10

Computer Networks – I

In This Chapter

10.1 INTRODUCTION

In the history of mankind, networking in any form has always given better results, better outcomes and better utilization of resources. For instance, you always have benefitted from *human networks e.g.*, you want to buy a certain book, which is not available at the bookshop near you. But your friend, who lives in a different part of the city, says he can buy it for you as this book is available in the bookshop near his house. You happily agree to this and the next day in school, he hands over the book to you and you pay to him the book-price. Both are happy–he is happy to help ; you are happy to get the book and to have a helping friend. :). See, networking is so useful ; in fact, networking is useful in all forms – computer networking is no exception. Connections among humans make human network and connections among computers make **computer networks.**

In this chapter, we shall talk about the basics of computer networks, their structures, types, devices, protocols etc.

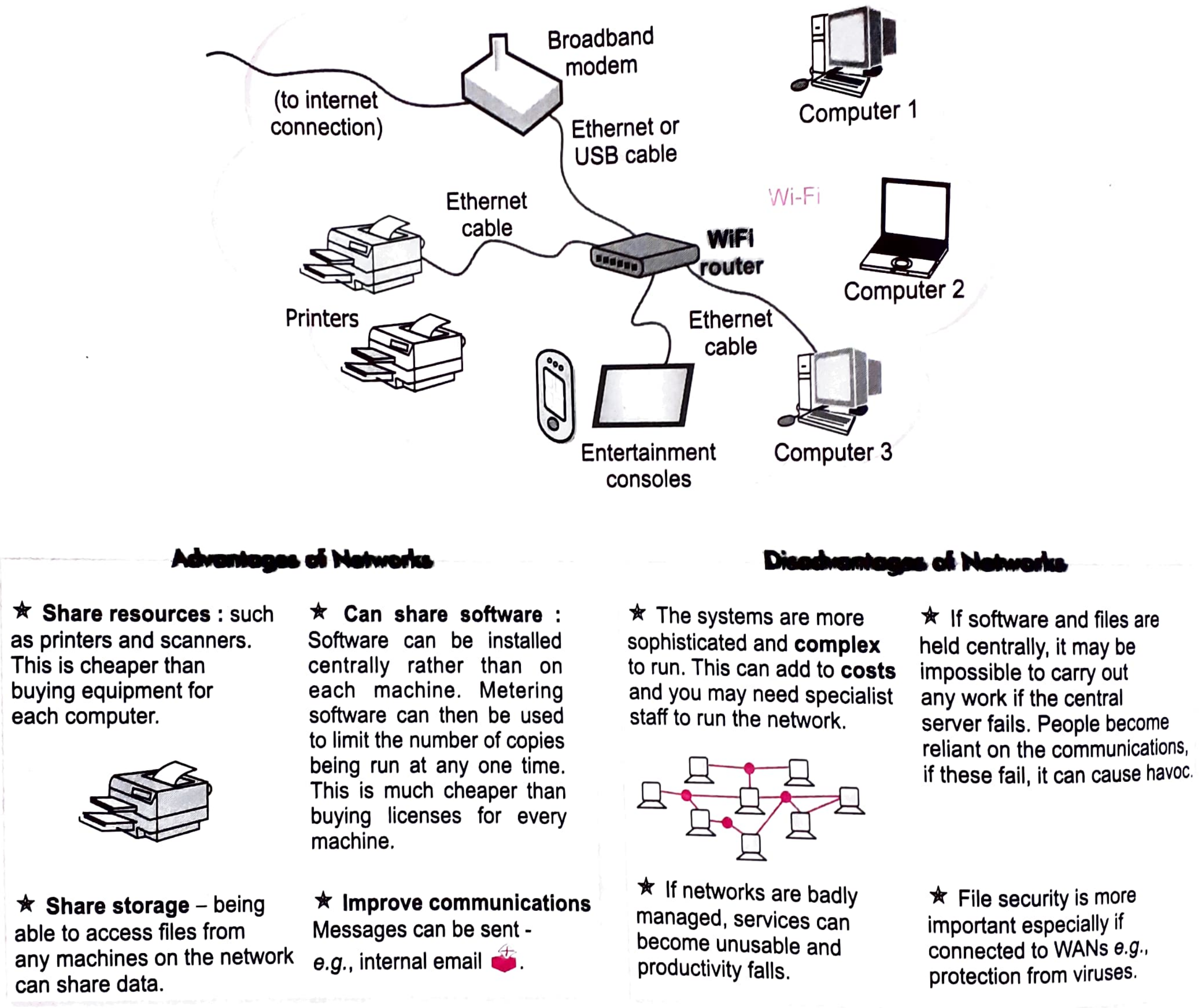
10.2 COMPUTER NETWORKS – AN INTRODUCTION

COMPUTER NETWORK

A **computer network** is a collection of interconnected autonomous computing devices so as to exchange information or share resources.

Two or more autonomous[1] **computing devices** connected to one another in order to exchange information or share resources, form a **computer network**. For example, if in your home, you can connect your *smartphone*, your *laptop* with your *smart TV*, *gaming console* and a *printer* simultaneously either using cables or through WiFi, it will be termed as a **Computer Network**.

Figure 10.1 shows a sample computer network.



Advantages of Networks

★ **Share resources :** such as printers and scanners. This is cheaper than buying equipment for each computer.

★ **Can share software :** Software can be installed centrally rather than on each machine. Metering software can then be used to limit the number of copies being run at any one time. This is much cheaper than buying licenses for every machine.

★ **Share storage** – being able to access files from any machines on the network can share data.

★ **Improve communications** Messages can be sent - *e.g.*, internal email.

Disadvantages of Networks

★ The systems are more sophisticated and **complex** to run. This can add to **costs** and you may need specialist staff to run the network.

★ If software and files are held centrally, it may be impossible to carry out any work if the central server fails. People become reliant on the communications, if these fail, it can cause havoc.

★ If networks are badly managed, services can become unusable and productivity falls.

★ File security is more important especially if connected to WANs *e.g.*, protection from viruses.

Figure 10.1 (*a*) A sample computer network. (*b*) Advantages and disadvantages of computer networks.

Computer networks are very useful in many ways. They facilitate **resource sharing** (resources such as storage, software etc. on the network can be shared), **enhanced communication** (communicating with devices on a network is easier), **cost reduction** (resource sharing cuts on costs) and so forth. Figure 10.1(*b*) shows some advantages and disadvantages of computer networks.

NOTE

Please note that now onwards, we shall use the terms 'computer network' and 'network' interchangeably.

[1] It means that no computing device on a network can start, stop or control other device(s).

10.2.1 Components of a Computer Network

Merely by joining two computers with a cable won't form a network. In fact, there are many components that together make a network. We are briefly discussing below, the major components of a computer network.

Major components of a Computer Networks are :

(*a*) **Hosts/Nodes** (such as PC, laptops, smartphones etc.)

(*b*) **Servers**

(*c*) **Client**

(*d*) **Network hardware** (such as *NIC*, *router*, *switch*, *hub* etc.)

(*e*) **Communication channel** (such as cables, radio-links etc.)

(*f*) **Software** (such as protocols, network operating system etc.)

(*g*) **Network services** (such as BNS, File-sharing etc.).

Let us talk about these, briefly.

(*a*) **Host or Nodes.** The term **host** or **node** refers to the computers that are attached to a network and are seeking to share the resources of the network. Of course, if there were no nodes (also called *workstations*), there would be no network at all.

So your PCs, laptops, smartphones etc. when connect to a network become hosts.

NOTE

A computer becomes a workstation of a network as soon as it is attached to a network.

(*b*) **Server.** A **Server** is a very important computer in a network. A **server** is responsible for making the networking tasks happen. In other words, a server facilitates networking tasks like *sharing of data*, *resource-sharing*, *communication among hosts* etc.

SERVER

Server A computer that facilitates the sharing of data, software, and hardware resources (*e.g.*, printers, modems etc.) on the network, is termed as a Server.

On small networks, sometimes, all the shareable stuff (like files, data, software etc.) is stored on the server. A network can have more than one server also. Each server has a unique name on the network and all users of network identify the server by its unique name.

On big networks, there can be servers dedicated to specialized tasks *e.g.*, a **file server** only handles files' related requests ; a **printer server** only handles printing requests and so on.

(*c*) **Clients.** Client is a related term. A client computer is a host computer that requests for some services from a server. In other words, a *server computer* serves the requests of client *computers*.

(*d*) **Network Hardware.** Other than hosts and wiring, a network requires specialized hardware to carry out various roles, such as establishing corrections, controlling network traffic etc. There are many different types of hardware that are required in a network. Some examples of network hardware are :

- **NIC (Network Interface Unit).** It is a network card attached to a host so as to establish network connections.
- ***Hub, switch, router.*** These are connectivity devices.
- many others.

(*e*) **Communication channel.** Hosts in a network interact with other hosts and server(s) through a ***communication channel*** or ***communication medium***. The communication channels can either be **wired** or **wireless** :

- **Wired Communication channels.** When hosts and server(s) are connected with one another through **guided media** like *network cables*, it is called a **wired communication channel/medium**. Examples of wired communication media are : **twisted-pair cables, coaxial cables, firbre-optic cables.**
- **Wireless Communication channels.** When hosts and server(s) are connected with one another through **unguided media** like ***radio waves***, satellite etc., it is called a wireless communication channel/medium. Examples of wireless communication media are : ***Microwaves, radio waves, satellites, infrared waves, laser*** etc.

(*f*) **Software.** The software layers of a network make networking possible. These comprise of network protocols, network operating system etc.

A **protocol** refers to a pre-decided set of rules using which all parties of a network connect and interact with one another.

A **network operating system** is a specialized operating system that can handle networking tasks.

(*g*) **Network Services.** These refer to the applications that provide different functionalities over a network, such as DNS (Domain Name System), File sharing, VoIP (Voice over IP) and many more.

Armed with this basic knowledge of computer networks, let us further our discussion by talking about types of networks.

10.3 TYPES OF NETWORKS

A computer network means a group of 'networked' computers *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.

Let us discuss types of networks based on these parameters.

10.3.1 Types of Networks based on Geographical Spread

Based on network span or geographical spread, networks can be divided into *two* basic types :

(*i*) LAN (Local Area Network)

(*ii*) WAN (Wide Area Network)

10.3.1A Local Area Network (LAN)

Small computer networks that are confined to a localised 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, printers, hard-disks, modems etc. Fig. 10.1(*a*) shows a Local Area Network.

In a typical LAN configuration, one computer is designated as the **file server**[2]. 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 server are called workstations. On most LANs, cables are used to connect the ***network interface cards***[3] in each computer.

Figure 10.1(*a*) that you have seen earlier shows a LAN.

NOTE

Traditionally, LANs are said to have geographical spread of upto 1 km.

10.3.1B Wide Area Network (WAN)

The networks spread across countries or on a very big geographical area are known as WANs. A *Wide Area Network* (WAN) 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 costs and higher speeds.

Computers connected to a wide-area network are often connected through public networks, such as the telephone system. Sometimes they can be connected through *leased lines*[4] or satellites. The largest WAN in existence is the *Internet*.

Figure 10.2 shows you a LAN and a WAN.

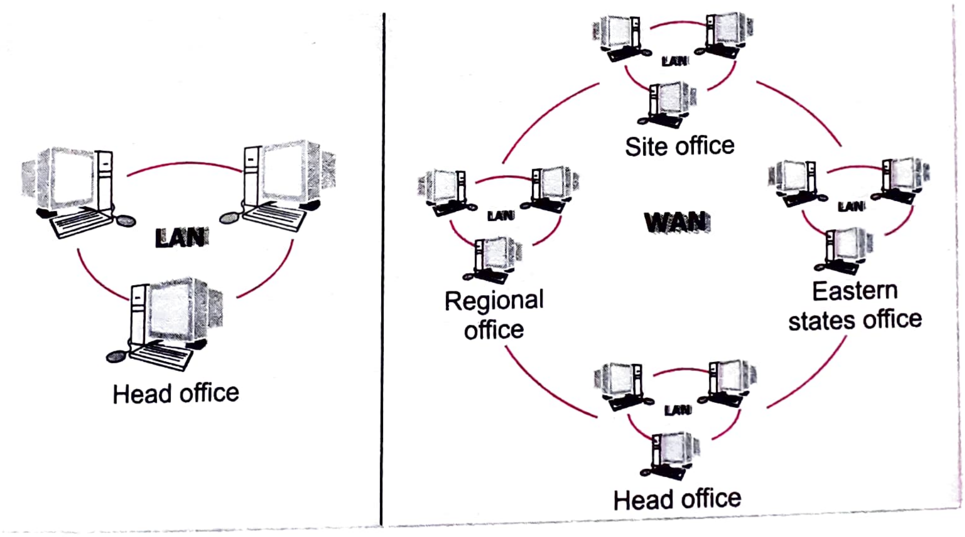


Figure 10.2 LAN *vs.* WAN.

There has been traditionally another type of networks – **MAN (Metropolitan Area Network)**, which refers to a network that is spread over an area as big as a city. But these days, this term has become redundant.

NOTE

The Internet is a giant WAN. The web is also a WAN. Please note that Web (World Wide Web) is a part of the Internet, not the complete Internet.

[2] A *server* is a computer that just serves the requests of doing some tasks, made by other computers in its network. A *file server* serves the requests related to file sharing, storing etc. A *print server* serves the printer related requests, and so on.

[3] The *network interface card* (NIC) provides the physical connection between the network and the computer workstation.

[4] A leased line is a permanent telephone connection between two points set up by a government-regulated organization that provides telecommunications services to the public.

Following table (10.1) lists some basic differences between LAN and WAN.

Table 10.1 LAN *vs.* WAN

S.No.	LAN	WAN
1.	It is spread over a small area.	It is spread over a very large area.
2.	It usually costs less to set it up.	It costs higher to set it up.
3.	It is usually a single network.	It is usually a network of many networks.

10.3.2 Types of Networks by Component Roles

Another parameter based on which you can classify networks is the **role played by network computers in the network operation**. On the basis of this, there can be two types of computer networks :

(*i*) Peer to Peer networks

(*ii*) Client/Server Networks.

Let us talk about these network types one by one.

10.3.2A Peer-to-Peer (P2P) Networks

Peer refers to someone with equal standing, *e.g.*, look at these example sentences :

The staff is trained by peers.

Peer group of children is really important.

The peer-to-peer network literally implements the meaning of the word 'peer', *i.e.*, each computer on a peer-to-peer network is equal. That is, each computer can play the role of a **client** or a **server**. In other words, there is no computer designated as in charge of network operation. Each computer controls its own information and plays role of either a client or a server depending upon what is needed at that point of time.

The computers that serve on a peer-to-peer computer are often termed as **non-dedicated servers**.

On small networks, a workstation that can double up 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 work-stations on a proportionately smaller scale. Since one computer works as a workstation as well as a server, it is slower and requires more memory. Recall that the (small) networks using such a server are known as ***PEER-TO-PEER*** networks.

NOTE

Peer-to-peer networks are popular as home networks and for use in small companies as they are inexpensive and easy to install, but they are limited in scope and are difficult to secure.

Typically a peer-to-peer network has upto ten computers (an accepted limit).

10.3.2B The Client-Server Networks

Unlike peer-to-peer networks, bigger networks prefer to have centralized control. They do this by clearly designating servers and clients. Such networks are called **client-server networks** or even **master-slave networks**.

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

On a network, there may be several servers that allow workstations to share specific resources. For example, there may be a server exclusively for serving files-related requests 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.

The key point about a client-server model is that the **client** is dependent on the **server** to provide and manage the information. For example, websites are stored on **web servers**. A **web browser** is the client which makes a request to the server, and the server sends the website to the browser.

NOTE

A **dedicated server** operates solely as a server on a network while a **non-dedicated server** can shuttle between the client as well as server roles.

CLIENT COMPUTER

A **Client computer** (or a **client**) is a computer or other device on the network that requests and utilizes network resources. A **Server** is a computer on network, dedicated to processing client requests.

Table 10.2 Differences between Client-server and P2P Networks

	Client-server	P2P
Security	The server controls security of the network.	No central control over security.
Management	The server manages the network. Needs a dedicated team of people to manage the server.	No central control over the network. Anyone can set up.
Dependency	Clients are dependent on the server.	Clients are not dependent on a central server.
Performance	The server can be upgraded to be made more powerful to cope with high demand.	If machines on the network are slow they will slow down other machines.
Backups	Data is all backed up on the main server.	Each computer has to be backed up. Data can easily be deleted by users.

10.3.3 Type of Networks based on Communication Channel

Computer networks are formed when computers are connected with one another. The connections among the hosts are established using specific communication media. Based on this parameter, the computer networks can be categorized as these :

(*i*) Wired Computer Networks (*ii*) Wireless Computer Networks.

Let us quickly talk about these computer network types.

10.3.3A Wired Computer Networks

As clear by the name, in *wired computer networks*, the hosts and other devices are interconnected through wiring or cables. Most wired computer networks are of LAN type. Although, there are wireless LANs too and there are bigger networks that use wireless media too.

Most commonly used cables in wired networks are one of the following *three* types :

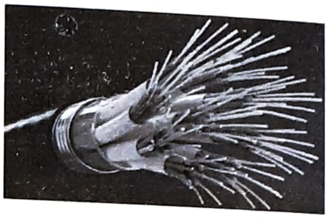
(*i*) **Twisted Pair Cable.** A twisted pair cable is a pair of insulated wires that are twisted together to improve electromagnetic capability and to reduce noise from outside sources. These are available in various forms such as CAT1, CAT2, CAT3, CAT4, CAT5, CAT6.

(*ii*) **Coaxial Cable (Coax).** This type of cable consists of a solid wire core surrounded by one or more foil or wire shields, each separated by some kind of plastic insulator. The *two* most commonly used types of coaxial cables are **thicknet** and **thinnet**.

(*iii*) **Fiber Optic Cable (or Optic Fiber Cable).** A fiber optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves. Common types of *Fiber Optic Cables* are **single node** and **multi-node**.

Twisted Pair Cable

Coaxial Cable (Coax)



Fiber Optic Cable

10.3.2B Wireless Computer Networks

The computer networks that use environment or air as the media, through which information is transmitted without requiring any cable or wires or other electronic conductors, rather by using electromagnetic waves like IR (Infrared), RF (radio frequencies), satellite, etc. are wireless computer networks.

For example, if you connect all smartphones of your house and your laptop through the common Wi Fi, it is a wireless computer network (a wireless LAN). WANs can also be formed using wireless media such as satellites.

Most commonly used transmission media in wireless networks are:

(*i*) **Microwave.** Microwave waves are high frequency waves that can be used to transmit data wirelessly over long distances. The microwave transmission consists of a *transmitter, receiver* and the *atmosphere*. Microwave radiation can be used to transmit signals such as mobile phone calls.

(*ii*) **Radio waves.** Radio waves are used to transmit television and radio programmes. All radios today, use **continuous sine waves** to transmit information (audio, video, data). WiFi that has become a common word today also used radio wave to transmit data among connected devices.

RADIO WAVE

Radio wave can be classified by frequency and wavelength. When the frequency is higher than 3 GHz, it is named microwave.

(*iii*) **Satellite (Satellite Microwave).** Satellite communication is a special case of microwave relay system. Satellite communication use the synchronous satellite to relay the radio signal transmitted from ground station.

A number of communication satellites, owned by both governments 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 another earth station. Using such a setup, data can be transmitted to the other side of the earth in only one step.

Some other wireless communication media are *infrared* and *laser waves*.

Info Box 10.1

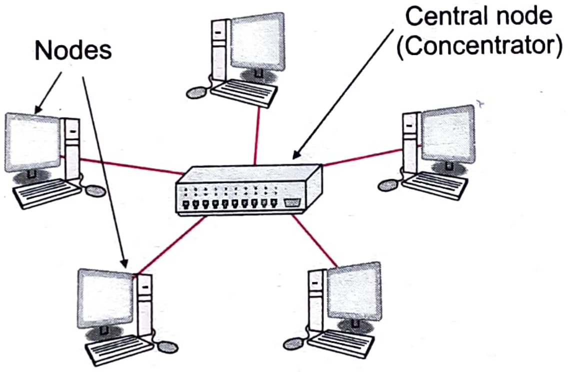
Network Topologies

The pattern of interconnection of nodes in a network is called the *Topology* or *the Network Topology*. Many topologies have been developed, but major ones are :

- the ***Star*** topology ;
- the ***Bus*** topology ;
- the ***Ring*** or ***circular*** topology ;
- the ***Mesh*** topology ;
- the ***Tree*** topology ;

1. The Star Topology

This topology consists of a central node (concentrator) to which all other nodes are connected by a single path. (*see* Fig.). It is the topology used in most existing information networks involving data processing or voice communications. A variation of star topology is *the Tree topology*.



Star Topology

Advantages of a Star Topology

- It is easy to install and wire.
- No disruptions to the network take place while connecting or removing devices.
- It is easy to detect faults and to remove parts.

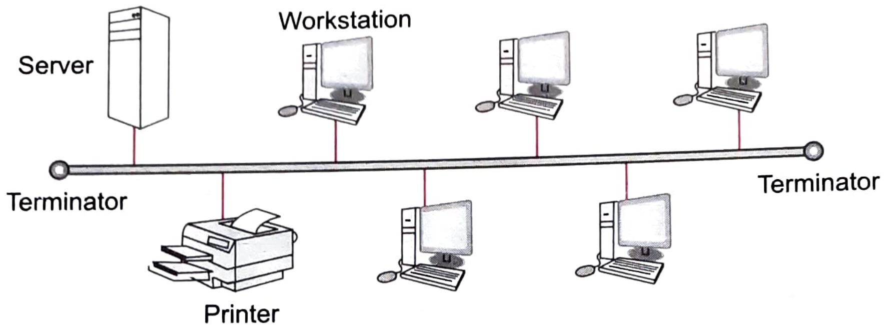
Disadvantages of a Star Topology

- It requires more cable length than a linear topology.
- If the hub, switch, or concentrator fails, nodes attached are disabled.
- It is more expensive than linear bus topologies because of the cost of the hubs, etc.

2. The Bus or Linear Topology

This topology consists of a single length of the transmission medium (normally coaxial cable) onto which the various nodes are attached (*see* Fig.). The transmission from any station travels the length of the bus, in both directions, and can be received by all other stations. At each end, there are terminators which remove the travelling data token from the network.

(Contd...)



Bus Topology

Advantages of a Linear Bus Topology

- It is easy to connect a computer or peripheral to a linear bus.
- It requires less cable length than a star topology.

Disadvantages of a Linear Bus Topology

- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- It is more difficult to identify the problem if the entire network shuts down.
- It is not meant to be used as a stand-alone topology in a large building.

3. The Ring or Circular Topology

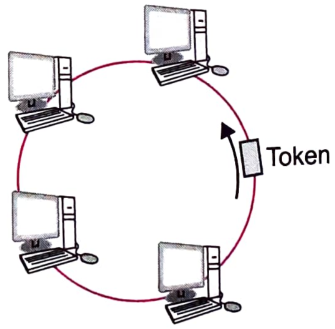
In this topology, each node is connected to two and only two neighbouring nodes. Data is accepted from one of the neighbouring nodes and is transmitted onwards to another (*see* Fig.). Thus ***data token*** travels in one direction only, from node to node around the ring. After passing through each node, it returns to the sending node, which removes it.

Advantages of Ring Topology

- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- It is comparatively cheaper to install and expand.

Disadvantages of Ring Topology

- Troubleshooting is difficult in ring topology.
- Adding or deleting the computers disturbs the network activity.
- Failure of one computer disturbs the whole network.

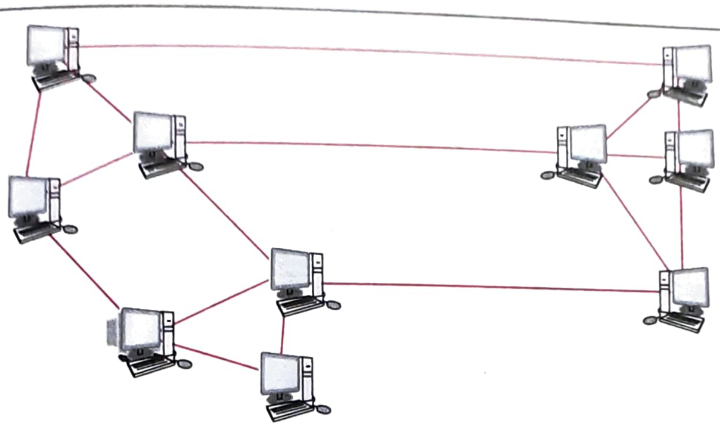


Ring Topology

4. Mesh Topology

In this topology, each node is connected to more than one node to provide an alternative route in the case the host is either down or too busy. The mesh topology is **excellent for long distance networking** because it provides extensive back-up, rerouting and pass-through capabilities. Communication is possible between any two nodes on the network either directly or by passing through. This is **also ideal for distributed networks.**

(Contd...)



Mesh Topology

Advantages of Mesh Topology

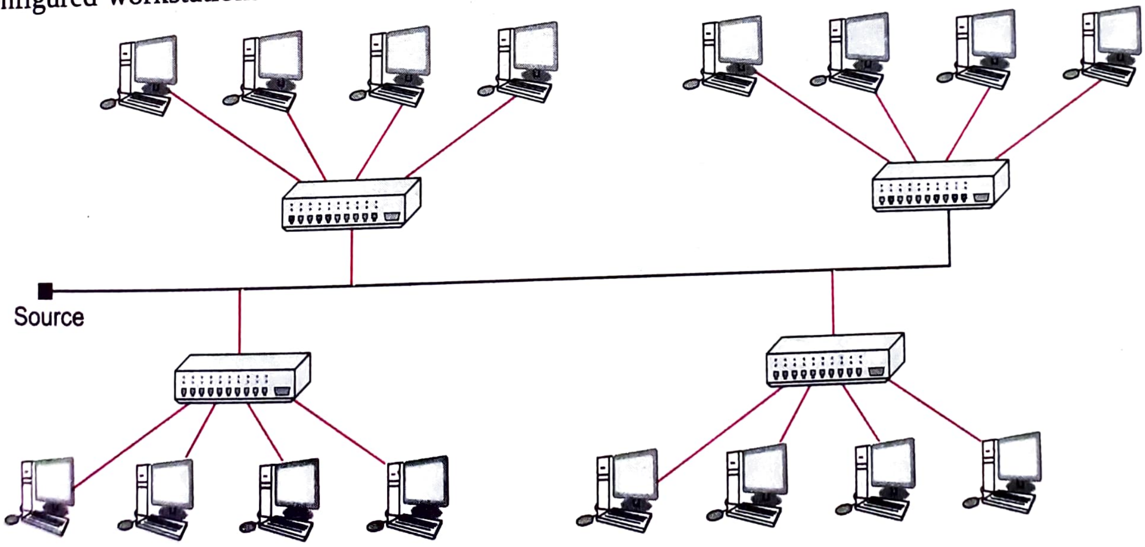
- Each connection can carry its own data load.
- It is robust and provides security and privacy.
- In this topology, fault diagnosis is easy.

Disadvantages of Mesh Topology

- Its installation and configuration is difficult.
- Cabling cost is more for mesh topology.
- Bulk wiring is required for mesh topology.

5. Tree or Expanded Star Topology

A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable (*see* Fig.).



Mesh Topology

Advantages of a Tree Topology

- It uses point-to-point wiring for individual segments.
- It is supported by several hardware and software venders.

Disadvantages of a Tree Topology

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- It is more difficult to configure and wire than other topologies.

10.4 NETWORK DEVICES/HARDWARE

In the smooth functioning of a computer network, other than computers and wiring, many devices or specialized hardware play important roles. In this section, we are discussing about these network devices/hardware.

10.4.1 NIC (Network Interface Card)

A standalone computer (a computer that is not attached to a network) lives in its own world and carries out its tasks with its own inbuilt resources. But as soon as it becomes a workstation, it needs an interface to help establish a connection with the network because without this, the workstations will not be able to share network resources.

The *network-interface-card* is a device that is attached to each of the workstations and the server, and helps the workstation establish the all-important connection with the network. Each *network-interface-card* that is attached to a workstation has a unique number identifying it, which is known as the *node address*. The NIC is also called *Terminal Access Point* (TAP). Different manufacturers have different names for the interface. The NIC is also called NIU – *Network Interface Unit.*

MAC ADDRESS

The MAC address refers to the physical address assigned by NIC manufacturer.

The NIC manufacturer assigns a unique physical address to each NIC card ; this physical address is known as **MAC address**. (Media Access Control Address)

MAC Address

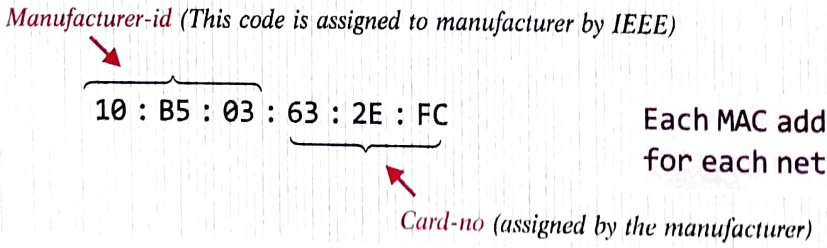
The NIC manufacturer assigns a unique physical address to each NIC card ; this physical address is known as *Media Access Control* address (**MAC address**). A MAC address is a 6-byte address with each byte separated by a colon *e.g.*, a sample MAC address could be :

```
10 : B5 : 03 : 63 : 2E : FC
```

So, now you know that this MAC address is actually the number assigned to the network card of your computer. The first *three* bytes of MAC address are the *manufacturer-id* (assigned to the manufacturer by an international organization namely IEEE) and the last three bytes are the *card-no* (assigned by manufacturer) (*see* Fig. 10.3 below).

NOTE

The NIC manufacturer assigns a unique physical address to each NIC card ; this physical address is known as *Media Access Control* address (**MAC address**)


Manufacturer-id (This code is assigned to manufacturer by IEEE)
10 : B5 : 03 : 63 : 2E : FC
Card-no (assigned by the manufacturer)

Each MAC address is unique for each network card.

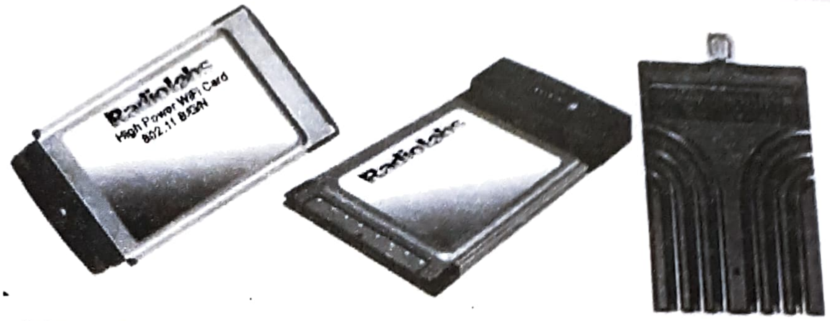
Figure 10.3 Sample MAC address.

10.4.2 WiFi Card

A WiFi card is either an internal or external *Local Area Network adapter* with a built-in wireless radio and antenna. The most common WiFi cards used in desktop computers are PCI-Express WiFi cards made to fit the PCI-Express card slots on the motherboard.

Benefits

The primary benefit of using a WiFi card in a desktop computer is that it allows you to setup your workstation or home office without considering the proximity or availability of hard line network access.



PCMCIA WiFi Card Express Card WiFi Card USB WiFi Card

Figure 10.4 Various types of WiFi cards.

10.4.3 Hub

A **hub** is a hardware device used to connect several computers together. A *hub* contains multiple independent but connected modules of network and inter-networked equipment. A similar term is **concentrator**. A *concentrator* is a device that provides a central connection point for cables from workstations, servers, and peripherals.

Basically, hubs are multi-slot concentrators into which a number of multi-port cards can be plugged to provide additional access as the network grows in size. Hubs can be either *passive* or *active*.

- **Active hubs** electrically amplify the signal as it moves from one connected device to another. Active concentrators are used like *repeaters*[5] to extend the length of a network.
- **Passive hubs** allow the signal to pass from one computer to another without any change.

HUB

A **hub** is networking device having multiple ports that are used for connecting multiple computers or segments of a LAN together.

10.4.4 Switch

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

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 can support any packet protocol. LANs that are segmented through switches are called *Switched 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.

A switch would be like a phone system with private lines in place of the hub's *party line*. For instance, *Meira Sen* at the Maurya Hotel calls *Ibrahim Soz* in another room, and the operator or phone switch connects the two of them on a dedicated line. This allows more conversations at any one time thereby allowing more guests to communicate.

[5] A repeater is a device that electrically amplifies the signal it receives and rebroadcasts it.

10.4.5 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 only allow those messages that need to get to the other side to cross the bridge.

Bridges can handle networks that follow same protocols.

10.4.6 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. The router is responsible for forwarding data from one network to a different network.

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. 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.

ROUTER

A Router is a network device that forwards data from one network to another. A router works like a *bridge* but can handle different protocols.

A router differs from a bridge in a way that former uses logical addresses and the latter uses physical addresses.

10.4.7 Gateway

A *gateway* is a device that connects dissimilar networks. 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.

GATEWAY

A **Gateway** is a network device that connects dissimilar networks. It establishes an intelligent connection between a local network and external networks with completely different structures.

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.

10.4.8 Access Point

An **access point (AP)**, also called **wireless access point (WAP)**, is a hardware device that establishes connection(s) of computing devices on wireless LAN with a fixed wire network. The AP is connected to a fixed wire network and it then broadcast wireless signals that computing devices having Wi Fi cards can detect; using these wireless signals, the computing devices get connected to fixed wired network via AP and use network as needed. So, you can say that an access point is a station that transmits and receives data (thus sometimes referred to as a *transceiver*).

ACCESS POINT

An **access point (AP)**, also called wireless access point (WAP), is a hardware device that establishes connection(s) of computing devices on wireless LAN with a fixed wire network.

Please note that every access point has a range (up to *150 feet* for home based APs) and only the devices within this range can connect to the network using AP. The moment a device moves out of this range, its connection with AP (and with the network) breaks. Similarly, every AP also has a limit on number of computing devices it can attach to simultaneously.

Different types of wireless access points are available that are suitable to different types of users with different needs, *e.g.*, an AP at home is different from an AP at a large enterprise or college campus.

Advantages of access points include : *easier installation, easier maintenance, bigger network coverage, stable signals,* and *ease of work.*

NOTE

Wireless routers can function as access points, but not all access points can work as routers.

10.5 THE CLOUD

So by now you know that in bigger networks (WANs) there are multiple servers employed where actual storage and actual work happens as per the requirements of workstations/host. Generally, the servers are placed at safe, secure, isolated place(s) and end users work on their workstations at separate places. The term **cloud** was coined to refer to the collection of servers.

NOTE

The cloud is a generic term used for Internet.

In modern days, the **cloud** refers to the Internet.

Cloud computing is Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand, like the electricity grid. A basic definition of *cloud computing* is the use of the Internet for the tasks you perform on your computer for storage, retrieval and access. The "cloud" represents the Internet. *Cloud computing* is a new name for an old concept : ***the delivery of computing services from a remote location.*** Cloud computing services are delivered through a network, usually the Internet.

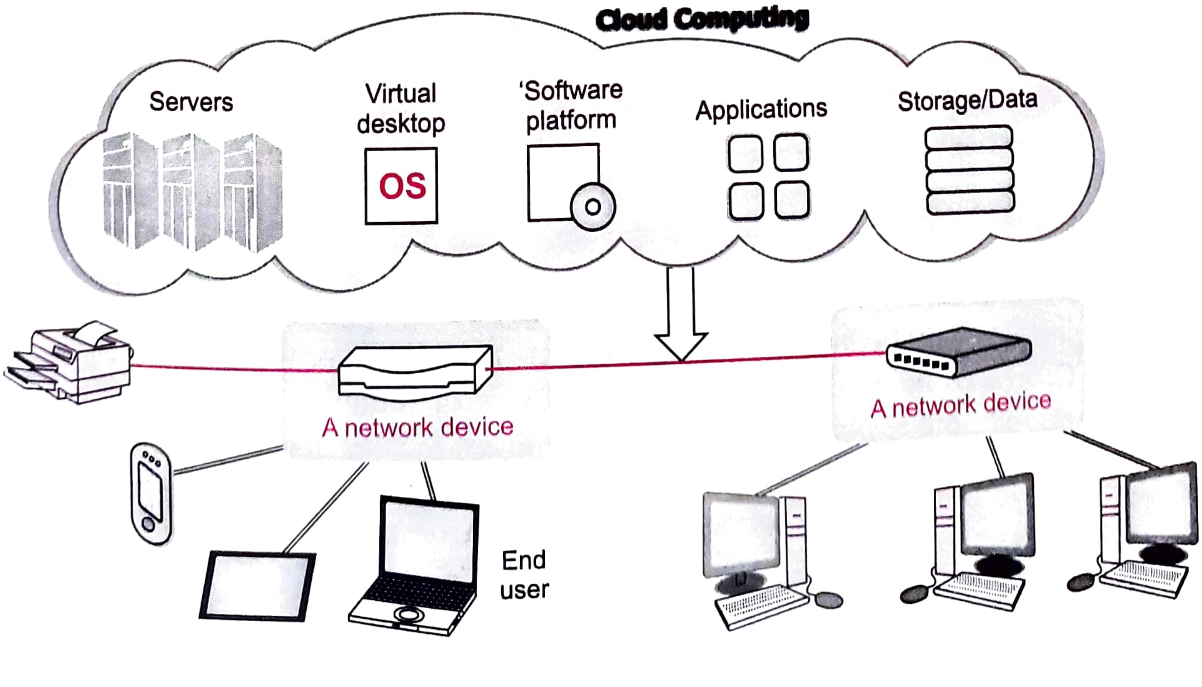


Figure 10.5 Cloud and Cloud computing.

10.5.1 Types of Clouds

There are different types of clouds that you can subscribe to depending on your needs. As a home user or small business owner, you will most likely use public cloud services. Enterprises can choose to deploy applications on *Public, Private* or *Hybrid* clouds.

Four deployment models of clouds are :

1. Private Clouds

These are the clouds for exclusive use by a single organization and typically controlled, managed and hosted in private data centers. The hosting and operation of private clouds may also be outsourced to a third party service provider, but a private cloud remains for the exclusive use of one organization.

2. Public Clouds

These are the clouds for use by multiple organizations (tenants) on a shared basis and hosted and managed by a third party service provider.

3. Community Clouds

These are the clouds for use by a group of related organizations who wish to make use of a common cloud computing environment. For example, a community might consist of the different branches of the military, all the universities in a given region, or all the suppliers to a large manufacturer.

4. Hybrid Clouds

When a single organization adopts both private and public clouds for a single application in order to take advantage of the benefits of both. For example, in a cloudbursting scenario, an organization might run the steady-state workload of an application on a private cloud, but when a spike in workload occurs, such as at the end of the financial quarter or during the holiday season, they can burst out to use computing capacity from a public cloud, then return those resources to the public pool when they are no longer needed.

10.6 INTERNET OF THINGS (IoT)

You have been hearing stories like : *now smart refrigerators are available in market that would automatically add items to your online shopping list by sensing which item(s) is less in quantity in the refrigerator. Modern day manufacturing machines can connect with one another and the managers and update about their status. Smart vehicles can connect with one another and interact.*

All these examples are using a revolutionary technology called **Internet of Things (IoT)**.

IoT is a technology that connects the ***things*** to the **Internet** over wired or wireless connections. Here the ***Things*** could refer to every smart device of today's age, *i.e.*, from computers and smartphones to home appliances, wearables, vehicles, factory machines, to tagged animals and consumables etc.. You can say that the **Internet of Things** allows people and things to be connected **Anytime, Anyplace, with Anything and Anyone**, ideally using **Any path/network** and **Any service**.

In this section, the word "Thing" will always refer to the smart devices that connect to form IoT.

IoT

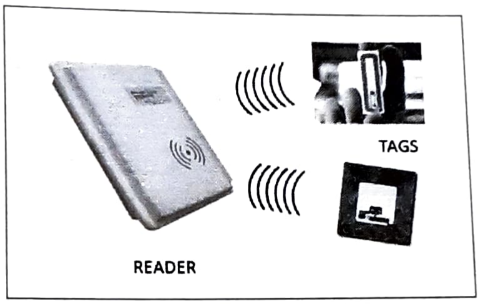
IoT is a phenomenon that connects the **things** (the smart devices) to the **Internet** over wired or wireless connections.

10.6.1 Enabling Technologies for IoT

IoT is a phenomenon that can connect a variety of devices to Internet. To make it possible, different technological concepts are implemented together.

These enabling technologies are :

(*i*) **RFID (Radio Frequencies Identification).** This technology is designed to use radio waves to read and capture information stored on a tag, called an **RFID tag**, attached to an object. Every device (the *thing*) on IoT has an RFID tag.



An RFID tag is a small microchip attached to an antenna. It identifies and tracks the data of the "**things**". This technology is composed of one or more readers and RFID tags that communicate with one another.

(*ii*) **Sensors.** A sensor is a device that is able to detect changes in an environment. A sensor is able to measure a physical phenomenon (like temperature, pressure, and so on) and transform it into an electric signal. The sensors enable us to collect data about the status of the "Thing".

Modern age IoTs contain different types of sensors for variety of applications. Most common types of sensors used in IoT are : *temperature sensors, proximity sensor, pressure sensor, optical sensors, humidity sensors, motion detection sensors, smoke sensors, gas sensors*, and many other types.

(*iii*) **Smart Technologies.** Smart technologies include additional functionality to take action and have other processing capabilities as per the requirements. For example, smart controllers can connect with the smart devices and act upon them also as per the need of the hour, *e.g.*, turning off or on a device, stopping a vehicle, locking/unlocking a door, adjusting the temperature of an oven and many more such actions. Smart technologies of IoT are able to interact with smart nano devices as well.

(*iv*) **Software.** The software part is equally important in the success of any technologies. The software provides the reusable solutions for connecting, taking actions and solving issues that may arise.

(*v*) **Efficient Network connectivity.** IoT is formed through interconnections of devices to the Internet. Hence the connectivity is very important. Modern age efficient network technologies play an important role in IoT.

10.6.2 Devices that can form IoT

Any device that has an RFID tag can be a part of an IoT. RFID technology has been used with a variety of devices such as the ones listed below and many more.

- **Home appliances.** fridges, cookers, coffee makers, heaters, HVAC, TVs, DVD players, lights, doors, windows etc.
- **Wearables.** Clothes, shoes, hats, watches, heart monitors etc.
- **Vehicles.** Cars, buses, bicycles, trains etc.
- **Factories.** Machines, robots, warehouse shelves, parts within machines, tools etc.
- **Agriculture.** Biochip transponders on farm animals and plants, farm humidity and temperature sensors etc.
- **Food.** Sensors for monitoring the condition of food.

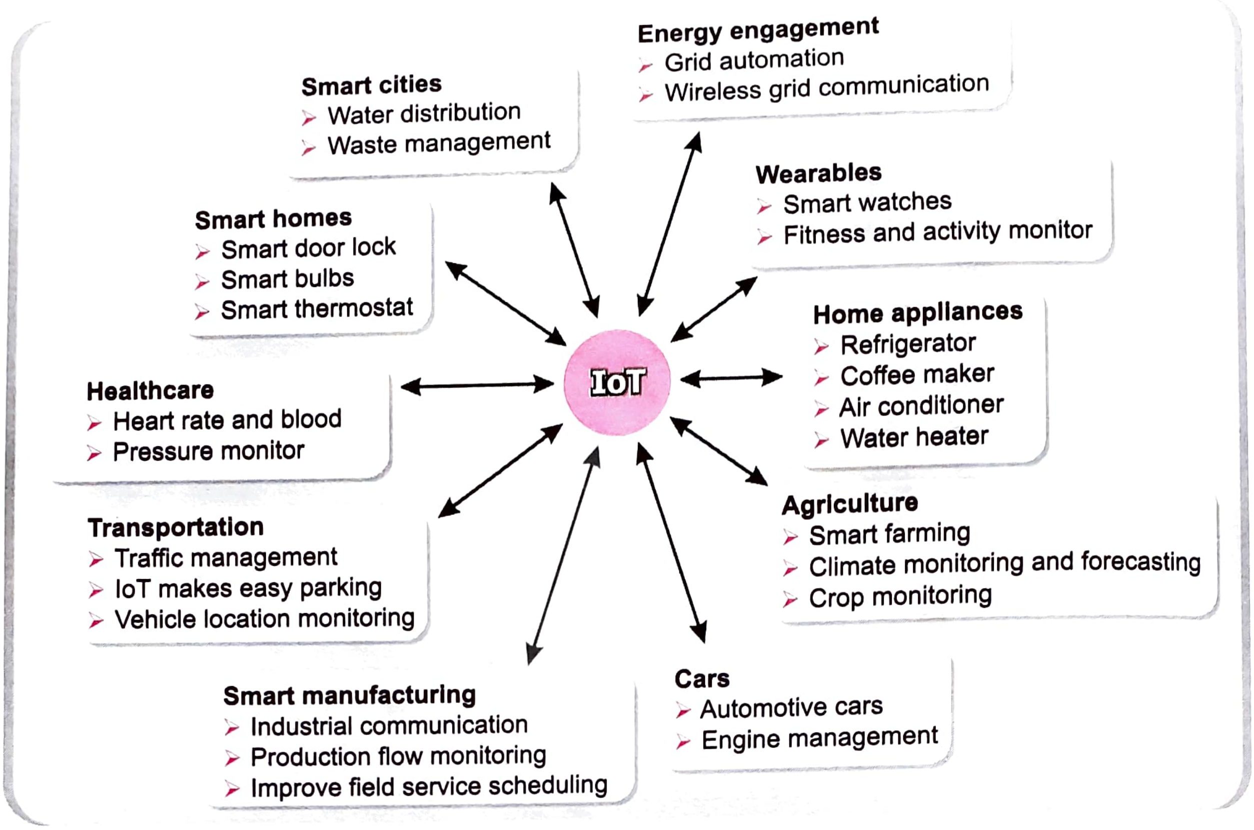


Figure 10.6 IoT devices.

10.6.3 Challenges and Risks

IoT has made many things easier and possible but there are many challenges and risks associated with it. Most important and critical challenge and risk is the security of IoT. How secure the data is and how immune an IoT is, is a critical question. Like other networks, cyber-attacks, hackers, and unauthorized intruders can attack IoTs as well. With billions of "Things" connected to the Internet, it could also mean that by unauthorized access one can create disasters – something that is unimaginable.

With this, we have come to the end of this chapter. Let us quickly revise what we have learnt in this chapter.

Let Us Revise

- *A network is a collection of interlinked computers by means of a communication system.*
- *The networks facilitate resource sharing, increased reliability, reduced costs, and increased and fast communication.*
- *On the basis of geographical spread, networks can be classified into LAN (Local Area Network), and WAN (Wide Area Network).*
- *Small computer networks that are confined to a localised area e.g., an office, a building etc., are called LANs.*
- *A WAN 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 a big LAN.*
- *On the basis of component roles, networks can be classified into : a peer-to-peer network and a client-server network.*
- *A Client computer (or a client) is a computer or other device on the network that requests and utilizes network resources.*
- *A Server is a computer on network, dedicated to processing client requests.*
- *In a peer-to-peer network, all computers are equal; each can double up as a client as well as a non-dedicated server.*

- *A client/server network has computer(s) designated as server(s) and these are dedicated servers. Clients do own job and the servers serve the requests of the clients.*
- *A hub is a hardware device used to connect several computers together. Hubs can be either active hubs or passive hubs.*
- *A switch is a device that is used to segment networks into different subnetworks called subnets or LAN segments.*
- *A bridge is a device that links two networks together.*
- *A router is a device that works like a bridge but can handle different protocols.*
- *A gateway is a device that connects dissimilar networks.*
- *An access point (AP), also called wireless access point (WAP), is a hardware device that establishes connection(s) of computing devices on wireless LAN with a fixed wire network.*
- *The cloud is a generic term for the Internet.*
- *IoT is a phenomenon that connects the smart devices to the Internet over wired or wireless connections.*
- *IoT technology uses other technologies like RFID, sensors, smart technologies like controllers and specialized software.*

Objective Type Questions

OTQs

Multiple Choice Questions

1. Two devices are in network if
   (*a*) a process in one device is able to exchange information with a process in another device
   (*b*) a process is running on both devices
   (*c*) the processes running of different devices are of same type
   (*d*) none of the mentioned

2. What is a stand alone computer ?
   (*a*) A computer that is not connected to a network
   (*b*) A computer that is being used as a server
   (*c*) A computer that does not have any peripherals attached to it
   (*d*) A computer that is used by only one person

3. Central Computer which is powerful than other computers in the network is called as ______ .
   (*a*) Client (*b*) Server (*c*) Hub (*d*) Switch

4. Network in which every computer is capable of playing the role of a client, or a server or both at same time is called
   (*a*) peer-to-peer network (*b*) local area network
   (*c*) dedicated server network (*d*) wide area network

5. In peer-to-peer network, each computer in a network is referred as
   (*a*) server (*b*) client (*c*) peer (*d*) sender

6. Which transmission media is capable of having a much higher bandwidth (data capacity) ?
   (*a*) Coaxial (*b*) Twisted pair cable
   (*c*) Untwisted cable (*d*) Fibre optic

7. Which type of transmission media is the least expensive to manufacture?
   (*a*) Coaxial (*b*) Twisted pair cable
   (*c*) CAT cable (*d*) Fibre optic

8. Which of these components is internal to a computer and is required to connect the computer to a network ?

   (*a*) Wireless Access Point (*b*) Network Interface card
   (*c*) Switch (*d*) Hub

9. A device that forwards data packet from one network to another is called a

   (*a*) Bridge (*b*) Router (*c*) Hub (*d*) Gateway

10. Which of the following is the fastest media of data transfer ?

    (*a*) Co-axial Cable (*b*) Untwisted Wire
    (*c*) Telephone Lines (*d*) Fibre Optic

11. Hub is a

    (*a*) Broadcast device (*b*) Unicast device
    (*c*) Multicast device (*d*) None of the above

12. Switch is a

    (*a*) Broadcast device (*b*) Unicast device
    (*c*) Multicast device (*d*) None of the above

13. The device that can operate in place of a hub is a :

    (*a*) Switch (*b*) Bridge (*c*) Router (*d*) Gateway

14. A repeater takes a weak and corrupted signal and ______ it.

    (*a*) Amplifies (*b*) Regenerates
    (*c*) Resembles (*d*) Reroutes

15. Which of the following is not a type of cloud ?

    (*a*) Private (*b*) Public (*c*) Protected (*d*) Hybrid

16. Which of the following is correct statement for IoT ?

    (*a*) It is a collection of networks
    (*b*) It is a collection of protocols
    (*c*) It is network of physical objects or "things" embedded with chips, sensors etc.
    (*d*) None of these

Fill in the Blanks

1. A computer network that spans a relatively large geographical area is called ______ .
2. WAN stands for ______ .
3. Wired networks use an access method called ______ .
4. Wireless networks use an access method called ______ .
5. ______ is a protocol which allows users to download E Mail messages from mail server to a local computer.
6. ______ is a protocol that allows to send/upload email message from local computer to an email server.
7. A network of networks is known as ______ .
8. In a network, a machine is identified by unique address called ______ .

9. The physical address assigned by NIC manufacturer is called ______ address.
10. A MAC address consumes ______ bytes or ______ bits.
11. ______ is an example of Public cloud. [CBSE Sample Paper 2019-20]
12. ______ is a network of physical objects embedded with electronics, software, sensors and network connectivity. [CBSE Sample Paper 2019-20]

True/False Questions

1. A LAN is connected to large geographical area.
2. A client is the computer that asks for the action in a network.
3. A computer is identified by 64 bit IP address.
4. Every object on the Internet has a unique URL.
5. A stand alone computer may also be referred to as host.
6. Big networks can be of peer-to-peer types.
7. MAC address is a 48 bit address.
8. A switch can work is place of a hub.
9. A gateway is like a modem.
10. The cloud is a generic term used for Internet.

NOTE : Answers for OTQs are given at the end of the book.

Solved Problems

1. *What is a network ? Why is it needed ?*

   Solution. A network is an interconnected collection of autonomous computers that can share and exchange information.

   Major reasons that emphasize on the need of networks are :

   (i) *Resource Sharing*. Through a network, data, software and hardware resources can be shared irrespective of the physical location of the resources and the user.

   (ii) *Reliability*. A file can have its copies on two or more computers of the network, so if one of them is unavailable, the other copies could be used. That makes a network more reliable.

   (iii) *Reduced Costs*. Since resources can be shared, it greatly reduces the costs.

   (iv) *Fast communication*. With networks, it is possible to exchange information at very fast speeds.

2. *What is a Hub ?*

   Solution. A *hub* is a hardware device used to connect several computers together.

3. *Explain in brief the capabilities and services supported by LAN.*

   Solution. Small computer networks that are confined to a localised 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. One node has a printer connected to it and other nodes on the LAN can communicate with it in order to print files and hence allowing expensive peripherals to be shared among number of users.

4. *What are routers ?*

Solution. A device that works like a bridge but can handle different protocols, is known as a **router**. For example, a router can link Ethernet (ethernet is a very popular and widely accepted method of linking local stations to one another (*i.e.*, a LAN) for sharing data, program and equipment resources.) 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.

5. *What are major types of networks and explain ?*

Solution.

- Server-based network
- Peer-to-peer network

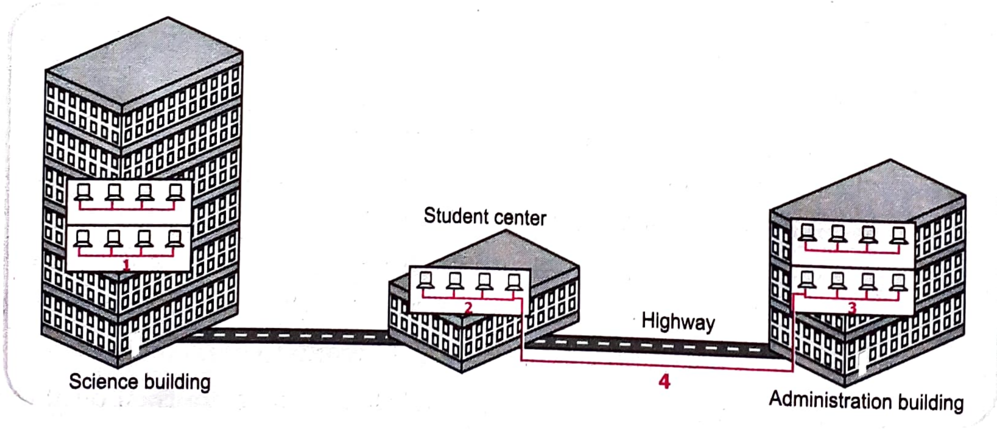
Server-based networks provide centralized control of network resources and rely on server computers to provide security and network administration.

Peer-to-peer network, computers can act as both servers sharing resources and as clients using the resources.

6. *What is the purpose of using router ?*

Solution. A router can work like a bridge and can also handle different protocols. A router can locate the destination required by sending the traffic to another router, if the destination is unknown to itself.

7. *Govt. of Delhi has computer networks inside each of its buildings. It has now interconnected the networks of Administration building and of Student center building. The networks so formed are marked below as numbers. Mention which types of networks is each of these ?*



Solution.

Network number	Type of network
1, 2, 3	LAN
4	WAN (it is connecting only networks 2 and 3)

8. *What is NIC ?*

Solution. NIC stands for Network Interface Card. It is also known as Network Adapter. It is in the form of add-in card and is installed in a computer so that the computer can be connected to a network. Each NIC has a MAC address which helps in identifying the computer on a network.

9. *What is the difference between Hub, Switch, and Router?*

Solution.

Hub	Switch	Router
Hub is the least expensive, least intelligent and least complicated of the three. It broadcasts all data to every port which may cause serious security and reliability concern.	Switches work similarly like Hubs but in a more efficient manner. It creates connections dynamically and provides information only to the requesting port.	The router is smartest and most complicated out of these three. It comes in all shapes and sizes. Routers are similar like little computers dedicated for routing network traffic.
In a Network, Hub is a common connection point for devices connected to the network. Hub contains multiple ports and is used to connect segments of LAN.	Switch is a device in a network which forwards packets in a network.	Routers are located at gateway and forwards data packets.

10. *What are the enabling technologies of IoT systems ?*

Solution. IoT system has been enabled through following technologies majorly :

(*i*) RFID (Radio Frequencies Identification)

(*ii*) Sensors

(*iii*) Network connectivity

(*iv*) Smart technologies

11. *What are the security concerns related to IoT ?*

Solution. Data security and privacy are major concerns related to IoT. These devices are vulnerable to hacking and cloud endpoints could be used by hackers to attack servers.

12. *What is the difference between working of switches and routers?*

Solution. The switches are found within LANs where there is a single path from source to the destination.

The routers connect LANs and these can be multiple paths from source to destination when data is travelling via routers.

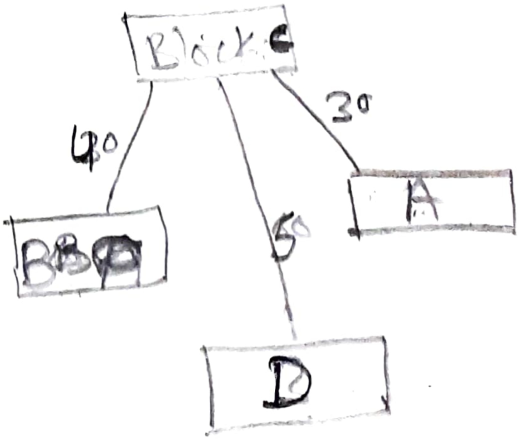
13. *Software Development Company has set up its new center at Raipur for its office and web based activities. It has 4 blocks of buildings named Block A, Block B, Block C, Block D.* [CBSE Sample Paper 2019-20]

Topology

Number of Computers

Block A	25
Block B	50
Block C	125
Block D	10

Layout ✓



Shortest distances between various Blocks in meters :

Block A to Block B	60 m
Block B to Block C	40 m
Block C to Block A	30 m
Block D to Block C	50 m

(*i*) Suggest the most suitable place (*i.e.*, block) to house the server of this company with a suitable reason.

(*ii*) Suggest the type of network to connect all the blocks with suitable reason.

(*iii*) The company is planning to link all the blocks through a secure and high speed wired medium. Suggest a way to connect all the blocks.

(*iv*) Suggest the most suitable wired medium for efficiently connecting each computer installed in every block out of the following network cables :

- Coaxial Cable
- Ethernet Cable
- Single Pair Telephone Cable.

Solution. (*i*) Block C, It has maximum number of computers.

(*ii*) LAN (*iii*) Star topology (*iv*) Ethernet cable

GLOSSARY

Bridge	Device that links two networks together.
Gateway	Device that connects dissimilar networks.
Hub	Hardware device used to connect several computers together.
Internetworking	Connection of two or more networks.
Network	An interconnected collection of autonomous computers.
Router	Device that works like a bridge but can handle different protocols.
Switch	Device used to segment networks into different subnetworks called subnets.
Transceiver	Transmitter/Receiver.

Assignment

1. What is a network ? What are its goals and applications ?
2. Discuss and compare various types of networks.
3. What are hubs ? What are its types ?
4. What is the role of a switch in a network ?
5. Briefly discuss the role of following devices in the context of networking.

   (*i*) router (*ii*) bridge (*iii*) gateway
6. When would you prefer (*i*) bridges over hubs (*ii*) switch over other network devices ?
7. When would you opt for a router in a network ?
8. What are hubs ? How are active hubs different from passive hubs ?
9. What are the facilities provided by the SERVER in a Network environment ?
10. In which network there is no server ?
11. What is a cloud ? What is cloud computing ?
12. What are different cloud deployment models ?
13. How is a public cloud different from a private cloud ?
14. What is Internet of Things ?
15. What are the technologies that have enabled IoT ?
16. What are the concerns related to IoT ?