of a postage stamp. A SIM is a tiny computer chip that gives a cellular device its unique phone number. It has memory, a processor and the ability to interact with the

user. Current SIMs typically have 16 to 64 Kb of memory, which provides plenty of room for storing hundreds of personal phone numbers, text messages and other data.

CDMA

CDMA is short Code Division Multiple Access, a digital cellular technology that uses spread spectrum techniques. Unlike competing systems, such as GSM, that use TDMA, CDMA does not assign a specific frequency to each user. Instead, every channel uses the full available spectrum. Individual conversations are encoded with a pseudo random digital sequence. CDMA is a form of spread spectrum, which simply means that data is sent in small pieces over a number of the discrete frequencies available for use at any time in the specified range. All of the users transmit in the same wide band chunk of spectrum. Each user's signal is spread over the entire bandwidth by a unique spreading code. At the receiver end, that same unique code is used to recover the signal.

WLL (Wireless in local loop)

Wireless in local loop (WLL or WILL), is meant to server subscribers at homes or offices. Wireless in local loop is analogous with local telephone service, but much more capable. A WLL system serves a local area by deploying multiplicity of multi channel transmit/receive bases stations (transceivers) that are within line of site of the intended customers. Each customer is equipped with a mini station of low power, into which the telephone is connected. The WLL unit consists of a radio transceiver and the WLL interface assembled in box. Two cables and a telephone connector are the only outlets from the box; one cable connects to a directional antenna and a phone receptable to connect to a common telephone set. Example, a fax or modem could also be connected for fax or computer communication.

When calls are made from the telephone, it signals the base station for a connection, which is subsequently established through a switch center, exactly as in conventional telephony. An incoming call is identified at the switch center and rooted to the base station assigned to serve the telephone being called. The wireless connection is then made, and the call is completed in a conventional manner.

The WLL system can operate with GSM handsets/mobile units, as well as with GSM compatible subscriber units. The system is transparent to the central office and subscribers, and interfaces with the most standard central office switches and subscriber telephone equipment.

Advantages of WLL

(i) WLL facilities do not significantly suffer from weather damage, vandalism and accidents.
(ii) WLL system offers better bandwidth than traditional telephone systems.
(iii) WLL system has much better bandwidth, superior customer service features and quality can be provided.

15.7.1 GPRS

GPRS is the abbreviation for General Packet Radio Service. GPRS is used for wireless communication using a mobile device. With this service you can access the internet, send emails and large data, real time news, download games and watch movies.

How does GPRS work?

You must be aware of how files are transferred from one location to another on your computer. They are broken down into packets and sent across. Similarly GPRS also uses the same function to transfer data through a network. The information is split into the smaller units or packets and sent through the network and is reassembled at the receiving end. GPRS provides a high speed data transfer, typically between 56 kilo bits per second to 114 kilo bits per second. A user of the GPRS network is charged only on the amount data is sent or received as opposed to the duration of the connection.

1G, 2G, 3G, 4G and 5G Networks

The “G” in wireless networks refers to the “generation” of the underlying wireless network technology. Technically generations are defined as follows.

1G Networks:

(NMT,C-Nets, AMPS, TACS) are considered to be the first analog cellular systems, which started early 1980s. There were radio telephone systems even

before that. 1G networks were conceived and designed purely for voice calls with almost no consideration of data services.

2G Networks:

(GSM, CDMAOne, D-AMPS) are the first digital cellular systems launched early 1990s, offering improved sound quality, better security and higher total capacity. GSM supports circuit switched data (CSD), allowing users to place dial-up data calls digitally, so that the networks switching station receives actual ones and zeros rather than the screech of an analog modem.

2.5G Networks: (GPRS, CDMA2000 1x) are the enhanced versions of 2G networks with theoretical data rates upto about 144k bit/s. GPRS offered the first always on data service.

3G Networks:

(UMTS FDD and TDD, CDMA 2000 1x EVDO, CDMA 2000 3x, TD-SCDMA, EDGE) are newer cellular networks that have data rates of 384k bit/sec and more. The UN's IMT – 2000 standard requires stationary speeds of 2Mbps and mobile speeds of 384kbps for a "true" 3G.

3G is a specification for the third generation (analog cellular was the first generation, digital PCS the second) of mobile communications technology. 3G promises increased bandwidth, up to 384 Kbps when a device is stationary or moving at pedestrian speed, 128 Kbps in a car and 2Mbps in fixed applications. UMTS (Universal Mobile Telecommunication System) is a broadband, packet–based transmission of text, digitized voice, video, and multimedia at data rates up to and possibly higher than 2 megabits per second (Mbps).

4G Network:

Based on the requirements for seamless interaction between networks, 4G is characterized by the following key attributes:

(i) **Support for Multiple Applications and Services** — Efficient support for unicast, multicast and broadcast services and the applications that rely on them. Prompt enforcement of Service Level Agreements (SLA) along

with privacy and other security features. Minimally, service classes include delay sensitive, loss sensitive, delay and loss sensitive and best effort.

(ii) Quality of Service — Consistent application of admission control and scheduling algorithms regardless of underlying infrastructure and operator diversity.

(iii) Network Detection and Network Selection — A mobile terminal that features multiple radio technologies or possibly uses software- defined radios if economical, allows participation in multiple networks simultaneously, thereby connecting to the best network with the most appropriate service parameters (cost, QoS and capacity among others) for the application. This requires establishing a uniform process for defining eligibility of a terminal to attach to a network and to determine the validity of link layer configuration.

5G Network:

The cellular concept was introduced in 5G Technology stands for 5th Generation Mobile technology. 5G technology has changed the means to use cell phones within very high bandwidth. User never experienced ever before such a high value technology. Nowadays mobile users have much awareness of the cell phone (mobile) technology. The 5G technologies include all type of advanced features which makes 5G technology most powerful and in huge demand in near future.

A new mobile generation has appeared every 10th year since the first 1G system (NMT) was introduced in 1981, including the 2G (GSM) system that started to roll out in 1992, 3G (W-CDMA/FOMA), which appeared in 2001, and "real" 4G standards fulfilling the IMT-Advanced requirements, that were ratified in 2011 and products expected in 2012-2013. Predecessor technologies have occurred on the market a few years before the new mobile generation.

KEY CONCEPTS OF 5G:

- Real wireless world with no more limitation with access and zone issues.
- Wearable devices with AI capabilities.
- Internet protocol version 6 (IPv6), where a visiting care-of mobile IP address is assigned according to location and connected network.
- One unified global standard.
- Pervasive networks providing ubiquitous computing: The user can simultaneously be connected to several wireless access technologies and

seamlessly move between them. These access technologies can be a 2.5G, 3G, 4G or 5G mobile networks, Wi-Fi, WPAN or any other future access technology. In 5G, the concept may be further developed into multiple concurrent data transfer paths.

• Cognitive radio technology, also known as smart-radio: allowing different radio technologies to share the same spectrum efficiently by adaptively finding unused spectrum and adapting the transmission scheme to the requirements of the technologies currently sharing the spectrum. This dynamic radio resource management is achieved in a distributed fashion, and relies on software defined radio.

• High Altitude stratospheric Platform Station (HAPS) systems.

Features of 5G Technology:

• 5G technology offer high resolution for crazy cell phone user and bi-directional large
bandwidth shaping. The advanced billing interfaces of 5G technology makes it more attractive
and effective.

• 5G technology also providing subscriber supervision tools for fast action.

• The high quality services of 5G technology based on Policy to avoid error.

• 5G technology is providing large broadcasting of data in Gigabit which supporting almost
65,000 connections.

• 5G technology offer transporter class gateway with unparalleled consistency.

• The traffic statistics by 5G technology makes it more accurate.

• Through remote management offered by 5G technology a user can get better and fast solution.

• The remote diagnostics also a great feature of 5G technology.

• The 5G technology is providing up to 25 Mbps connectivity speed.

• The 5G technology also support virtual private network.

• The new 5G technology will take all delivery service out of business prospect

• The uploading and downloading speed of 5G technology touching the peak.

• The 5G technology network offering enhanced and available connectivity just about the world.

EDGE

The new EDGE air interface has been developed specifically to meet the bandwidth needs of 3G. Enhanced Data rates for Global Evolution (EDGE) are a ratio based mobile high speed data standard. It allows data transmission speeds of 384 kbps to be achieved when all eight time slots are used. In fact, EDGE was formerly called GSM384. This means a maximum bit rate of 48 kbps per time slot. Even higher speed may be available in good ratio conditions. EDGE is considered an intermediate step in the evolution to 3G WCDMA (Wideband CDMA), although some carriers are expected to stop short of that final step.

15.8.1 Applications in networking

SMS

Short Message Service (SMS) is the transmission of short text messages to and from a mobile phone, fax machine and/or IP address. Messages must be no longer than some fixed number of alpha-numeric characters and contain no images or graphics. Once a message is sent, it is received by a Short Message Service Center (SMSC), which must then get it to the appropriate mobile device.

To do this, the SMSC sends a SMS request to the home location register (HLR) to find the roaming customer. Once the HLR receives the request, it will respond to the SMC with the subscriber's status: (1) inactive or active (2) where subscriber is roaming.

Chat

Chatting : Realtime communication between two users via computer. In telephone conservations, you say something, people hear it and respond, and one can hear their responses on the spot and can reply instantly. In the same manner, in chatting, you type a message on your screen, which is immediately received by the recipient; then the recipient can type a message in response to your message, which is received by you instantly.

Video Conferencing

A video conference is a live, visual connectio between two or more perople residing in seprate locations for the purpose of communication. People who have a multimedia PC with camera and video compression hardware, access to internet over an ordinary telephone line, and videophone software can see each other while talking, which is what is called Video conferencing.

15.8.2 Wi-Fi

Wi-Fi refers to **Wireless Fidelity,** which lets you connect to the internet without a direct line from your PC to the ISP. For Wi-Fi to work, you need:

- A broadband internet connection.
- A wireless router, which relays your Internet connection from the “wall” to the PC.
- A laptop or desktop with a wireless internet card or external wireless adapter.

Transmitting computer data without wires makes your data especially susceptible to hackers, computer users who can intercept your connection and steal your data. If you decide to use Wi-Fi at home, be sure that the network you set up is security enabled.

Wi-Fi Hotspots

A hotspot is a venue that offers Wi-Fi access. The public can use a laptop, Wi-Fi phone or other suitable portable devices to access the internet through a WiFi Hotspot. Hotspots are public locations (such as libraries, hotels, airports, etc) with free or fee-based wireless internet access. There are Wi-Fi hotspots in thousands of locations around the world.

WiMax

WiMax is a wireless digital communications system. WiMax can provide Broadband Wireless Access (BWA) up to 30 miles (50 km) for fixed stations and 3-10 miles (5-15 km) for mobile stations. WiMax requires a tower called WiMax Base Station, similar to a cell phone tower, which is connected to the Internet using a standard wired high-speed connection. But as opposed to a traditional Internet Service Provider (ISP), which divides that bandwidth among customers via wire, it uses a microwave link to establish a connection. In other words, WiMax does not depend on cables to connect each end-point, the internet connectivity to an end-user is provided through microwave link between the tower and the user-endpoint, known as WiMax Subscriber unit.

15.9.1 Network Security

The networking offers endless possibilities and opportunities to every user of it, alone with convince. But this convinces and endless benefits are not free from risks as there are many a risks to network security.

While ensuring network security, the concerns are to make sure that only legal or authorized user and programs gain access to information resources like databases. Also, certain control mechanisms are setup to ensure that properly authenticated users get access only to those resources that they are entitled to

use. Under this type of security, mechanisms like authorization, authentication, encrypted smart cards, biometrics and firewalls, etc are implemented.

The problems encountered under network security can be summarized as follows:

1. Physical security holes. When individuals gain unauthorized physical access to a computer and temper with files. Hackers do it by guessing passwords of various users and then gaining access to the network systems.
2. Software security holes. When badly written programs or 'privileged' software are compromised into doing things that they should not be doing.
3. Inconsistent usage holes. When a system administrator assembles a combination of hardware and software such that the system is seriously flawed from a security point of view.

PROTECTION METHODS

1. Authorization: It determines whether the service provider has granted access to the web service to the requestor. Basically, authorization confirms the service requestors credentials. It determines if the service requestor is entitled to perform the operation, which can range from invoking the web service to executing a certain part of its functionality. Authorization is performed by asking the user a legal login ID. If the user is able to provide a legal login ID, he/she is considered an authorized user.

2. Authentication: It ensures that each entity involved in using a web service– the requestor, the provider and the broker (if there is one) – is what it actually claims to be. Authentication involves accepting credentials from the entity and validating them against an authority.

Authentication also termed as password protection as the authorized user is asked to provide a valid password and if he or she is able to do this, he or she considered to be an authentic user.

3. Encrypted Smart Cards: Passwords in a remote login session generally pass over the network in unencrypted form; any hacker can simply record it and can use it later maliciously to corrupt data/files or to harm anyone etc. To counter such threats newer approaches are suggested such as encrypted smart cards.

An encrypted smart card is a hand held smart card that can generate a token that a computer system can recognize. Every time a new and different token is generated, which even though cracked or hacked, cannot be used later.

4. Bio Metric Systems: They form the most secure level of authorization. The Biometric systems involve some unique aspects of a person's body such as finger prints, retinal patterns, etc to establish his/her identity.

5. Firewall: A system designed to prevent unauthorized access to or from a private network is called firewall. They can be implemented in both hardware and software or a combination of both. Firewalls are frequently used to prevent

unauthorized internet users from accessing private networks connected to the internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques.

(i) **Packet Filter:** Looks as each packet entering or leaving the network and accepts or rejects it based on user defined rules. It is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

(ii) **Application gateway:** It apples security mechanisms to specific applications, such as FTP and Telnet Servers. This is very effective, but can impose performance degradation.

(iii) **Circuit Level Gateway:** It applies security mechanisms when a connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

(iv) **Proxy Server:** It intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

15.10.1 Cookies

Cookies are messages that a web server transmits to a web browser so that a web server can keep track of the user's activity on a specific web site.

Hackers and Crackers

The **Crackers** malicious programmers who break into secure systems where as **Hackers** are more interested in gaining knowledge about computer systems and possibly using this knowledge for play full pranks.

Cyber Law

Cyber Law is a generic term, which refers to all the legal and regulatory aspects of internet and the WWW.

India's IT Act

In India the cyber laws are contained in the information technology act, 2000 which was notified on 17 October 2000. It is based on the United Nations Commission for International Trade Related Laws (UNCITRAL) model law.

The IT act aims to provide the legal infrastructure for ecommerce in India by governing the transactions through the internet and other electronic medium.

15.11.1 Viruses

Computer Virus is a malicious program that requires a host and is designed to make a system sick, just like a real virus. Viruses can spread from computer to computer and they can replicate themselves. Some viruses are categorized as harmless pranks, while others are far more malicious. Broadly three types of viruses are:

1. **File Infectors –** These types of viruses either infect executable files or attach themselves to a program file and create duplicate files.
2. **Boot Sector Viruses –** Install themselves on the beginning tracks of a hard drive or the Master Boot Record or simply they change the pointer to an active boot sector.
3. **Macro Viruses –** Infect data files like electronic spreadsheets or databases of several software packages.
4. **Network Viruses –** These virus use protocols and commands of computer network to spread themselves on the network. Generally they use email or any data transfer files to spread themselves on the network.

Most viruses are spread by email attachment and warn them to be suspicious of any files attached to unsolicited messages.

The following are characteristics of a computer virus.

1. It is able to replicate
2. It requires a host program as a carrier
3. It is activated by external action
4. Its replication ability is limited to the system.

Virus Prevention

Virus Prevention is not a difficult task. All you need to be is extra careful and ensure to follow the following guidelines to lead virus free computing life.

1.Never use a "Foreign" disk or CD without scanning it for viruses.
2.Always scan files downloaded from the internet or other sources.
3.Never boot your PC from a floppy unless you are certain that it is virus free.
4.Write protect your disks.
5.Use licensed software.
6.Password protect your PC to prevent unattended modification.
7.Install and use antivirus software.
8.Keep antivirus software up to date.

Some of the antivirus are Kaspersky , Quick heal, K7, Norton 360, Micro trend titanium, AVG, Panda, ESET Nod32, Avast.McAFee etc.,

Cloud tecnology: Cloud technology or cloud computing as it is more commonly known today is a computing platform widely used by Information Technology (IT) Service Companies.

Review questions

One mark questions:

1. What is networking.
2. What is server?
3. What is client ?
4. What is topology?
5. Expand 2G.
6. What is a virus?
7. What is chatting?
8. What is cyber law?
9. What are cookies?
10. What are Hackers?

Two marks questions:

1. List the Goals for networking.
2. What do you mean by transmission modes?
3. Which are the switching technology used ?
4. What is SIM card ?
5. What is network security?

Three marks questions:

1. Explain the HTTP ?
2. Classify and explain servers.
3. Explain the types of networking.
4. Explain the cables and different types of cables used in transmission?
5. List the differences between simplex, half duplex and full duplex.
6. Explain the applications of networking?

Five marks questions:

1. Explain the working of OSI and TCP/IP?
2. Explain various networking devices used?
3. What is topology explain in detail.
4. What is gateway? Explain.
5. Explain the network security in detail?
6. Give the measures for preventing virus?