Data Communication and Computer Network

Avinash Maskey

Introduction

- The term **communications**, when used in a computer context, refers to **telecommunications**; that is, data sent from one device to another using communications media, such as ***telephone lines***, ***privately owned cables***, and the ***airwaves***.
- Communications usually take place over a **private** (such as a home or business) computer network, the Internet, or a telephone network, and are an integral part of our personal and professional lives today.

What is a network? (Contd.)

- In most businesses, computer networks are essential. They enable employees to share expensive resources, access the Internet, and communicate with each other, as well as with business partners and customers.
- They facilitate the exchange and collaboration of documents and they are often a key component of the ordering, inventory, and fulfillment systems used to process customer orders.
- In homes, computer networks enable individuals to share resources, access the Internet, and communicate with others. In addition, they allow individuals to access a wide variety of information, services, and entertainment, as well as share data (such as digital photos, downloaded movies, and music) among the networked devices in a home.
- On the go, networks enable individuals to work from remote locations, locate information whenever and wherever it is needed, and stay in touch with others.

Uses/Importance of Computer Networks

- Sharing an Internet connection among several users.
- Sharing application software, printers, and other resources.
- Facilitating Voice over IP (VoIP), e-mail, video conferencing, messaging, and other communications applications.
- Working collaboratively; for example, sharing a company database or using collaboration tools to create or review documents.
- Exchanging files among network users and over the Internet.
- Connecting the computers and the entertainment devices (such as TVs, gaming consoles, and stereo systems) located within a home.

Network Characteristics

- Networks can be identified by a variety of characteristics, including whether they are designed for wired or wireless access, their topology, their architecture, and their size or coverage area.
- These topics are described in the next few sections.
  - Wired and Wireless
  - Network Topology
  - Network Architecture
  - Network size and coverage area (or ***Types of network***)

Wired Vs Wireless Network

- **Networks** can be designed for access via ***wired and/or wireless*** connections. With a ***wired network*** connection, the computers and other devices on the network are physically connected (***via cabling***) to the network. With a ***wireless network*** connection, wireless (usually radio) signals are used to send data through the air between devices, instead of using physical cables.
- ***Wired networks*** include conventional telephone networks, cable TV networks, and the wired networks commonly found in schools, businesses, and government facilities.
- Where as, ***Wireless networks*** include conventional television and radio networks, cellular telephone networks, satellite TV networks, and the wireless networks commonly found in homes, schools, and businesses. Wireless networks are also found in many public locations (such as coffeehouses, businesses, airports, hotels, and libraries) to provide Internet access to users while they are on the go via public wireless hotspots.

Wired Vs Wireless Network (Contd.)

- Many networks today are accessible via both wired and wireless connections.
- ***For instance***, a business may have a wired main company network to which the computers in employee offices are always connected, as well as provide wireless access to the network for visitors and employees to use while in waiting rooms, conference rooms, and other locations within the office building.
- A home network may have a wired connection between the devices needed to connect the home to the Internet (such as a modem and router), plus wireless access for the devices in the home (such as computers, printers, televisions, and gaming devices) that will access the home network wirelessly.

Wired Vs Wireless Network (Contd.)

- Wired networks tend to be faster and more secure than wireless networks, but wireless networks have the advantage of allowing easy connections in locations where physical wiring is impractical or inconvenient (such as inside an existing home or outdoors), as well as giving users much more freedom regarding where they can use their computers.

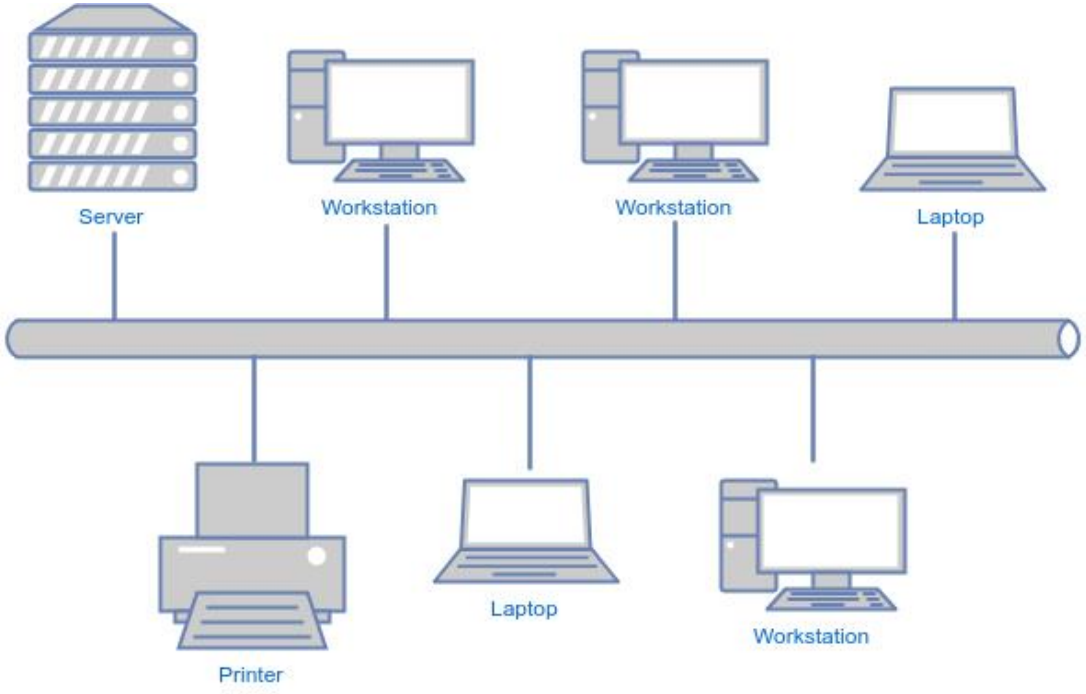
- With wireless networking, for example, you can surf the Web on your notebook computer from anywhere in your house, access the Internet with your media tablet or smartphone while you are on the go, and create a home network without having to run wires among the rooms in your house.

Network Topologies

- ***Network Topology*** refers to layout of a network. How different nodes in a network are connected to each other and how they communicate is determined by the network's topology.
- Topology defines the structure of the network of how all the components are interconnected to each other.
- Network topology refers to the physical or logical layout of a network.
- There are two types of network topologies: ***physical*** and ***logical***.
  - ***Physical topology*** emphasizes the physical layout of the connected devices and nodes, while the ***logical topology*** is a concept in networking that defines the architecture of the communication mechanism for all nodes in a network. Using network equipment such as routers and switches, the logical topology of a network can be dynamically maintained and reconfigured.
- The topologies commonly used are: ***Bus topology, Star topology***, and ***Ring topology***. Other topologies are ***Tree topology***, ***Mesh topology*** and ***Hybrid topology***.

Bus Topology

- **Bus topology** is a network type in which every computer and network device is connected to single cable.When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- It uses a central cable to which all network devices connect. All data is transmitted down the bus line from one device to another so, if the bus line fails, then the network cannot function.



Bus Topology Network

Bus Toplology

Advantages:

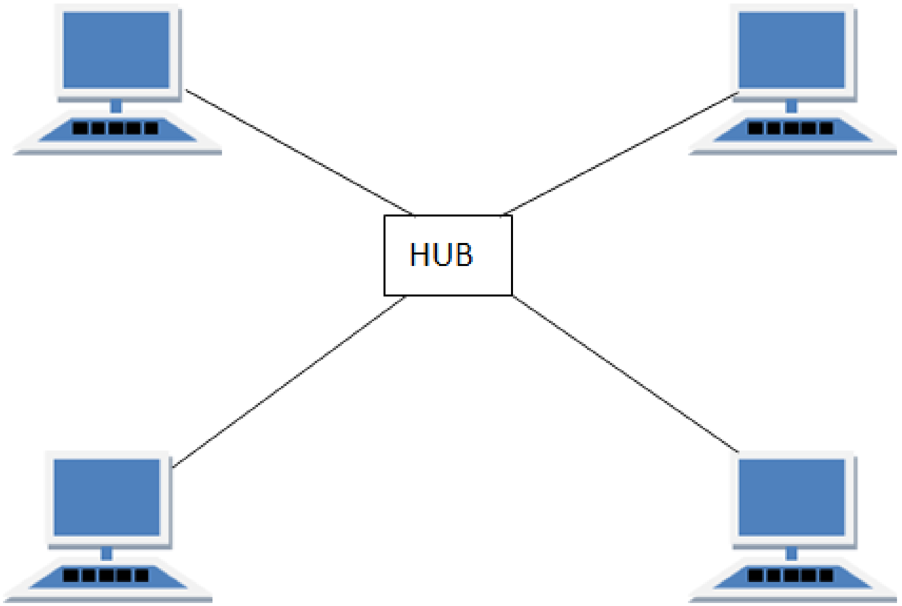
- If any node or cable (except backbone) fails, it does not affect the whole network.
- They are relatively cheap and easy to install.
- Don't require much cabling.
- Easy to add and remove any node or cable except the backbone cable.

Disadvantages:

- If the backbone cable fails, the entire network goes down.
- Since all the data are transmitted through the backbone cable, data traffic is high.
- Bus networks work best with a limited number of devices.

Star Topology

- ***Star topology*** is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a ***server***, and the peripheral devices attached to the server are known as ***clients***.
- It is used in traditional ***mainframe environments*** (central data hub), as well as in small office, home, and wireless networks.
- All the networked devices connect to a central device (such as a server or a switch) through which all network transmissions are sent. If the central device fails, then the network cannot function.



Star Toplology

Advantages:

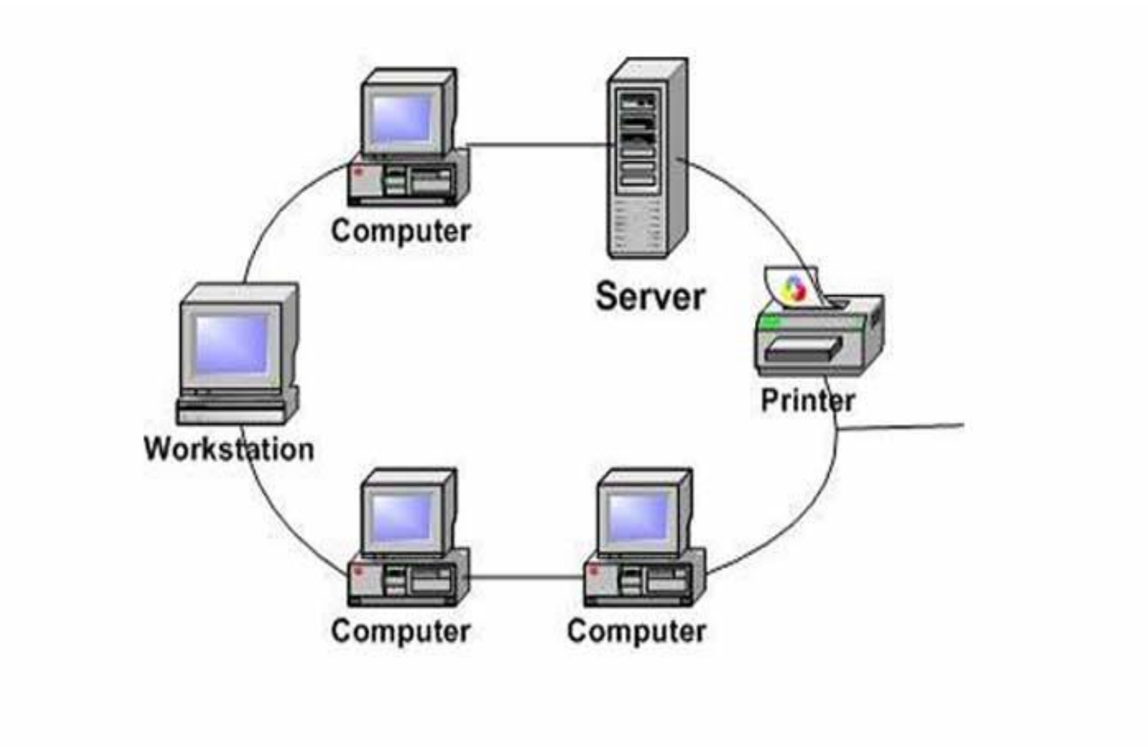
- A failure in any node or cable will only take down one computer's network access and not the entire LAN.
- Easy to diagnose the fault.
- Easy to add and remove a node or cable.

Disadvantages:

- Expensive to use because compared to the bus topology, a star network generally requires more cables.
- If the hub fails then the whole network is stopped because all the nodes depend on the hub.
- No two nodes can transmit the data at the same time.

Ring Topology

- A ***ring topology*** is a network configuration where device connections create a circular data path. Each networked device is connected to two others, like points on a circle. Together, devices in a ring topology are referred to as a ring network.
- In a ***ring network***, packets of data travel from one device to the next until they reach their destination. Most ring topologies allow packets to travel only in one direction, called a ***unidirectional ring network***. Others permit data to move in either direction, called ***bidirectional***.



Ring Toplology

Advantages:

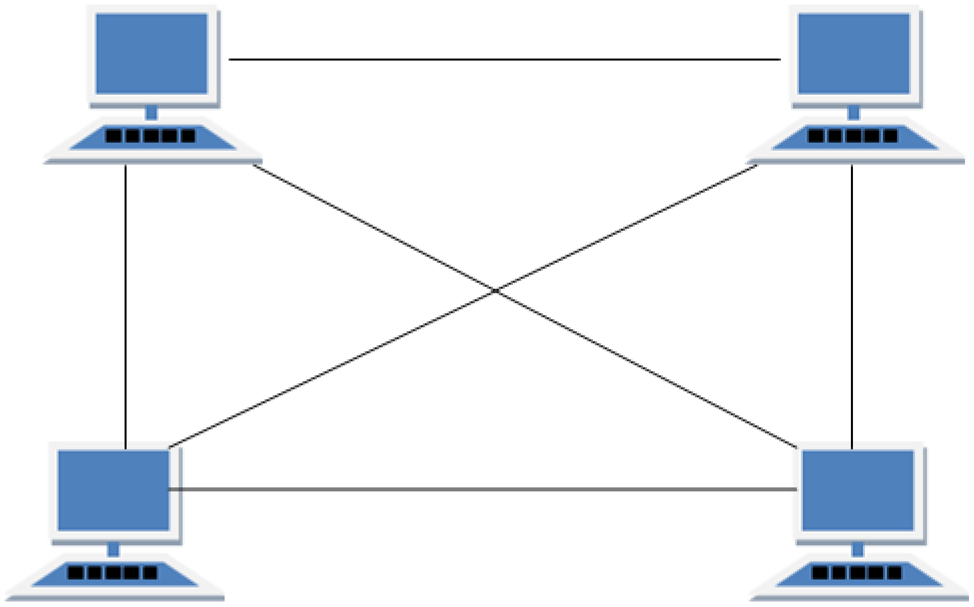
- All data flows in one direction, reducing the chance of packet collisions.
- A network server is not needed to control network connectivity between each workstation.
- Data can transfer between workstations at high speeds.
- Additional workstations can be added without impacting performance of the network.

Disadvantages:

- All data being transferred over the network must pass through each workstation on the network, which can make it slower than a star topology.
- The entire network will be impacted if one workstation shuts down.
- The hardware needed to connect each workstation to the network is more expensive than ethernet cards and hubs/switches.

Mesh Topology

- ***Mesh Topology*** uses a number of different connections between network devices so that data can take any of several possible paths from source to destination.
- With a ***full mesh topology*** each device on the network is connected to every other device on the network. With a ***partial mesh topolog***y, some devices are connected to all other devices, but some are connected only to those devices with which they exchange the most data.
- ***Consequently,*** if one device on a mesh network fails, the network can still function, assuming there is an alternate path available. Mesh networks are used most often with wireless networks.



Mesh Toplology

Advantages:

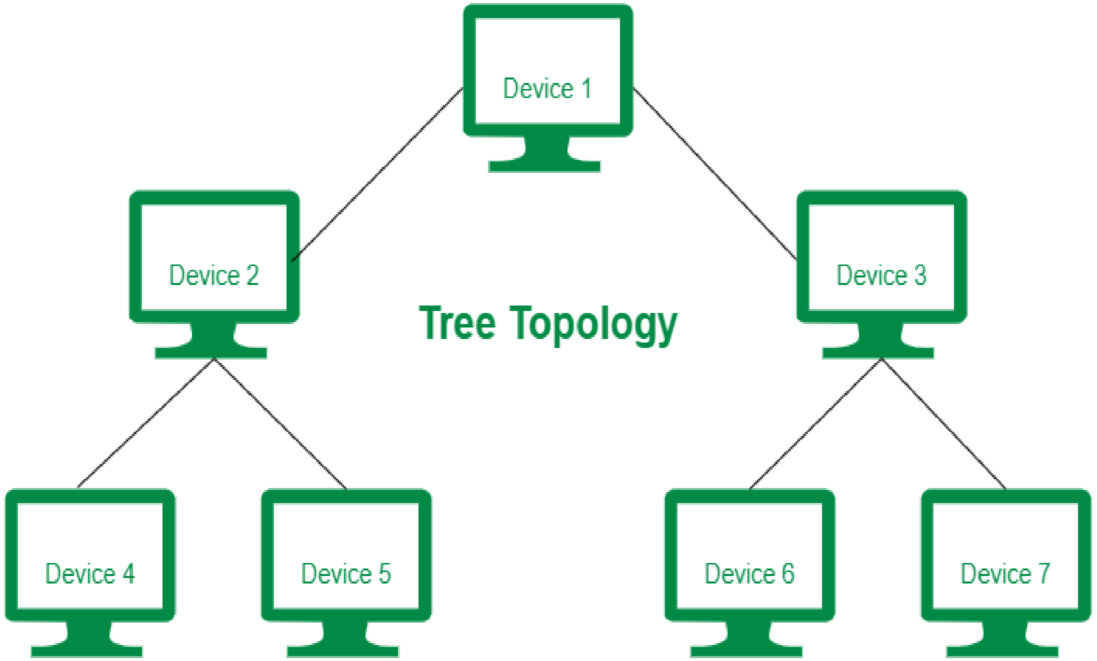
- Manages high amounts of traffic, because multiple devices can transmit data simultaneously.
- A failure of one device does not cause a break in the network or transmission of data.
- Adding additional devices does not disrupt data transmission between other devices.

Disadvantages:

- The cost to implement is higher than other network topologies, making it a less desirable option.
- Building and maintaining the topology is difficult and time consuming.
- The chance of redundant connections is high, which adds to the high costs and potential for reduced efficiency.

Tree Topology

- A ***tree topology*** is a special type of structure where many connected elements are arranged like the branches of a tree.
- For example, tree topologies are frequently used to organize the computers in a ***corporate network***, or the ***information in a database***.
- In a **tree topology**, there can be only one connection between any two connected nodes. Because any two nodes can have only one mutual connection, tree topologies create a natural parent and child hierarchy.
- In computer networks, a tree topology is also known as a ***star bus topology***. It incorporates elements of ***both*** a ***bus topology*** and a ***star topology***.



Tree Toplology

Advantages:

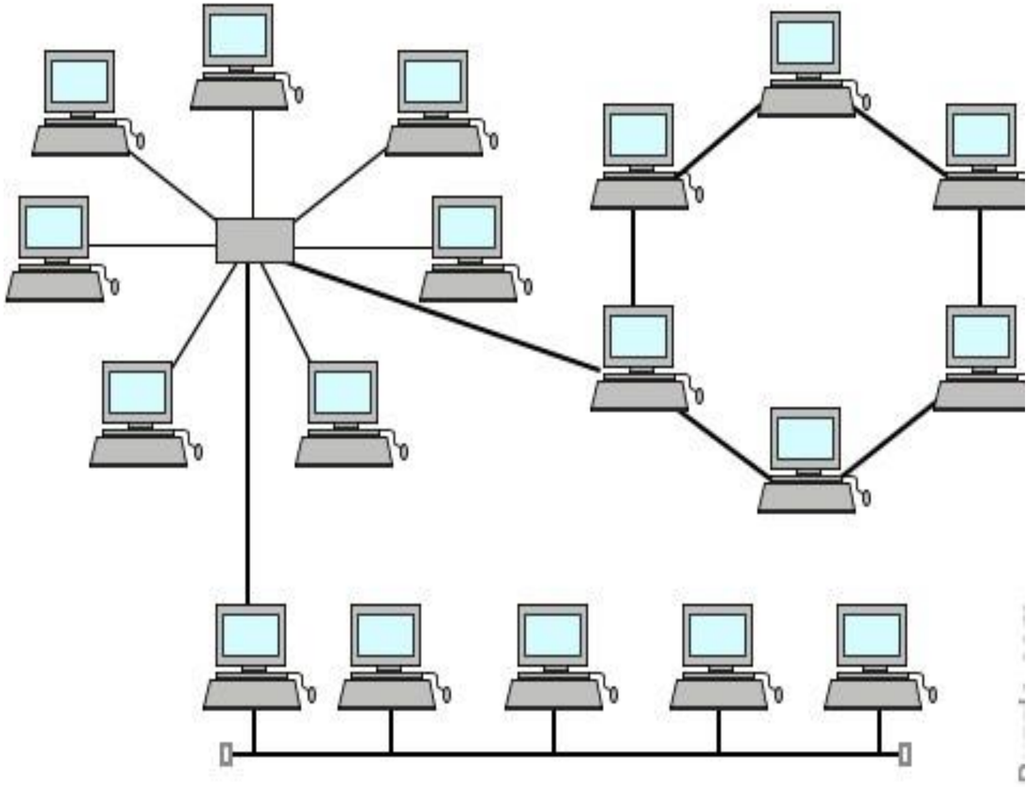
- Expansion of nodes is possible and easy.
- If any devices damaged, other hierarchical networks are not affected.
- Other segments are not affected if any node or any segment gets damage.
- Easy to manage and maintain.

Disadvantages:

- If the main backbone line breaks then the entire network shut down.
- Huge amount of cable is needed.
- Maintenance is difficult if more devices are added.
- If the hub or connector fails, attached nodes are also disabled.

Hybrid Topology

- A ***hybrid topology*** is a type of network topology that uses two or more differing network topologies. These topologies can include a ***mix*** of ***bus topology***, ***mesh topology***, ***ring topology***, ***star topology***, and ***tree topology***.
- The choice to use a ***hybrid topology*** over a standard topology depends on the needs of a business, school, or the users. The number of computers, their location, and desired network performance are all factors in the decision.



Hybrid Toplology

Advantages:

- This type of topology combines the benefits of different types of topologies in one topology.
- Can be modified as per requirement.
- It is extremely flexible.
- It is very reliable.
- It is easily scalable as Hybrid networks are built in a fashion which enables for easy integration of new hardware components.
- Error detecting and trouble shooting is easy.
- Handles large volume of traffic.
- It is used to create large network.

Disadvantages:

- It is a expensive type of network.
- Design of a hybrid network is very complex.
- Usually hybrid architectures are usually larger in scales so they requires a lot of cables in installation process.
- Hubs which are used to connect two distinct networks, are very costly. And hubs are different from usual hubs as they need to be intelligent enough to work with different architectures.
- Installation is a difficult process.

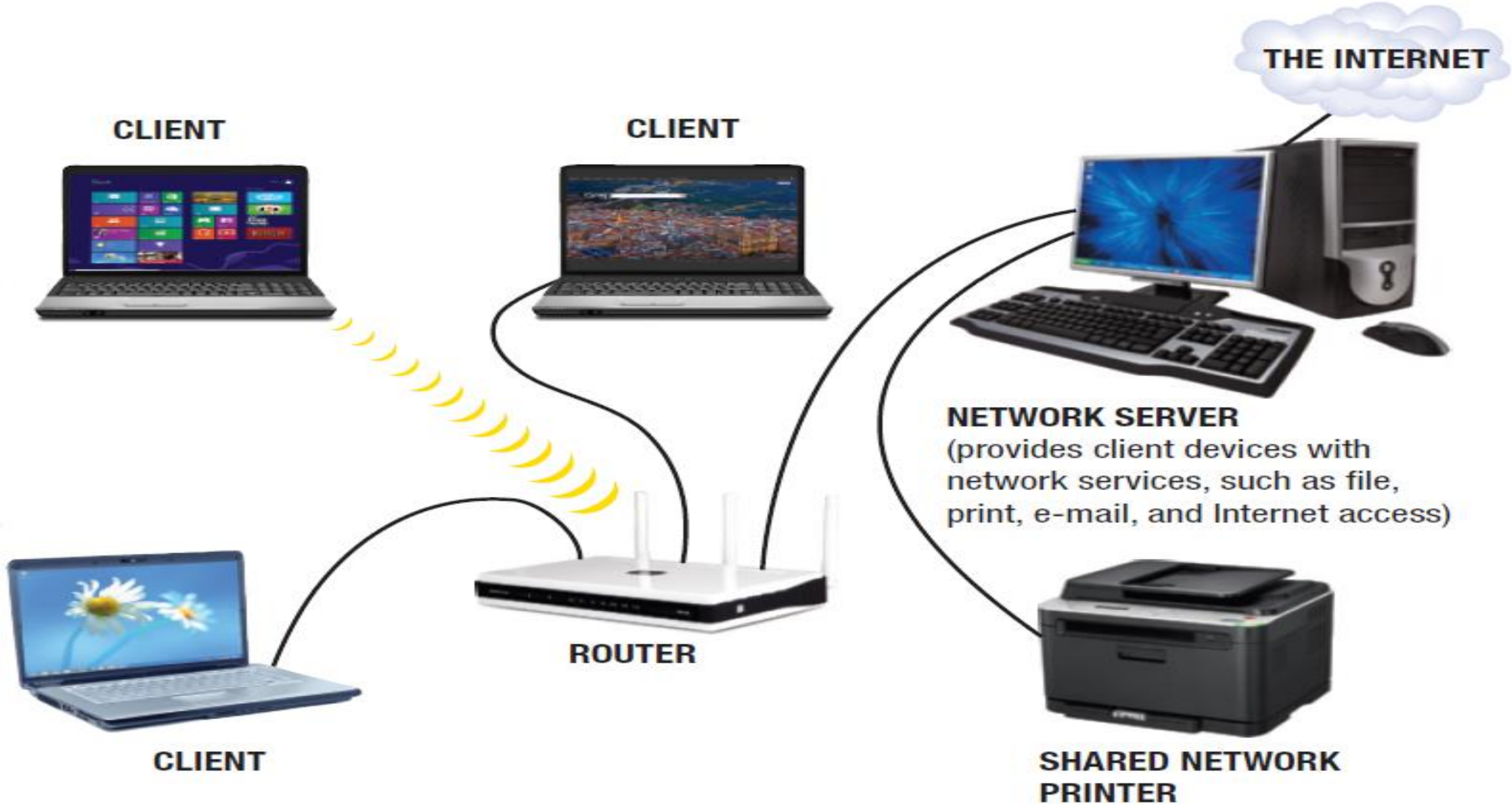
Network Architectures

- ***Network Architecture*** refers to how computers are organized in a system and how tasks are allocated between these computers.
- Networks also vary by their architecture; that is, the way they are designed to communicate.
- The two most common network architectures are ***client-server*** and ***peer-to-peer (P2P)***.

Client/Server Architrcture

- ***Client-server networks*** include both **clients** (computers and other devices on the network that request and utilize network resources) and **servers** (computers that are dedicated to process client requests).
- Network servers are typically powerful computers with lots of memory and a very large hard drive. They provide access to software, files, and other resources that are being shared via the network.
- Servers typically perform a variety of tasks. For example, a ***single server*** can act as a ***network server*** to manage network traffic, a ***file server*** to manage shared files, a ***print server*** to handle printing-related activities, and/or a ***mail server*** or ***web server*** to manage e-mail and web page requests, respectively.
- For instance, there is only one server in the network illustrated in Figure, and it is capable of performing all server tasks for that network. When a client retrieves files from a server, it is called ***downloading***; transferring data from a client to a server is called ***uploading***.

Fig: Client/Server Architrcture


THE INTERNET
CLIENT
CLIENT
NETWORK SERVER
(provides client devices with network services, such as file, print, e-mail, and Internet access)
ROUTER
CLIENT
SHARED NETWORK PRINTER

Peer-to-Peer (P2P) Architecture

- With a ***peer-to-peer (P2P) network***, a central server is not used (see Figure). Instead, all the computers on the network work at the same functional level, and users have direct access to the computers and other devices attached to the network.
- For instance, users can access files stored on a peer computer’s hard drive and print using a peer computer’s printer, provided those devices have been designated as ***shared devices***.
- Peer-to-peer networks are ***less expensive*** and ***less complicated*** to implement than client-server networks because there are ***no dedicated servers***, but they may not have the same performance as client-server networks under heavy use.
- Peer-to-peer capabilities are built into many personal operating systems and are often used with small office or home networks.

Peer-to-Peer (P2P) Architecture (Contd.)

- Another type of peer-to-peer networking— sometimes called ***Internet peer-to-peer*** (***Internet P2P***) ***computing*** — is performed via the ***Internet***. Instead of placing content on a Web server for others to view via the Internet, content is exchanged over the Internet directly between individual users via a peer-to-peer network.
- ***For instance,*** one user can copy a file from another user's hard drive to his or her own computer via the Internet. Internet P2P networking is commonly used for exchanging music and video files with others over the Internet—an illegal act if the content is copyright-protected and the exchange is unauthorized, although legal Internet P2P networks exist.

Fig 1: P2P network

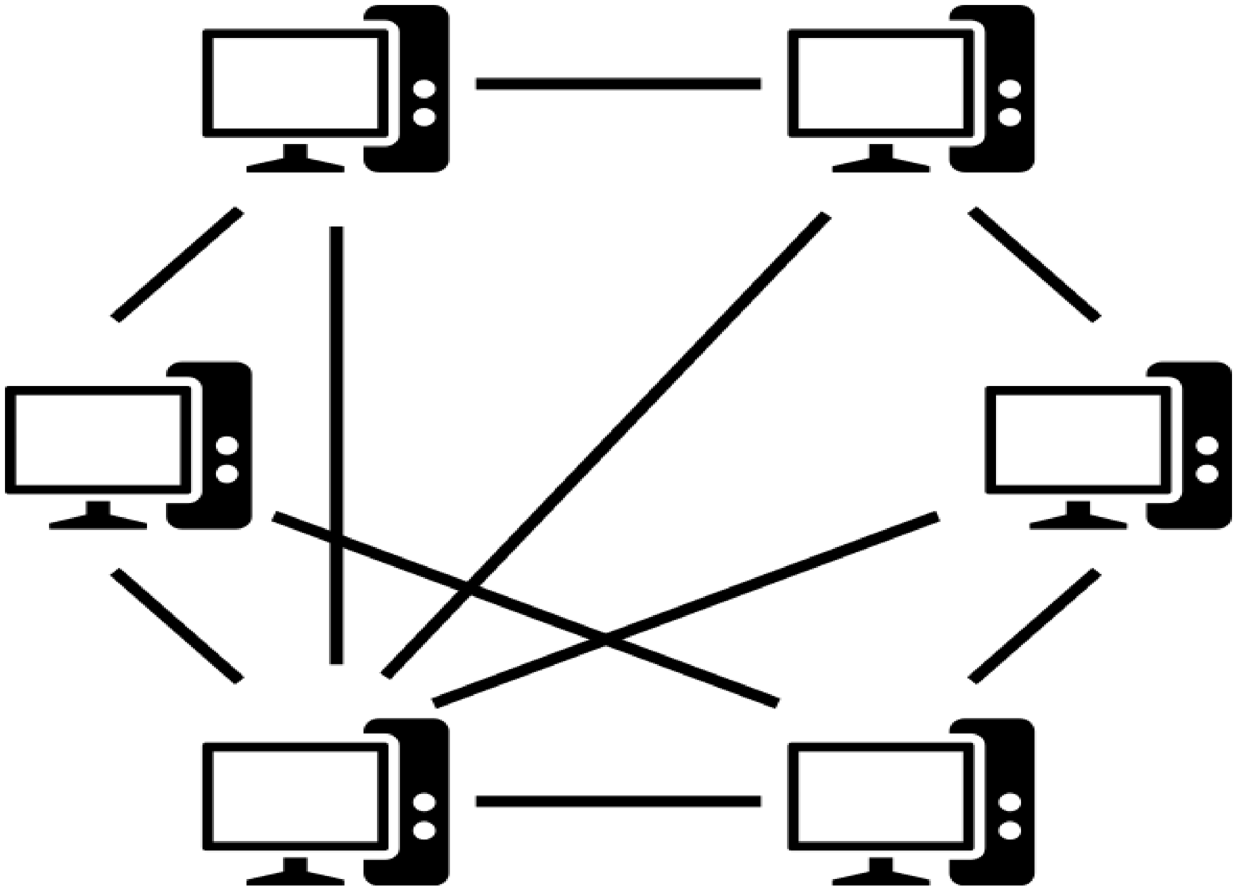
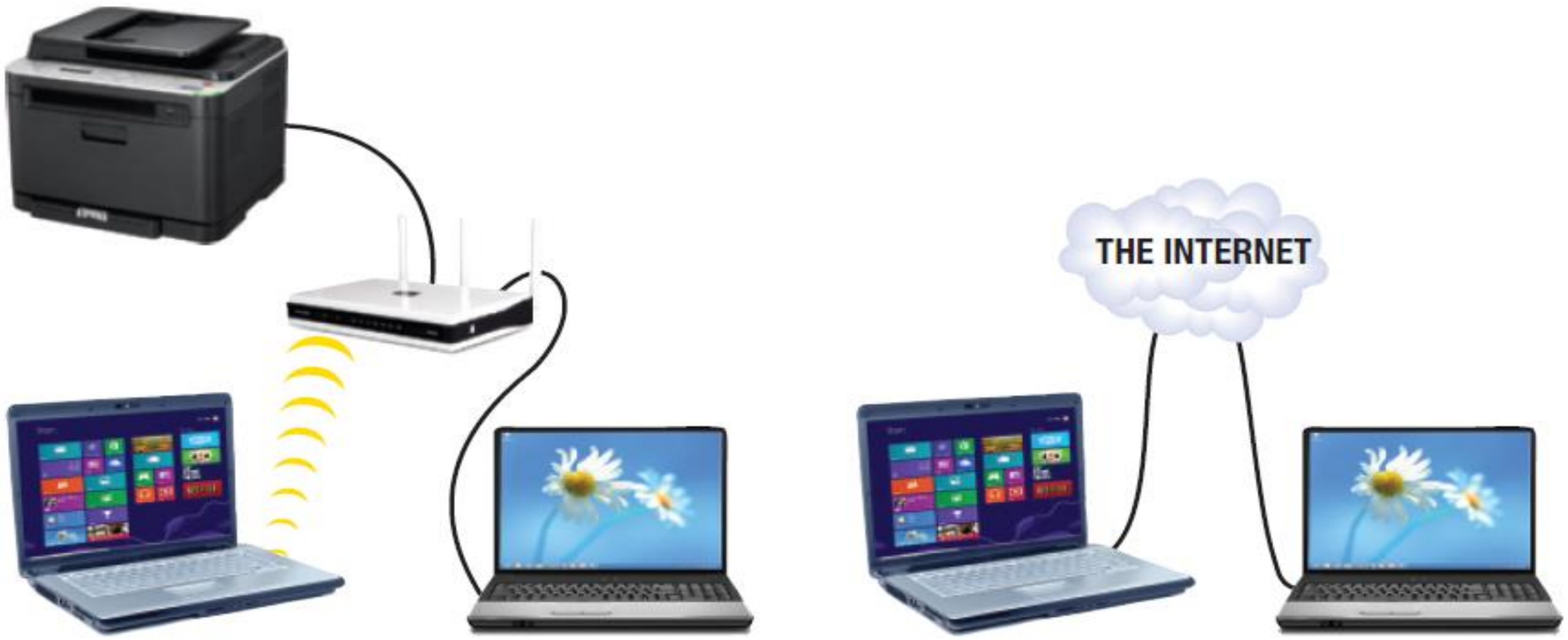


Fig 2: P2P and Internet P2P



P2P HOME NETWORKS
Devices connect and communicate via the home network.

INTERNET P2P NETWORKS
Devices connect and communicate via the Internet.

Network Size and Coverage Area (Types of Networks)

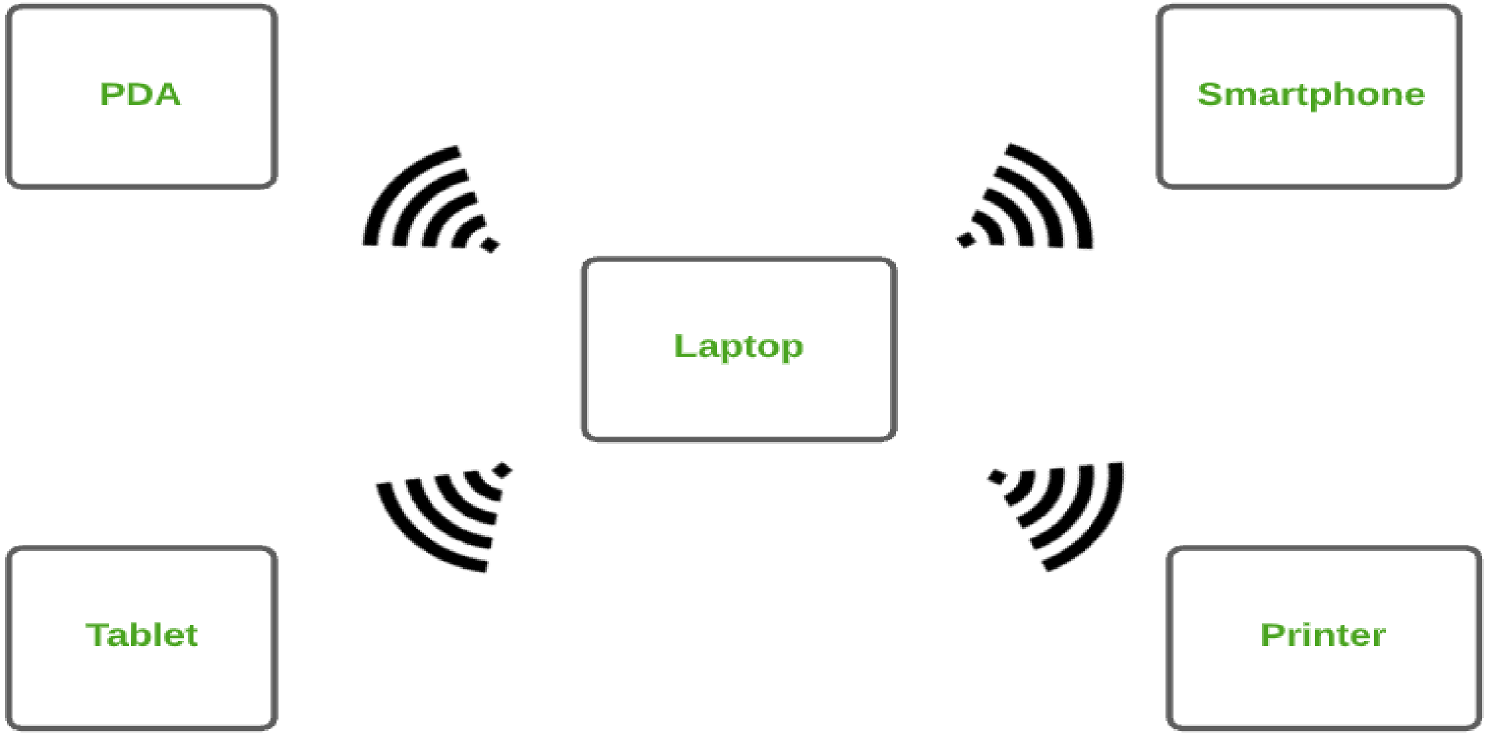
- One additional way networks are classified is by the size of their coverage area. This also impacts the types of users the network is designed to service. The most common categories of networks are discussed next; these networks can use both wired and wireless connections.

- On the basis of network size and coverage the types of networks are:
  - **PAN** (Personal Area Networks)
  - **LAN** (Local Area Networks)
  - **MAN** (Metropolitan Area Networks)
  - **WAN** (Wide Area Networks)
  - Intranets and Extranets
  - **VPNs** (Virtual Private Networks)

Personal Area Networks (PANs)

- A ***personal area network*** (**PAN**) is a small network of two or more personal devices for one individual (such as a computer, mobile phone, headset, media tablet, portable speakers, smart watch, fitness gadget, and printer) that is designed to enable those devices to communicate and share data.
- PANs can be set up on demand or set up to work together automatically as soon as the devices get within a certain physical distance of each other.
- For instance, a PAN can be used to synchronize a mobile device automatically with a personal computer whenever the devices are in range of each other, to connect a media tablet to a portable speaker, or to connect a mobile phone to a headset and/or smart watch.
- ***Wireless PANs*** (**WPANs**) are more common today than wired PANs and are typically implemented via Bluetooth or via the Internet using Google or another cloud service.

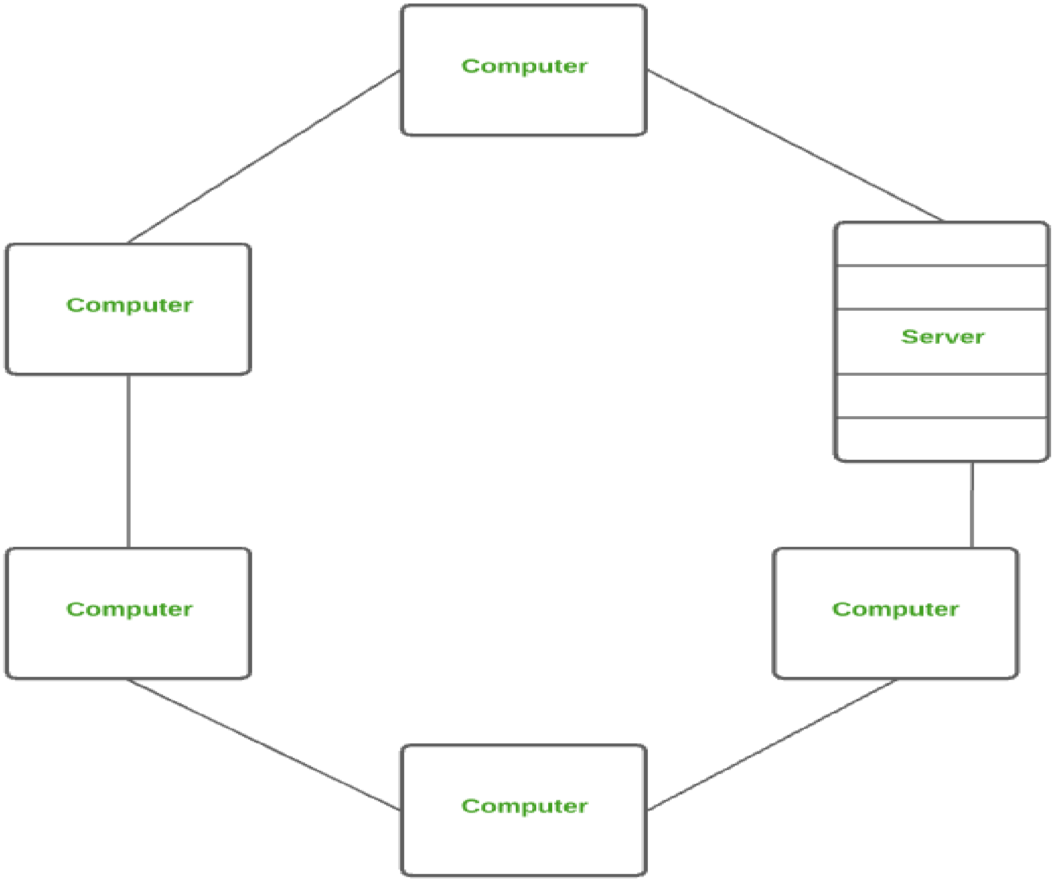
Fig: Personal Area Networks (PANs)



Local Area Networks (LANs)

- A ***local area network*** (**LAN**) is a network that covers a relatively small geographical area, such as a home, an office building, or a school.
- LANs allow users on the network to exchange files and e-mail, share printers and other hardware, and access the Internet.
- The client-server network shown in Figure previously is an example of a LAN.

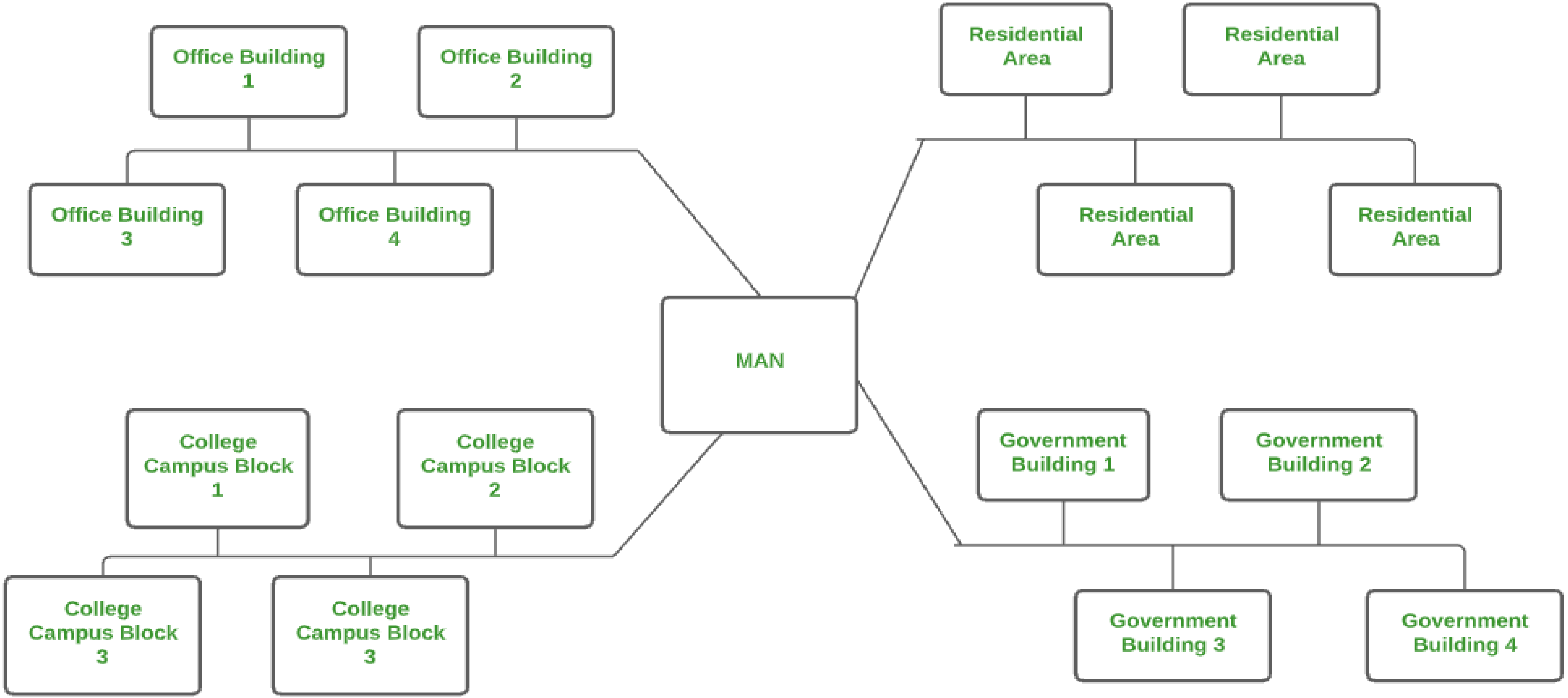
Fig: Local Area Networks (LANs)



Metropolitan Area Networks (MANs)

- A ***metropolitan area network*** (**MAN**) is a network designed to service a metropolitan area, typically a city or country. Most **MANs** are owned and operated by a city or by a network provider in order to provide individuals in that location access to the MAN.
- Some wireless MANs (often referred to as ***municipal Wi-Fi projects***) are created by cities or large organizations to provide free or low-cost Internet access to area residents.
- In addition, some Internet service providers are experimenting with setting up free wireless MANs in selected metropolitan areas for their subscribers to use for Internet access when they are on the go.

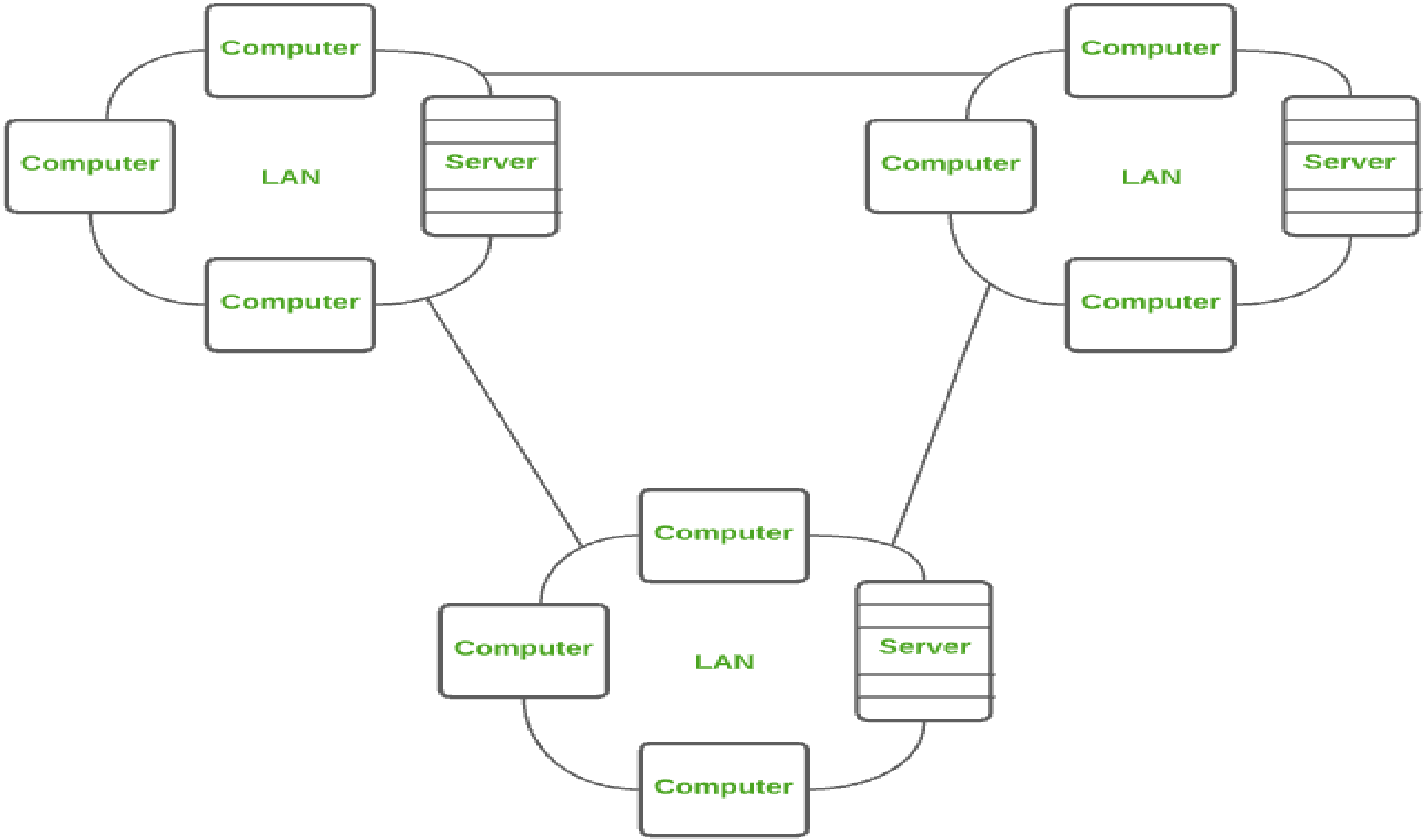
Fig: Metropolitan Area Networks (MANs)



Wide Area Networks (WANs)

- A ***wide area network*** (**WAN**) is a network that covers a large geographical area. Typically, a WAN consists of two or more LANs that are connected together using communications technology.
- The **Internet**, by this definition, is the world’s largest WAN. WANs may be publicly accessible, like the Internet, or they may be privately owned and operated.
- For instance, a company may have a private WAN to transfer data from one location to another, such as from each retail store to the corporate headquarters. Large WANs, like the Internet, typically use a ***mesh topology***.

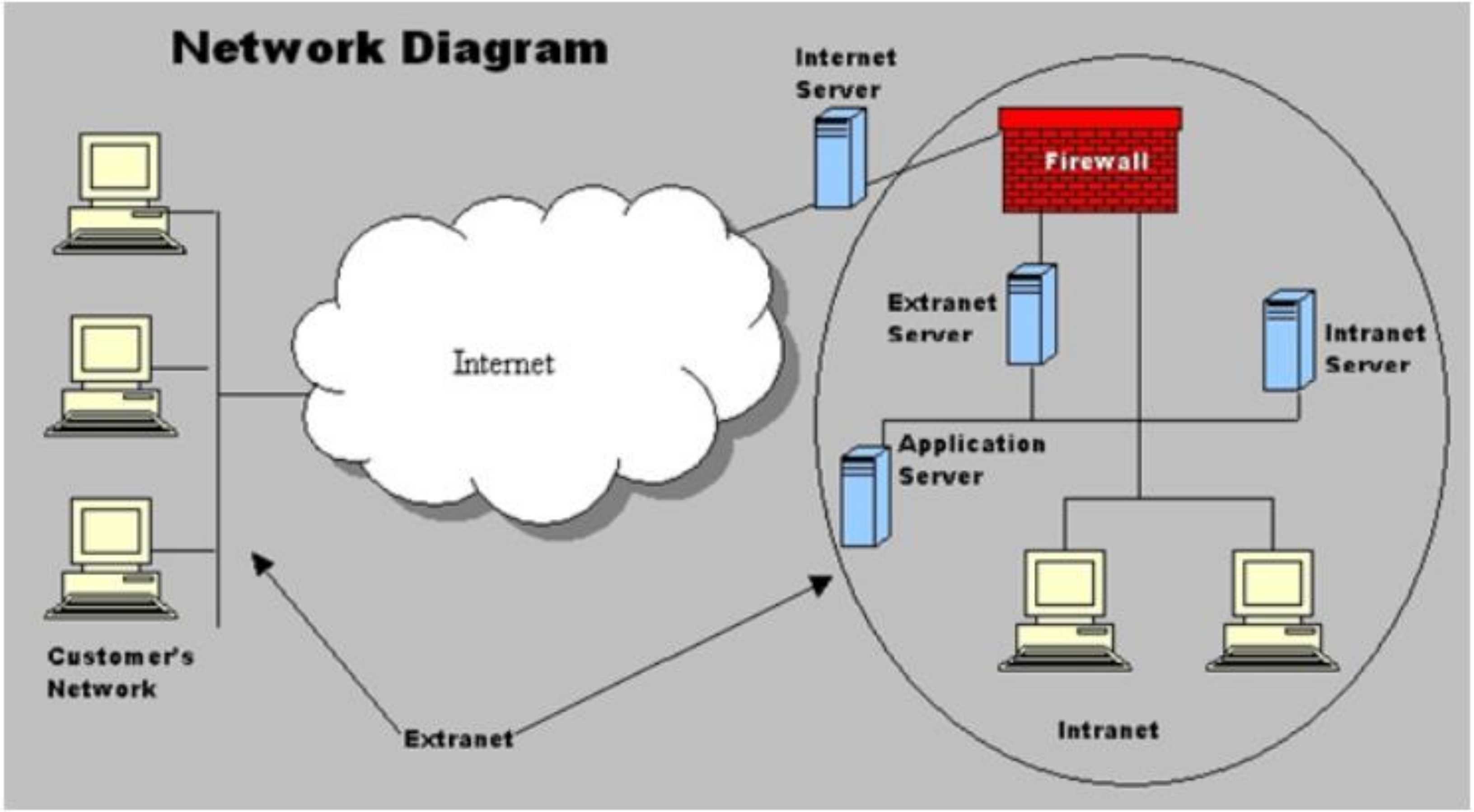
Fig: Wide Area Networks (WANs)



Intranets and Extranets

- An ***intranet*** is a private network (such as a company **LAN**) that is designed to be used by an organization’s employees and is set up like the Internet (with data posted on Web pages that are accessed with a Web browser).
- Consequently, little or no employee training is required to use an intranet, and intranet content can be accessed using a variety of devices.
- Intranets today are used for many purposes, including coordinating internal e-mail and communications, making company publications (such as contact information, manuals, forms, job announcements, and so forth) available to employees, facilitating collaborative computing, and providing access to shared calendars and schedules.
- A company network that is accessible to authorized outsiders is called an ***extranet***. ***Extranets*** are usually accessed via the Internet, and they can be used to provide customers and business partners with access to the data they need.

Fig: Intranets and Extranets



Virtual Private Networks (VPNs)

- A ***virtual private network*** (**VPN**) is a private, secure path across a public network (usually the Internet) that is set up to allow authorized users private, secure access to the company network.
- For instance, a VPN can allow a traveling employee, business partner, or employee located at a satellite office or public wireless hotspot to connect securely to the company network via the Internet.
- A process called ***tunneling*** is typically used to carry the data over the Internet; special encryption technology is used to protect the data so it cannot be understood if it is intercepted during transit.
- Essentially, VPNs allow an organization to provide secure, remote access to the company network without the cost of physically extending the private network.

Fig 1: Virtual Private Networks (VPNs)

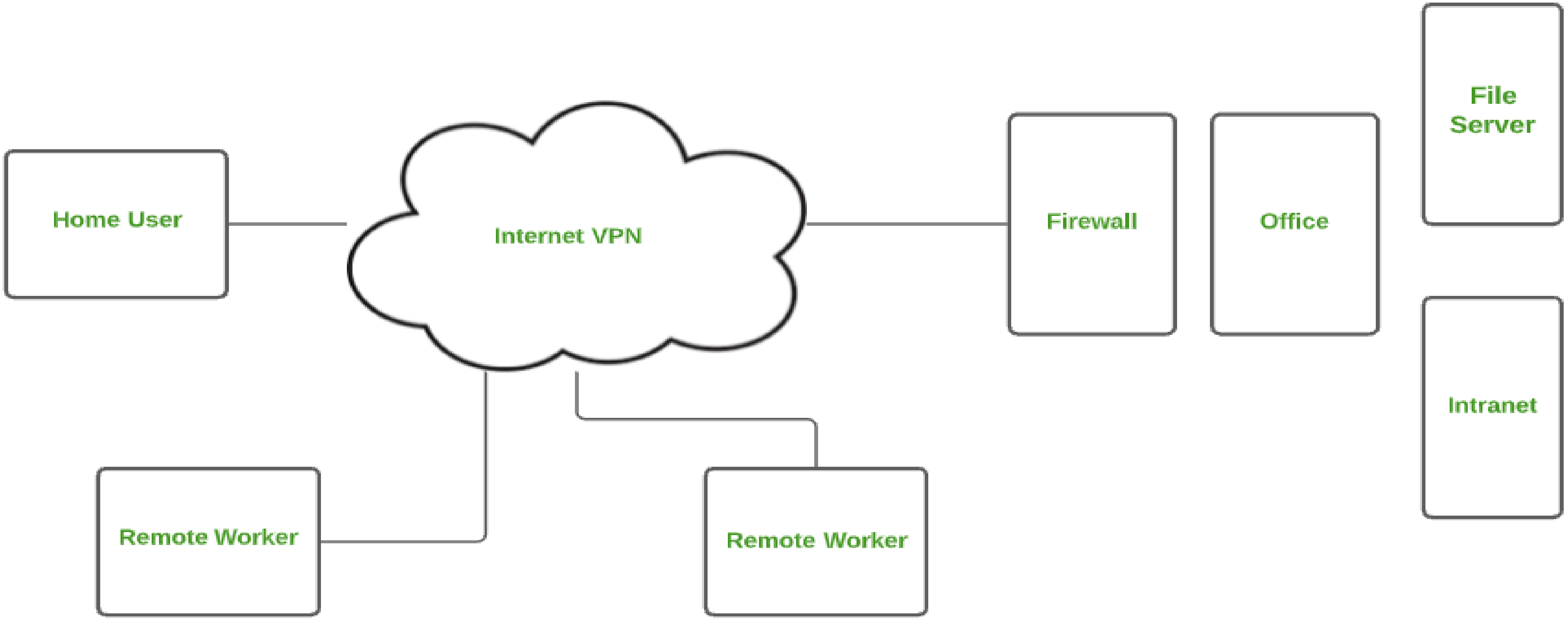
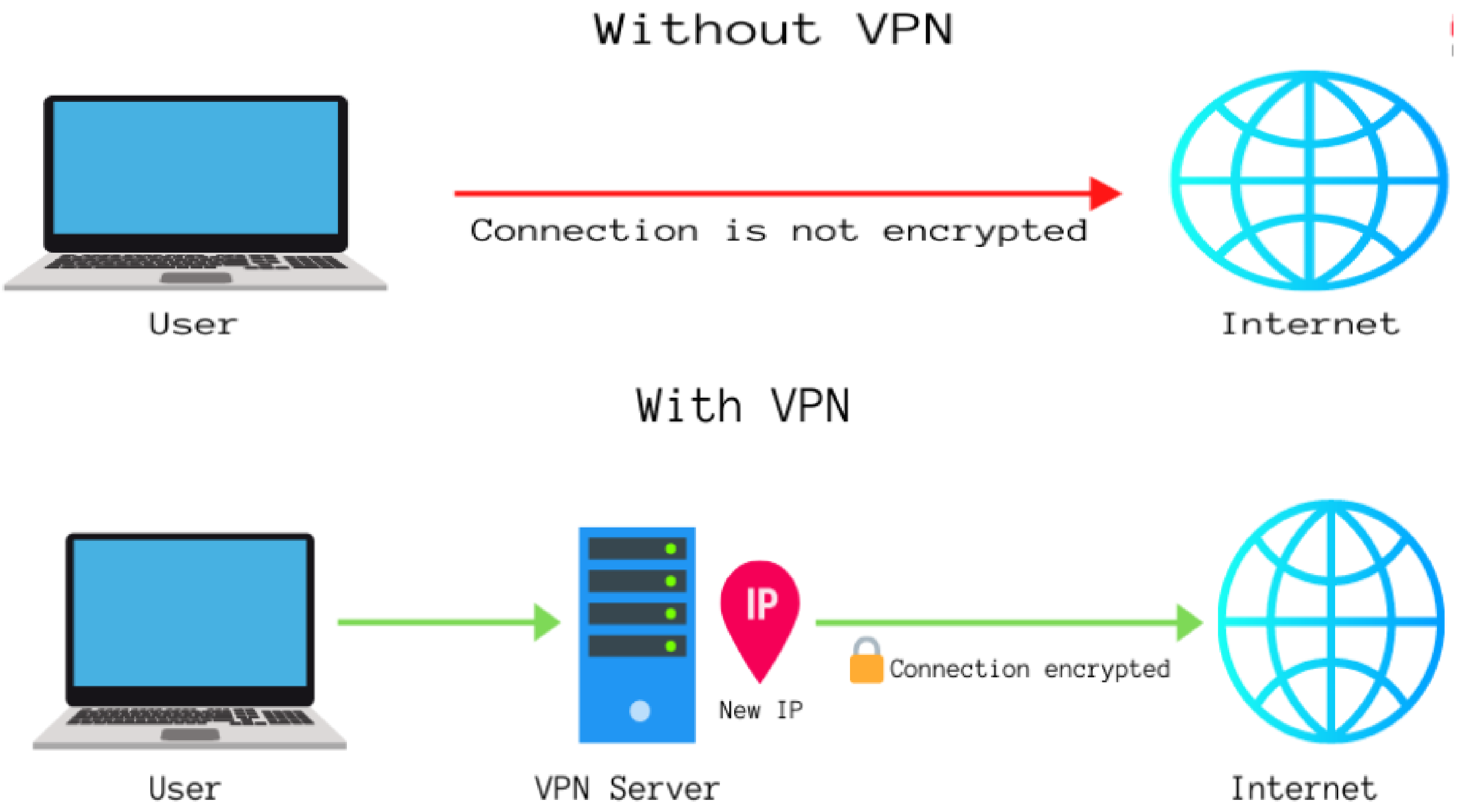


Fig 2: Virtual Private Networks (VPNs)



How can an individual surf safely at a public Wi-Fi hotspot?

- **First**, install Internet security software that includes antivirus, local firewall, and intrusion protection.
- **Next,** know the name of your Wi-Fi provider, create a unique username for that connection, and use a complex password comprised of random letters and numbers.
- When connecting through a logon page, view the site’s certificate presented by the browser to verify that the site is operated by the expected organization.
- In addition, turn off file and printer sharing to make it harder for a stranger to check your wireless activities, and avoid sending any confidential information (Social Security numbers, bank account passwords, and so on) over a Wi-Fi connection.
- If you can delay doing your online shopping or banking until you are back at home or the office, then do so!
- Unless you are connected to the Internet over an encrypted connection, assume that someone could potentially gain access to your personal information.
- **Lastly,** when possible, use a Virtual Private Network (VPN), which provides stronger protection against a variety of risks.

Data Transmission Across Media

DATA TRANSMISSION CHARACTERISTICS

- Data transmitted over a network has specific characteristics, and it can travel over a network in various ways.
- These are some characteristics related to data transmission:
  - Bandwidth
  - Analog vs. Digital Signals
  - Transmission Type and Timing
  - Delivery Method

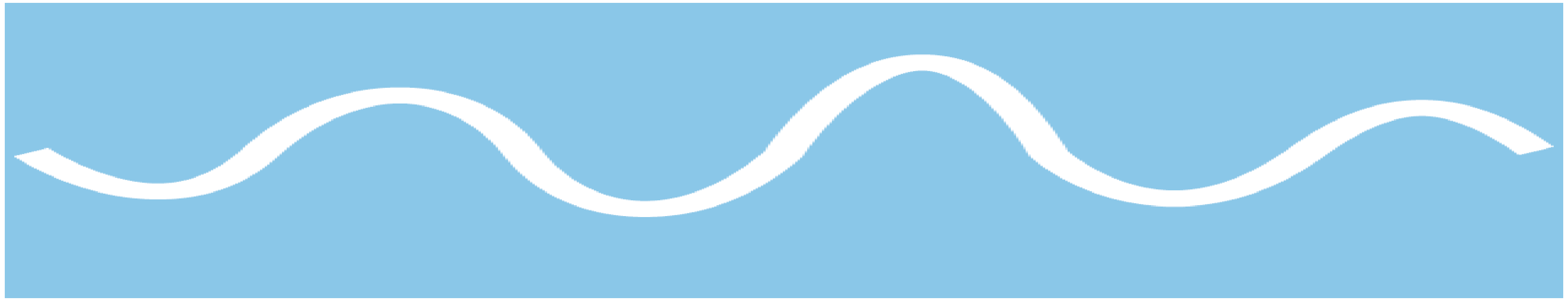
Bandwidth

- The term ***bandwidth*** (also called ***throughput***) refers to the amount of data that can be transferred (such as over a certain type of networking medium) in a given time period.
- Text data requires the least amount of bandwidth; video data requires the most; a networking medium with a high bandwidth allows more data to pass through it per unit of time than a networking medium with a low bandwidth.
- Bandwidth is usually measured in the number of bits per second (bps), Kbps (thousands of bits per second), Mbps (millions of bits per second), or Gbps (billions of bits per second).

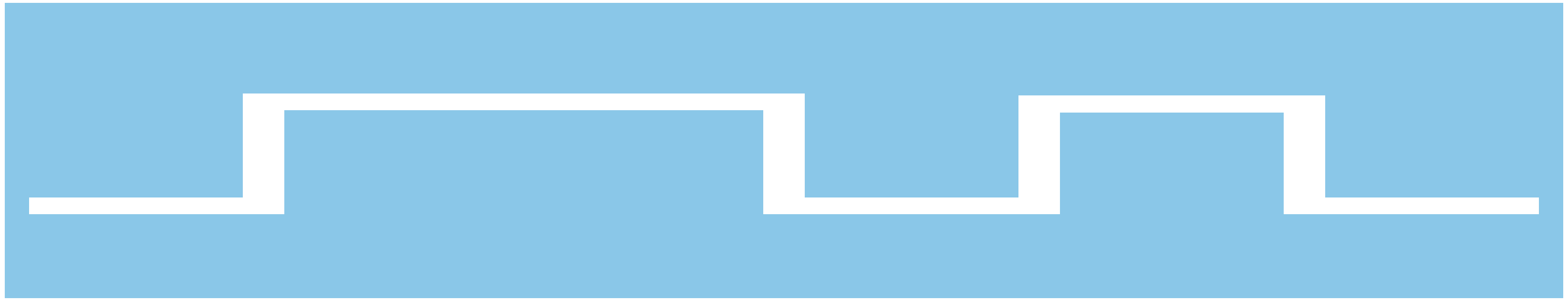
Analog vs. Digital Signals

- Data can be represented as either analog or digital signals. Voice and music data in its natural form, for instance, is analog, and data stored on a computer is digital.
- Most networking media send data using ***digital signals***, in which data is represented by only two discrete states: 0s and 1s.
- ***Analog signals***, such as those used by conventional telephone systems, represent data with ***continuous waves***. The data to be transmitted over a networking medium must match the type of signal (analog or digital) that the medium supports; if it doesn't originally, then it must be converted before the data is transmitted.
- For instance, analog data that is to be sent using digital signals (such as analog music broadcast by a digital radio station) must first be converted into digital form, and digital data to be sent using analog signals (such as computer data sent over a conventional analog telephone network) must be converted into analog form before it can be transmitted.
- The conversion of data between analog and digital form is performed by networking hardware.

Fig: Analog vs. Digital Signals



ANALOG SIGNALS

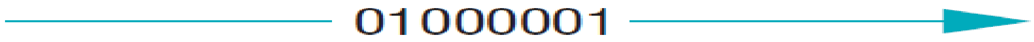


DIGITAL SIGNALS

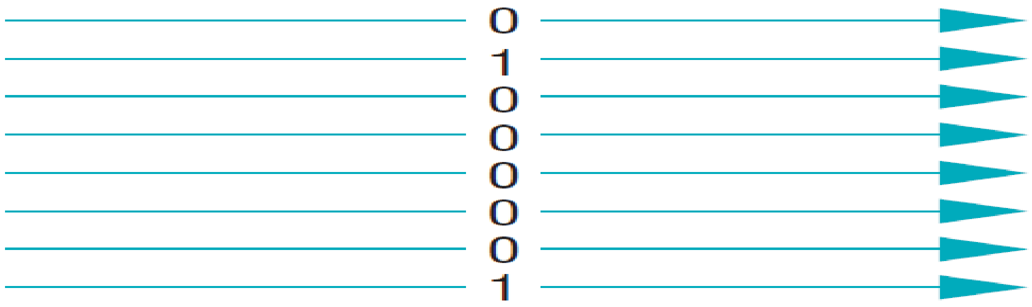
Transmission Type and Timing

- Networking media can also use either ***serial transmission*** or ***parallel transmission***.
- With ***serial transmission***, data is sent one bit at a time, one after the other along a single path (see Figure). When ***parallel transmission*** is used, the message is sent at least one byte at a time, with each bit in the byte taking a separate path (refer to Figure). While ***parallel transmission*** is frequently used within computer components (such as buses) and is used for some wireless networking applications, networking media typically use ***serial transmission***.
- When data is sent using ***serial transmission***, a technique must be used to organize the bits being transferred so the data can be reconstructed after it is received.
- Three ways of timing serial transmissions are by using ***synchronous***, ***asynchronous***, and ***isochronous connections*** (see Figure).

Serial vs. Parallel transmissions.



SERIAL TRANSMISSIONS
All the bits in one byte follow one another over a single path.



PARALLEL TRANSMISSIONS
The eight bits in each byte are transmitted over separate paths at the same time.

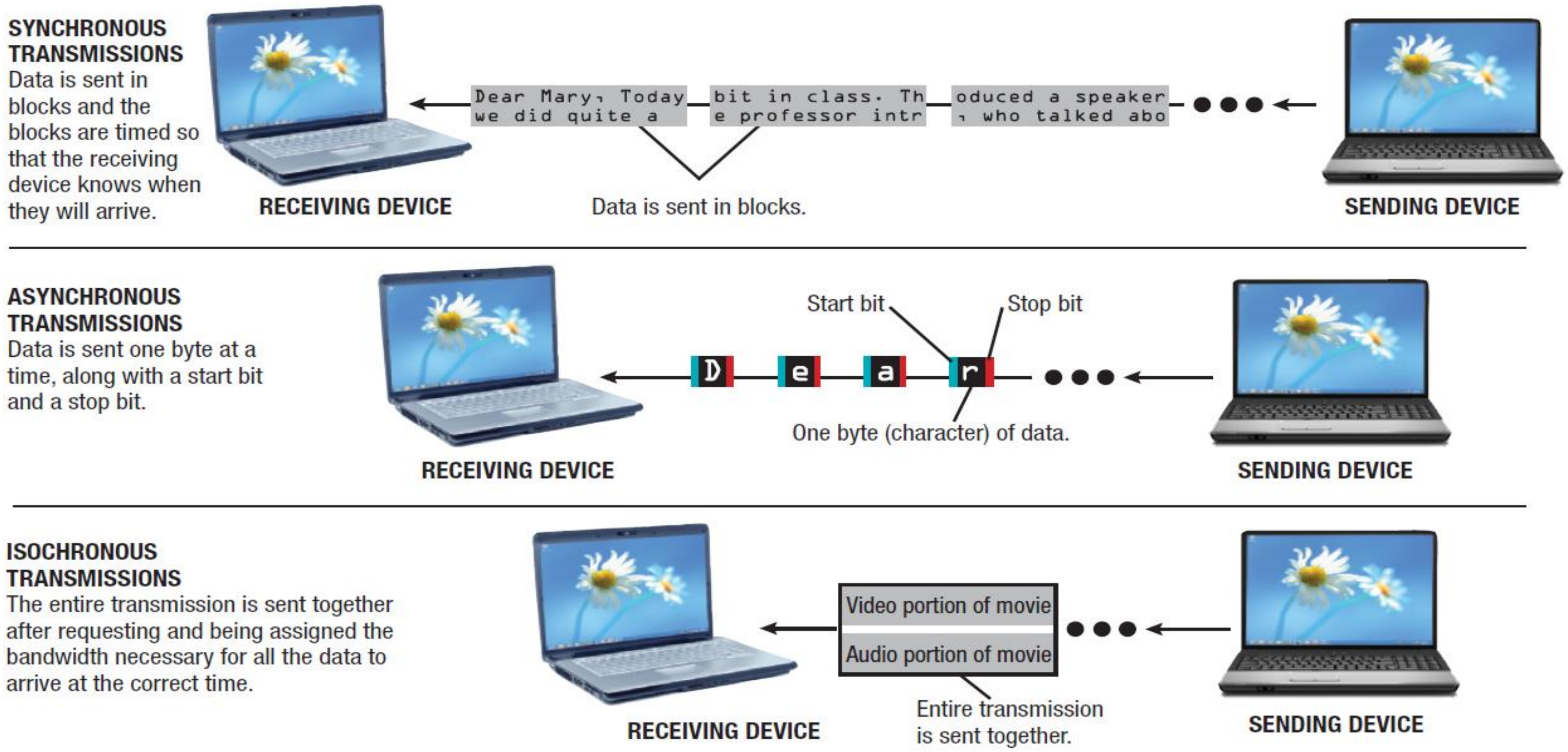
Transmission Type and Timing (Contd.)

- Although all three of these methods send data one bit at a time, the methods vary with respect to how the bits are organized for transfer.
  - ➢ ***Synchronous transmission***—data is organized into groups or blocks of data, which are transferred at regular, specified intervals. Because the transmissions are synchronized, both devices know when data can be sent and when it should arrive. Most data transmissions within a computer and over a network are synchronous transmissions.
  - ➢ ***Asynchronous transmission***—data is sent when it is ready to be sent, without being synchronized. To identify the bits that belong in each byte, a start bit and stop bit are used at the beginning and end of the byte, respectively. This overhead makes asynchronous transmission less efficient than synchronous transmission and so it is not as widely used as synchronous transmission.

Transmission Type and Timing (Contd.)

- ***Isochronous transmission***—data is sent at the same time as other related data to support certain types of real-time applications that require the different types of data to be delivered at the proper speed for that application. For example, when transmitting a video file, the audio data must be received at the proper time in order for it to be played with its corresponding video data. To accomplish this with isochronous transmission, the sending and receiving devices first communicate to determine the bandwidth and other factors needed for the transmission, and then the necessary bandwidth is reserved just for that transmission.

Transmission timing - Most network transmissions use synchronous transmission.



SYNCHRONOUS TRANSMISSIONS
Data is sent in blocks and the blocks are timed so that the receiving device knows when they will arrive.

RECEIVING DEVICE
Dear Mary, Today we did quite a
bit in class. The professor intr
oduced a speaker, who talked abo
Data is sent in blocks.
SENDING DEVICE

ASYNCHRONOUS TRANSMISSIONS
Data is sent one byte at a time, along with a start bit and a stop bit.

Start bit
Stop bit
D
e
a
r
One byte (character) of data.
RECEIVING DEVICE
SENDING DEVICE

ISOCHRONOUS TRANSMISSIONS
The entire transmission is sent together after requesting and being assigned the bandwidth necessary for all the data to arrive at the correct time.

Transmission Type and Timing (Contd.)

- Another distinction between types of transmissions is the direction in which transmitted data can move.
  - ➢ ***Simplex transmission***—data travels in a single direction only (like a doorbell). Simplex transmission is relatively uncommon in data transmissions because most devices that are mainly one-directional, such as a printer, can still transmit error messages and other data back to the computer.
  - ➢ ***Half-duplex transmission***—data can travel in either direction, but only in one direction at a time (like a walkie-talkie where only one person can talk at a time). Some network transmissions are half-duplex.
  - ➢ ***Full-duplex transmission***—data can move in both directions at the same time (like a telephone). Many network and most Internet connections are full-duplex; sometimes two connections between the sending device and receiving device are needed to support full-duplex transmissions.

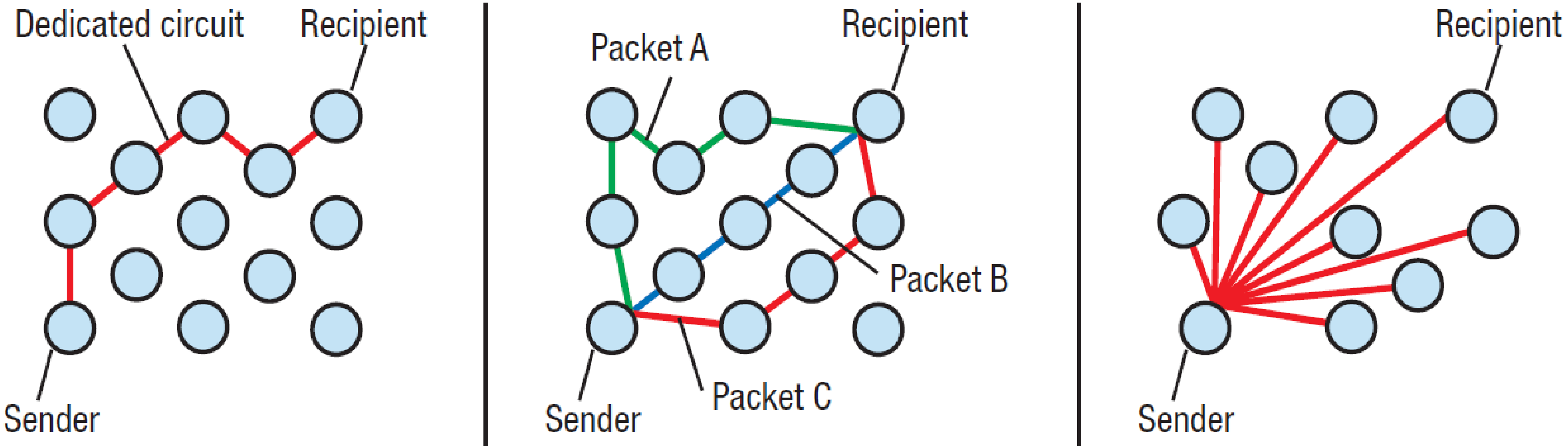
Delivery Method

- When data needs to travel across a large network (such as a **WAN**), typically one of three methods is used such as ***circuit-switched***, ***packet-switched***, and ***broadcast networks***.
- With ***circuit switching***, a dedicated path over a network is established between the sender and receiver and all data follows that path from the sender to the receiver. Once the connection is established, the physical path or circuit is dedicated to that connection and cannot be used by any other device until the transmission is finished. The most common example of a ***circuit-switched network*** is a ***conventional telephone system***.
- The technique used for data sent over the Internet is ***packet switching***. With ***packet switching***, messages are separated into small units called ***packets***. Packets contain information about the sender and the receiver, the actual data being sent, and information about how to reassemble the packets to reconstruct the original message.

Delivery Method (Contd.)

- ***Packets*** travel along the network separately, based on their final destination, network traffic, and other network conditions. When the packets reach their destination, they are reassembled in the proper order.
- Another alternative is ***broadcasting***, in which data is sent out (typically in ***packets***) to all nodes on a network and is retrieved only by the intended recipient. ***Broadcasting*** is used primarily with LANs.

Fig: Circuit-switched, packet-switched, and broadcast networks.



CIRCUIT-SWITCHED NETWORKS
Data uses a dedicated path from the sender to the recipient.

PACKET-SWITCHED NETWORKS
Data is sent as individual packets, which are assembled at the recipient's destination.

BROADCAST NETWORKS
Data is broadcast to all nodes within range; the designated recipient retrieves the data.

Data Communication Media

NETWORKING MEDIA

- To connect the devices in a network, either **wired media** (physical cables) or **wireless media** (typically radio signals) can be used. The most common are wired and wireless networking media.
- A ***transmission medium*** can be broadly defined as anything that can carry information from a source to a destination. The transmission medium is usually **twisted-pair**, **fiber-optic cable**, **radio transmission** etc.
- Transmission media can be generally categorized as either ***guided*** (**wired media**) or ***unguided*** **(wireless media)**.

Wired Networking Media (or Guided Media)

- In the ***guided media***, the data signals are sent along a specific path, through a wire or a cable. Copper wire and optical fibers are the most commonly used guided media that transmits data as electric signals.
- The most common types of wired networking media are
  - Twisted-Pair Cable
  - Coaxial Cable
  - Fiber-Optic Cable

Guided Media – Twisted Pair Cable

- A twisted-pair cable is made up of pairs of thin strands of insulated wire twisted together. Twisted-pair is the least expensive type of networking cable and has been in use the longest.
- In fact, it is the same type of cabling used inside most homes for telephone communications. Twisted-pair cabling can be used with both analog and digital data transmission and is commonly used for LANs.
- Twisted-pair cable is rated by ***category***, which indicates the type of data, speed, distance, and other factors that the cable supports.
- ***Category 3*** (**Cat 3**) twisted-pair cabling is regular telephone cable; higher speed and quality cabling—such as ***Category 5*** (**Cat 5**), ***Category 6*** (**Cat 6**), and ***Category 7*** (**Cat 7**)—is frequently used for home or business networks.
- To further improve performance, it can be shielded with a metal lining. Twisted-pair cables used for networks have different connectors than those used for telephones. Networking connectors are typically ***RJ-45*** connectors, which look similar to, but are larger than, telephone ***RJ-11*** connectors.

Guided Media – Twisted Pair Cable (Contd.)

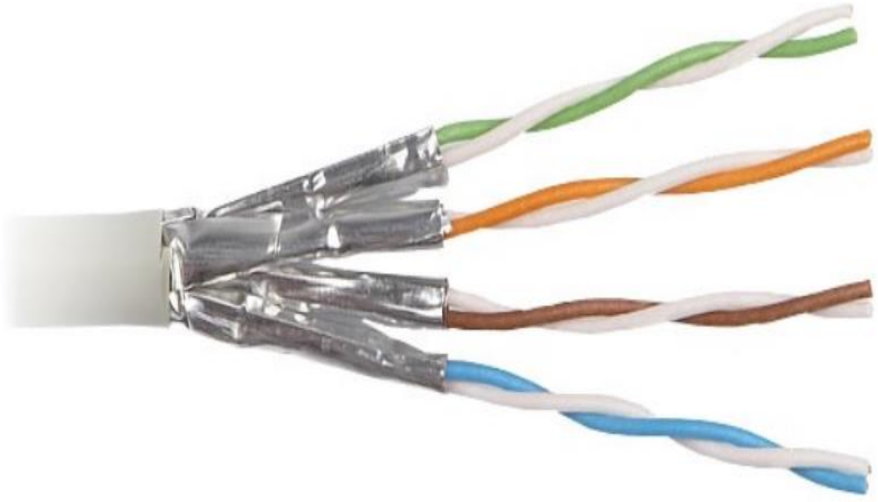
- The two basic types of twisted-pair transmission lines specified are ***unshielded twisted pair*** **(UTP)** and ***shielded twisted pair*** **(STP)**.

  - **STP cable** has an extra layer of metal foil between the twisted pair of copper wires and the outer covering. The metal foil covering provides additional protection from external disturbances. However, the covering increases the resistance to the signal and thus decreases the length of the cable. STP is costly and is generally used in networks where cables pass closer to devices that cause external disturbances.

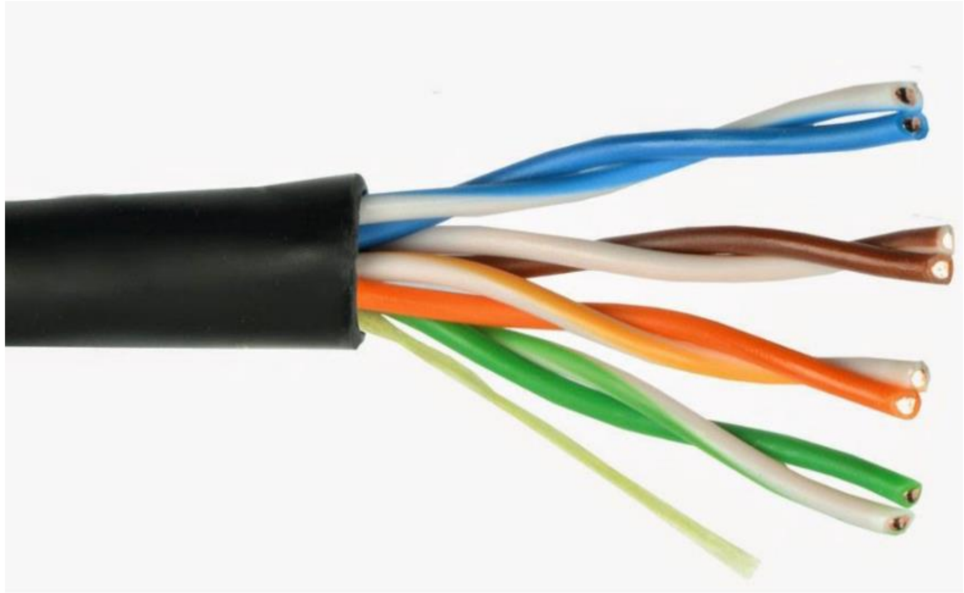
  - **UTP cable** is the most commonly used medium for transmission over short distances up to 100m. Out of the four pairs of wires in a UTP cable, only two pairs are used for communication. A twisted pair consists of two insulated conductors (usually copper) in a twisted configuration. Color bands are used in plastic insulation for identification

Fig: STP and UTP

STP



UTP



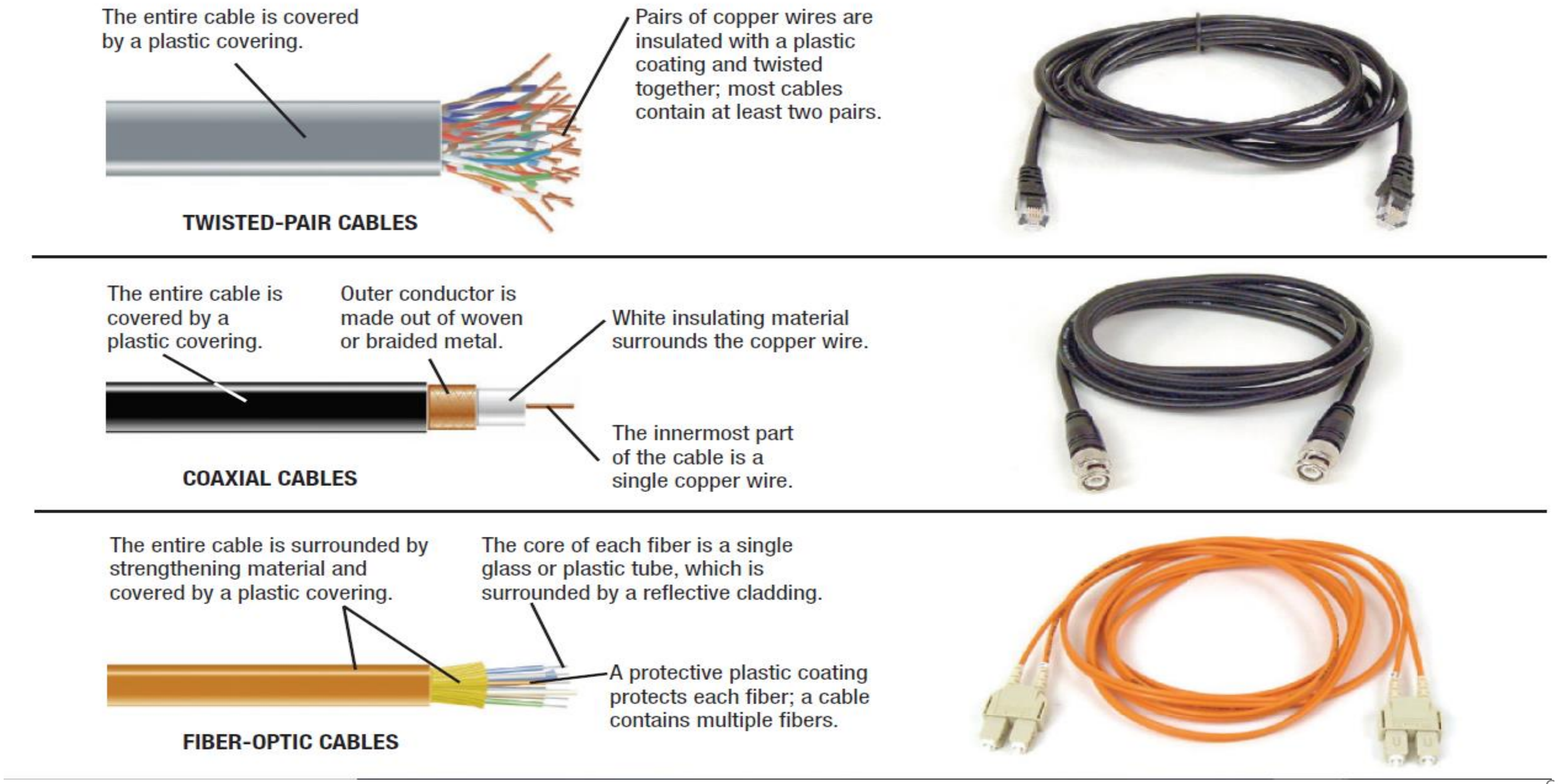
Guided Media – Coaxial Cable

- ***Coaxial cable*** (also ***known as coax***) was originally developed to carry a large number of high-speed video transmissions at one time, such as to deliver cable TV service.
- A coaxial cable consists of a relatively thick center wire surrounded by insulation and then covered with a shield of braided wire to block electromagnetic signals from entering the cable.
- Coaxial cable is commonly used today in computer networks, for short-run telephone transmissions outside of the home, and for cable television delivery.
- Although more expensive than twisted-pair cabling, it is much less susceptible to interference and can carry more data more quickly.

Guided Media – Fiber-Optic Cable

- ***Fiber-optic cable*** is the newest and fastest of these three types of wired transmission media. It contains multiple (sometimes several hundred) clear glass or plastic fiber strands, each about the thickness of a human hair.
- Fiber-optic cable transfers data represented by light pulses at speeds of billions of bits per second. Each strand has the capacity to carry data for several television stations or thousands of voice conversations, but each strand can only send data in one direction so two strands are needed for full-duplex data transmissions.
- Fiber-optic cable is commonly used for the high-speed backbone lines of a network, such as to connect networks housed in separate buildings or for the Internet infrastructure.
- It is also used for telephone backbone lines and, increasingly, is being installed by telephone companies all the way to the home or business to provide super-fast connections directly to the end user.
- The biggest ***advantage*** of fiber-optic cabling is ***speed***; the main ***disadvantage*** of fiber-optic cabling is the ***initial expense of both the cable and the installation***.

Fig: Fiber-Optic Cable



The entire cable is covered by a plastic covering.

Pairs of copper wires are insulated with a plastic coating and twisted together; most cables contain at least two pairs.

TWISTED-PAIR CABLES

The entire cable is covered by a plastic covering.

Outer conductor is made out of woven or braided metal.

White insulating material surrounds the copper wire.

The innermost part of the cable is a single copper wire.

COAXIAL CABLES

The entire cable is surrounded by strengthening material and covered by a plastic covering.

The core of each fiber is a single glass or plastic tube, which is surrounded by a reflective cladding.

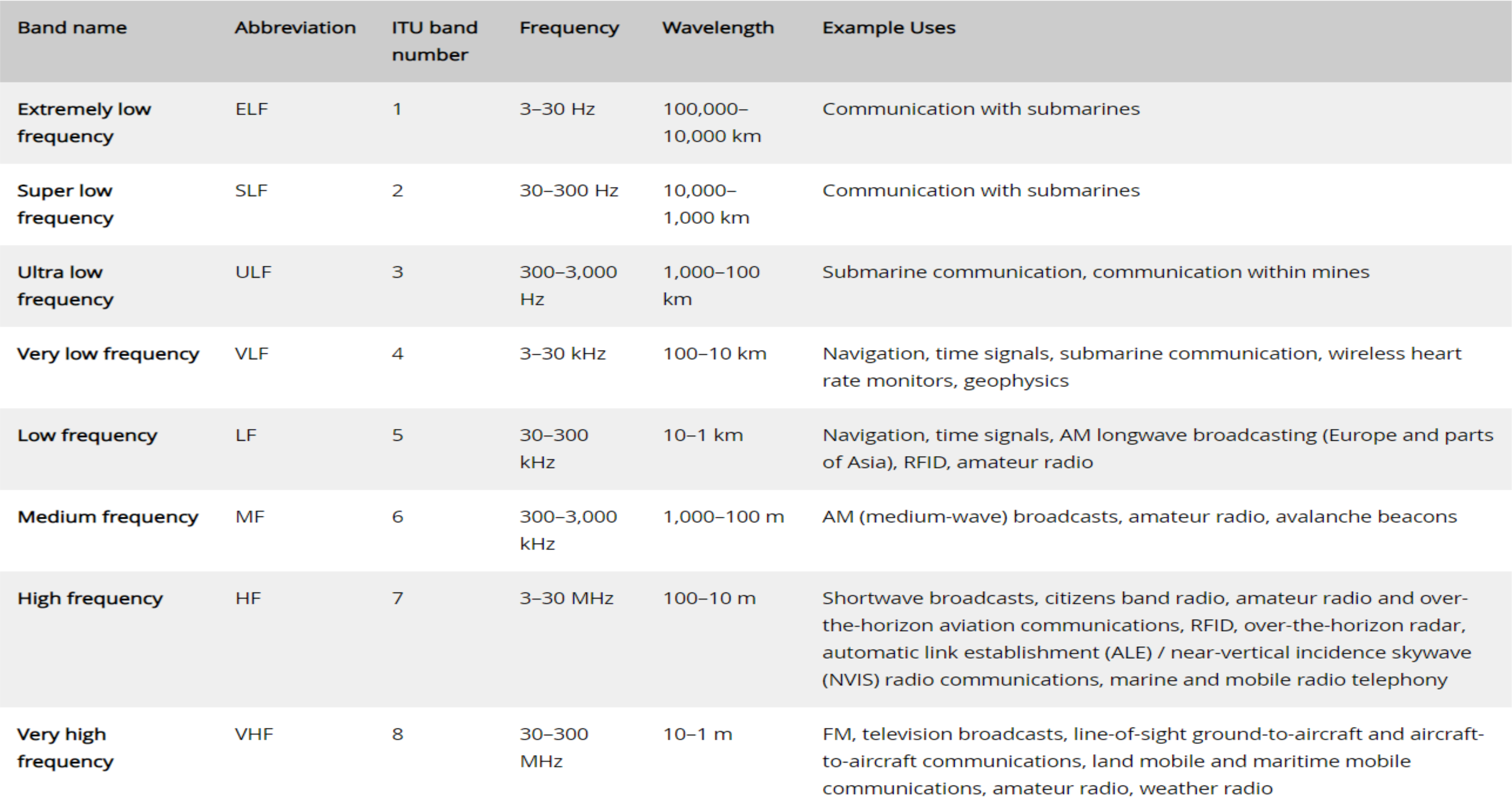
A protective plastic coating protects each fiber; a cable contains multiple fibers.

FIBER-OPTIC CABLES

Wireless Networking Media(or Unguided Media)

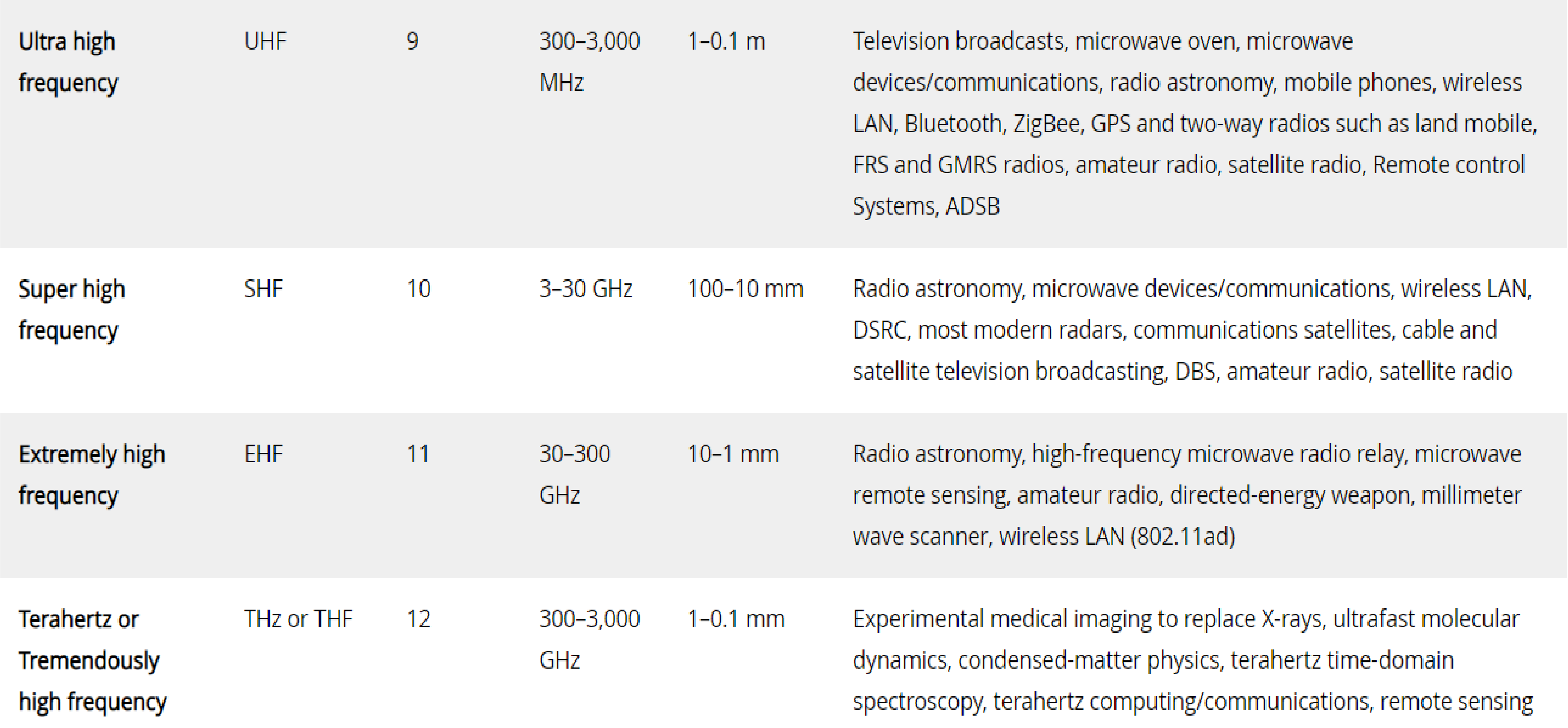
- ***Wireless networks*** usually use radio signals to send data through the airwaves.
- Depending on the networking application, ***radio signals*** can be ***short range*** (such as when used to connect a wireless keyboard or mouse to a computer), ***medium range*** (such as when used to connect a computer to a wireless LAN or public hotspot), or ***long range*** (such as when used to provide Internet access or cell phone coverage to a relatively large geographic area or to broadcast TV or radio shows).
- Signals are normally broadcast through ***free space*** and thus are available to anyone who has a device capable of receiving them.
- ***Cellular Radio Transmissions***, ***microwave*** and ***satellite transmissions*** and ***Infrared (IR) Transmissions*** fall into this category.

RF frequency bands



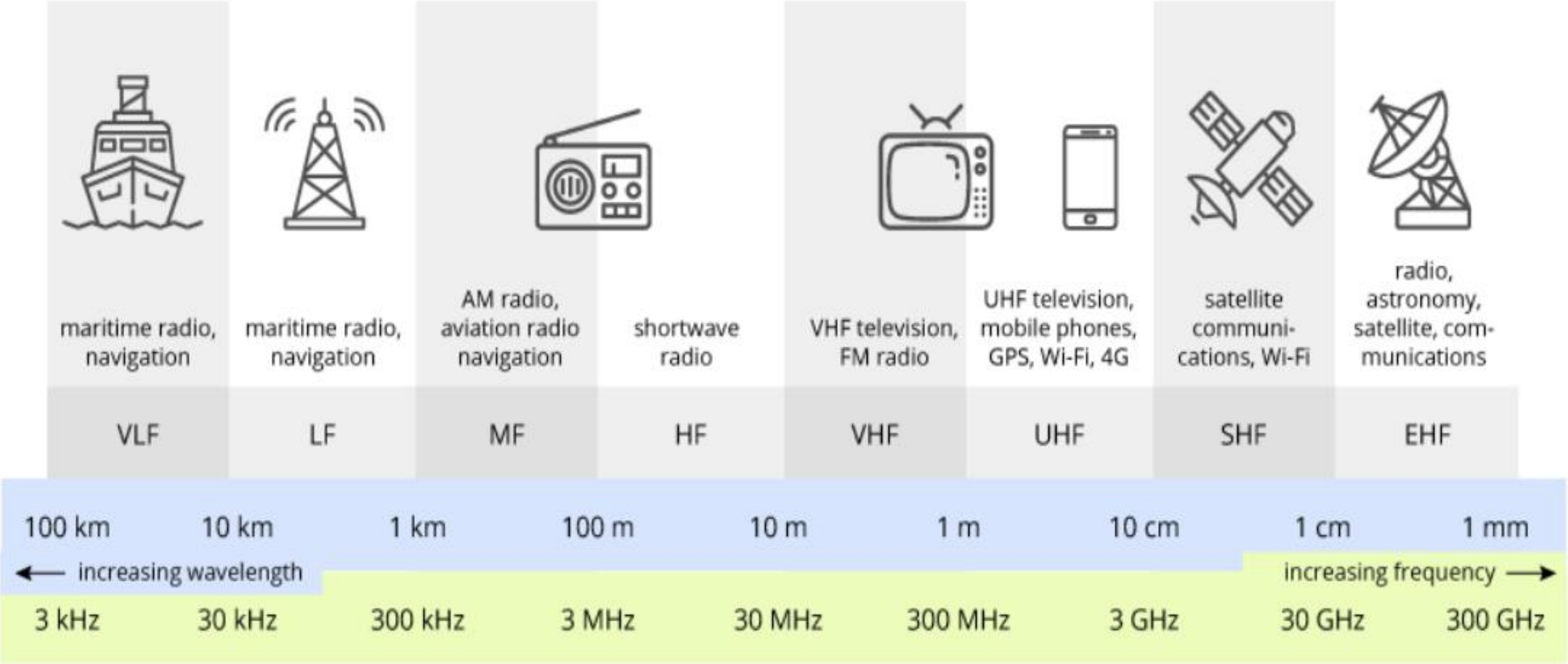
Band name	Abbreviation	ITU band number	Frequency	Wavelength	Example Uses
Extremely low frequency	ELF	1	3–30 Hz	100,000–10,000 km	Communication with submarines
Super low frequency	SLF	2	30–300 Hz	10,000–1,000 km	Communication with submarines
Ultra low frequency	ULF	3	300–3,000 Hz	1,000–100 km	Submarine communication, communication within mines
Very low frequency	VLF	4	3–30 kHz	100–10 km	Navigation, time signals, submarine communication, wireless heart rate monitors, geophysics
Low frequency	LF	5	30–300 kHz	10–1 km	Navigation, time signals, AM longwave broadcasting (Europe and parts of Asia), RFID, amateur radio
Medium frequency	MF	6	300–3,000 kHz	1,000–100 m	AM (medium-wave) broadcasts, amateur radio, avalanche beacons
High frequency	HF	7	3–30 MHz	100–10 m	Shortwave broadcasts, citizens band radio, amateur radio and over-the-horizon aviation communications, RFID, over-the-horizon radar, automatic link establishment (ALE) / near-vertical incidence skywave (NVIS) radio communications, marine and mobile radio telephony
Very high frequency	VHF	8	30–300 MHz	10–1 m	FM, television broadcasts, line-of-sight ground-to-aircraft and aircraft-to-aircraft communications, land mobile and maritime mobile communications, amateur radio, weather radio

RF frequency bands (Contd.)



Ultra high frequency	UHF	9	300–3,000 MHz	1–0.1 m	Television broadcasts, microwave oven, microwave devices/communications, radio astronomy, mobile phones, wireless LAN, Bluetooth, ZigBee, GPS and two-way radios such as land mobile, FRS and GMRS radios, amateur radio, satellite radio, Remote control Systems, ADSB
Super high frequency	SHF	10	3–30 GHz	100–10 mm	Radio astronomy, microwave devices/communications, wireless LAN, DSRC, most modern radars, communications satellites, cable and satellite television broadcasting, DBS, amateur radio, satellite radio
Extremely high frequency	EHF	11	30–300 GHz	10–1 mm	Radio astronomy, high-frequency microwave radio relay, microwave remote sensing, amateur radio, directed-energy weapon, millimeter wave scanner, wireless LAN (802.11ad)
Terahertz or Tremendously high frequency	THz or THF	12	300–3,000 GHz	1–0.1 mm	Experimental medical imaging to replace X-rays, ultrafast molecular dynamics, condensed-matter physics, terahertz time-domain spectroscopy, terahertz computing/communications, remote sensing

RF frequency bands (Contd.)



VLF	LF	MF	HF	VHF	UHF	SHF	EHF
maritime radio, navigation	maritime radio, navigation	AM radio, aviation radio navigation	shortwave radio	VHF television, FM radio	UHF television, mobile phones, GPS, Wi-Fi, 4G	satellite communi-cations, Wi-Fi	radio, astronomy, satellite, com-munications

100 km	10 km	1 km	100 m	10 m	1 m	10 cm	1 cm	1 mm
3 kHz	30 kHz	300 kHz	3 MHz	30 MHz	300 MHz	3 GHz	30 GHz	300 GHz

Unguided Media - Cellular Radio Transmissions

- ***Cellular radio transmissions*** are used with cell phones and are sent and received via ***cellular (cell) towers***—tall metal towers with antennas on top. Cellular service areas are divided into honeycomb-shaped zones called ***cells***; each cell contains one cell tower.
- When a cell phone user begins to make a call, it is picked up by the appropriate cell tower (the one that is located in the cell in which the cell phone is located and that is associated with the user's wireless provider).
- That cell tower then forwards the call to the wireless provider's ***Mobile Telephone Switching Office*** (**MTSO**), which routes the call to the recipient's telephone via his or her mobile or conventional telephone service provider (depending on the type of phone being used by the recipient).
- When a cell phone user moves out of the current cell into a new cell, the call is passed automatically to the appropriate cell tower in the cell that the user is entering.
- Data (such as e-mail and Web page requests) sent via cell phones works in a similar manner.

Unguided Media - Microwave and Satellite Transmissions

- ***Microwaves*** are high-frequency radio signals that can send large quantities of data at high speeds over long distances.
- Microwave signals can be sent or received using ***microwave stations or communications satellites***, but they must travel in a straight line from one station or satellite to another without encountering any obstacles because microwave signals are ***line of sight (los)***.
- ***Microwave stations*** are earth-based stations that can transmit microwave signals directly to each other over distances of up to about 30 miles. To avoid buildings, mountains, and the curvature of the earth obstructing the signal, microwave stations are usually placed on tall buildings, towers, and mountaintops.
- Microwave stations typically contain both a dish-shaped microwave antenna and a transceiver. When one station receives a transmission from another, it amplifies it and passes it on to the next station. Microwave stations can exchange data transmissions with communications satellites, as well as with other microwave stations.

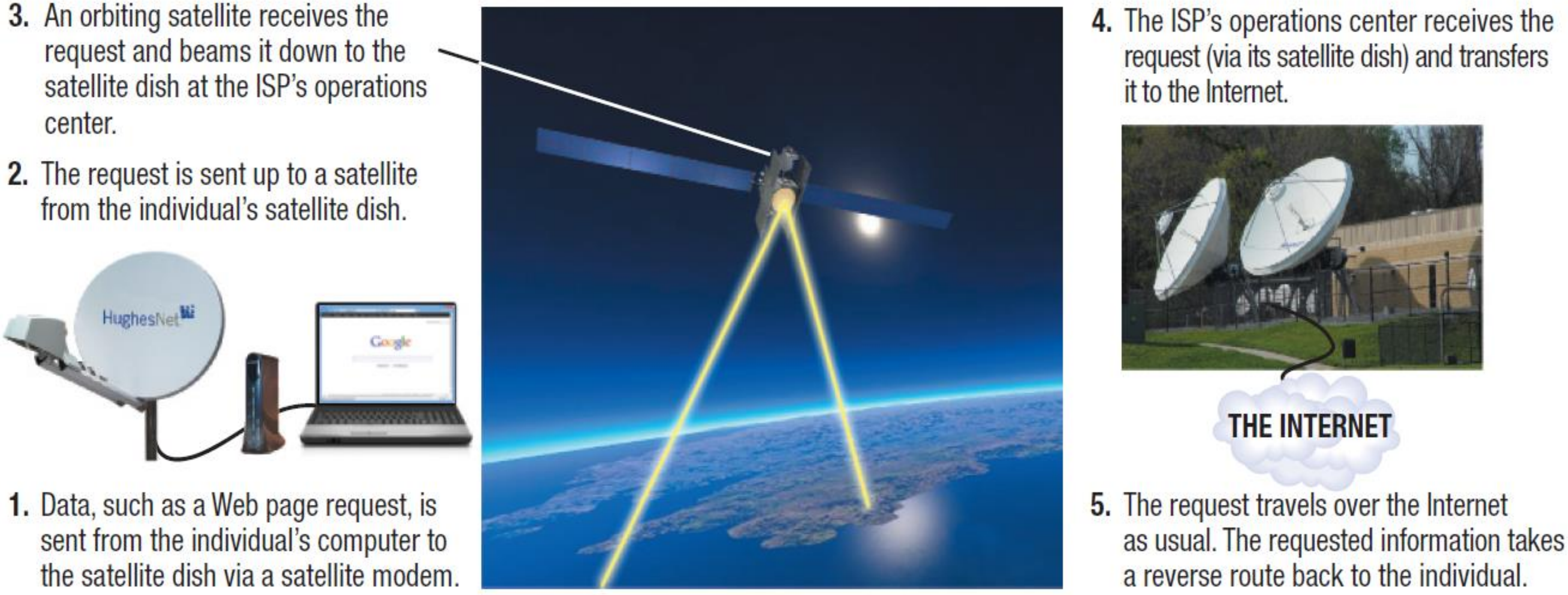
Unguided Media - Microwave and Satellite Transmissions (Contd.)

- ***Microwave stations*** designed specifically to communicate with satellites (such as those used to provide satellite TV and satellite Internet services) are typically called ***satellite dishes***.
- Satellite dishes are usually installed permanently where they are needed, but they can also be mounted on trucks, boats, RVs, and other types of transportation devices when portable transmission capabilities are necessary or desirable, such as when used for military or recreational applications.
- ***Communications satellites*** are space-based devices launched into orbit around the earth to receive and transmit microwave signals to and from earth.
- ***Communications satellites*** were originally used to facilitate microwave transmission when microwave stations were not economically viable (such as over large, sparsely populated areas) or were physically impractical (such as over large bodies of water) and were used primarily by the military and communications companies (such as for remote television news broadcasts).

Unguided Media - Microwave and Satellite Transmissions (Contd.)

- Today, ***communications satellites*** are used to send and receive transmissions to and from a variety of other devices, such as personal satellite dishes used for satellite television and Internet service, GPS receivers, satellite radio receivers, and satellite phones.
- They are also used for ***earth observation (EO)*** applications, including weather observation, mapping, and government surveillance.
- Traditional communications satellites maintain a ***geosynchronous orbit*** 22,300 miles above the earth and, because they travel at a speed and direction that keeps pace with the earth's rotation, they appear (from earth) to remain stationary over any given spot.
- This delay—less than one half-second—is not normally noticed by most users (such as individuals who receive Internet or TV service via satellite) but it does make geosynchronous satellite transmissions less practical for voice, gaming, and other real-time communications.

Fig: Microwave and Satellite Transmissions



1. Data, such as a Web page request, is sent from the individual's computer to the satellite dish via a satellite modem.

2. The request is sent up to a satellite from the individual's satellite dish.

3. An orbiting satellite receives the request and beams it down to the satellite dish at the ISP's operations center.

4. The ISP's operations center receives the request (via its satellite dish) and transfers it to the Internet.

5. The request travels over the Internet as usual. The requested information takes a reverse route back to the individual.

Unguided Media - Infrared (IR) Transmissions

- One type of wireless networking that does not use signals in the RF band of the electromagnetic spectrum is ***infrared (IR) transmission***, which sends data as infrared light rays over relatively short distances.
- Like an infrared television remote control, infrared technology requires line-of-sight transmission. Because of this limitation, many formerly infrared devices (such as wireless mice and keyboards) now use RF radio signals instead.
- Infrared transmissions are still used with remote controls (such as for computers that contain TV tuners).
- They are also used to beam data between some mobile devices, as well as between some game consoles, handheld gaming devices, and other home entertainment devices.

COMMUNICATIONS PROTOCOLS

Introduction

- A ***protocol*** is a set of rules to be followed in a specific situation; in networking, for instance, there are ***communications protocols*** that determine how devices on a network communicate.
- The term ***standard*** refers to a set of criteria or requirements that has been approved by a recognized standards organization (such as the ***American National Standards Institute (ANSI)***, which helps to develop standards used in business and industry, or ***IEEE***, which develops networking standards) or is accepted as a de facto standard by the industry.
- Standards are extremely important in the computer industry because they help hardware and software manufacturers ensure that the products they develop can work with other computing products.
- ***Networking standards*** typically address both how the devices in a network physically connect (such as the types of cabling that can be used) and how the devices communicate (such as the communications protocols that can be used).

OSI Reference Model

- The **OSI Model** (***Open Systems Interconnection Model***) is a conceptual framework used to describe the ***functions*** of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software.
- In the ***OSI reference model***, the communications between a computing system are split into seven different abstraction layers: ***Physical***, ***Data Link***, ***Network***, ***Transport***, ***Session***, ***Presentation***, and ***Application***.
- Created at a time when network computing was in its infancy, the OSI was published in 1984 by the International Organization for Standardization (ISO). Though it does not always map directly to specific systems, the OSI Model is still used today as a means to describe Network Architecture.

7 Layers of the OSI Model - Physical Layer

- The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured data bits across the network from the physical layer of the sending device to the physical layer of the receiving device.
- It can include specifications such as voltages, pin layout, cabling, and radio frequencies. At the physical layer, one might find “physical” resources such as network hubs, cabling, repeaters, network adapters or modems.
- This layer specifies the basic network hardware. Some of the characteristics defined in the specification are - interface between transmission media and device, encoding of bits, bit rate, error detection parameters, network topology, and the mode of transmission (duplex, half-duplex or simplex).
- Layer 1 is anything that carries 1’s and 0’s between two nodes.

7 Layers of the OSI Model - Data Link Layer

- At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer.
- The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols.
- It specifies the organization of data into frames, error detection in frames during transmission, and how to transmit frames over a network. Data Link layer is to deliver packets from one NIC to another.
- Layer 2 uses MAC addresses and is responsible for packet delivery from hop to hop.

7 Layers of the OSI Model - Network Layer

- The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol).
- At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.
- The network layer specifies the assignment of addresses (address structure, length of address etc.) to the packets and forwarding of packets to the destination i.e. ***routing***.
- Layer 3 uses IP addresses and is responsible for packet delivery from end to end.

7 Layers of the OSI Model - Transport Layer

- The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol.
- It specifies the details to handle reliable transfer of data. It handles end-to-end error control and flow control, breaking up data into frames and reassembling the frames.
- Layer 4 is responsible for service to service delivery.

7 Layers of the OSI Model - Session Layer

- The session layer controls the conversations between different computers.
- A session or connection between machines is set up, managed, and determined at layer 5.
- It includes specifications for password and authentication, and maintaining synchronization between the sender and the receiver.

7 Layers of the OSI Model - Presentation Layer

- This layer specifies the presentation and representation of data. Its functions include translation of the representation of the data into an identifiable format at the receiver end, encryption, and decryption of data etc.
- The presentation layer formats data for the application layer based on the syntax or semantics that the application accepts. Because of this, it at times also called the syntax layer.

7 Layers of the OSI Model - Application Layer

- At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser or Office 365. The application layer identifies communication partners, resource availability, and synchronizes communication.
- It contains the protocols used by users like HTTP, protocol for file transfer and electronic mail.

Fig: 7 Layers of the OSI Model

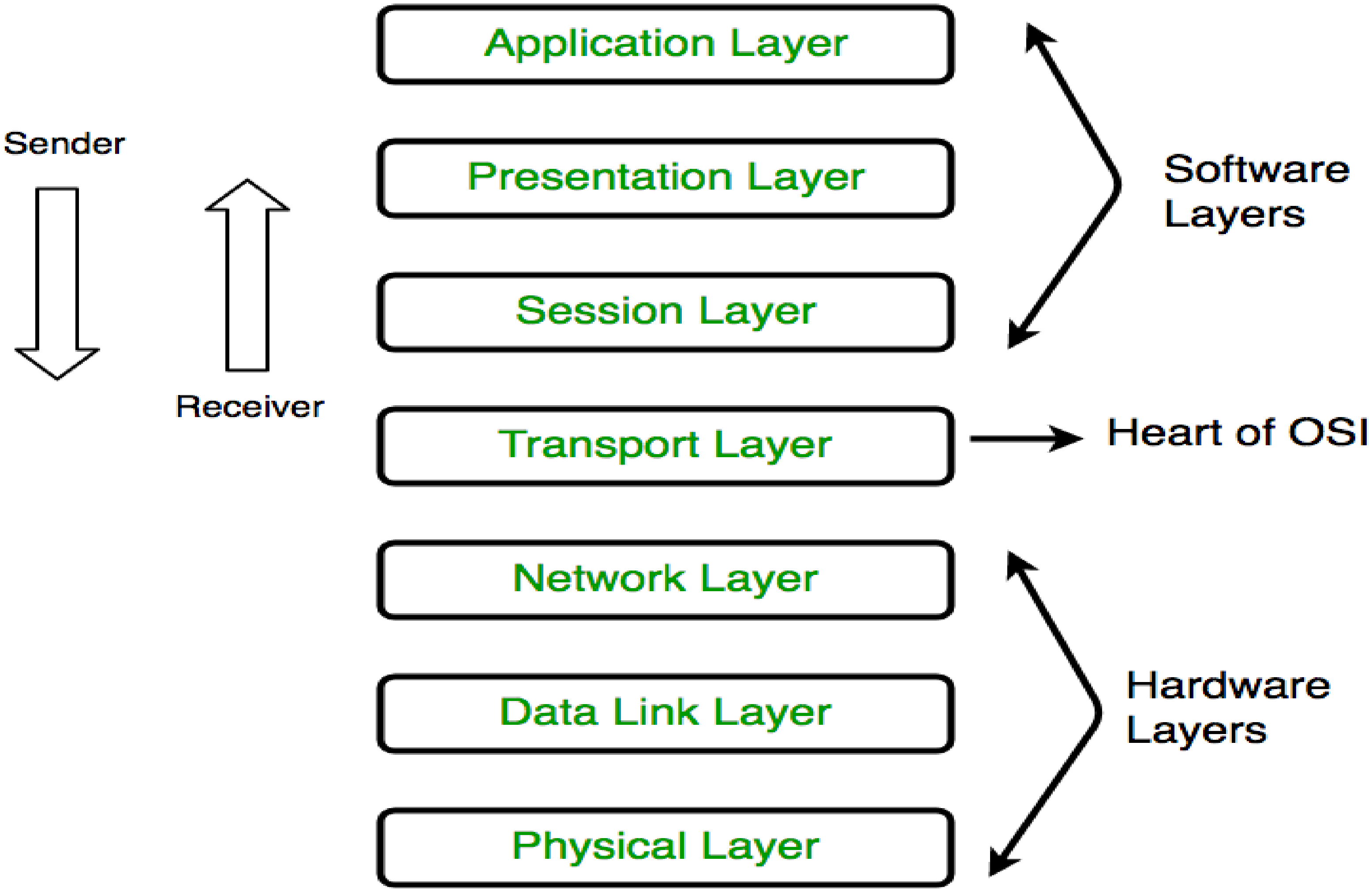


Fig: 7 Layers of the OSI Model

- Each layer at the sender’s side transforms the data according to the function it handles. For this it attaches headers to the data. At the receiver’s side, the corresponding layer applies the inverse of the transformation that has been applied at the source.

- As an example, if the Data link layer at the sender’s side adds an error detection code to the frame, then at the receiver’s side, the Data link layer verifies the error detection code and removes it from the frame before passing it to the next higher level, i.e. the Network layer.

Example: TCP/IP and Other Communications Protocols

- The most widely used communications protocol today is ***TCP/IP***. ***TCP/IP*** is the protocol used for transferring data over the Internet and actually consists of two protocols: ***Transmission Control Protocol*** (**TCP**), which is responsible for the delivery of data, and ***Internet Protocol*** (**IP**), which provides addresses and routing information.
- TCP/IP uses packet switching to transmit data over the Internet; when the packets reach their destination, they are reassembled in the proper order.
- Support for TCP/IP is built into operating systems, and IP addresses are commonly used to identify the various devices on computer networks.
- The first widely used version of IP was ***Internet Protocol Version 4*** (**IPv4**), which was standardized in the early 1980s. IPv4 uses ***32-bit addresses*** and so allows for 2^{32} (***4.3 billion***) possible unique addresses. While still in use today, ***IPv4*** was never designed to be used with the vast number of devices that access the Internet today and ***IPv4 addresses*** are ***running out***.

Example: TCP/IP and Other Communications Protocols (Contd.)

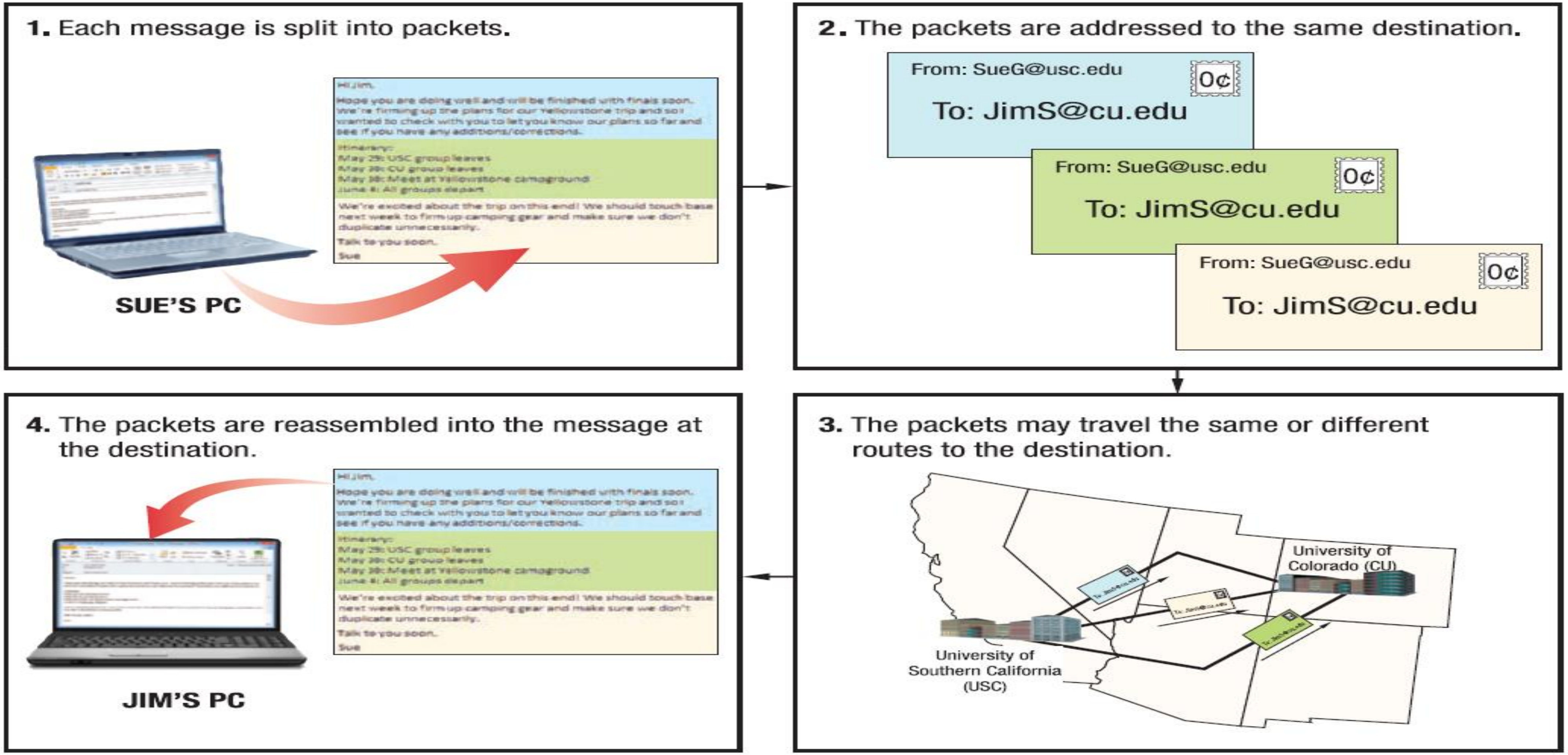
- Consequently, a newer version of IP (**IPv6**) was developed and is in the process of being implemented. IPv6 uses ***128-bit addresses*** (and so allows for 2^{128} possible unique addresses).
- It provides enough addresses so that all devices can have their own direct public IP address.
- Using ***IPv6 addressing***, your devices can be accessible on the Internet directly via their own IP address, instead of all the devices in your home being identified by your router's IP address (which requires the router to relay the appropriate traffic to and from each device).
- The use of IPv6 addressing will make applications such as home automation and gaming easier to implement. It is expected that external systems (such as company Web sites) will switch over to IPv6 first and that IPv4 and IPv6 will coexist for several years.

Example: TCP/IP and Other Communications Protocols (Contd.)

- However, in some countries (such as China) where IPv4 address are scarce, end users are expected to switch over faster. In the United States, the government has mandated that all federal agencies be capable of switching to IPv6 and to purchase only IPv6-compatible new hardware and software.
- Experts suggest that businesses perform a network audit to determine what hardware and software changes will be needed to switch to IPv6 so that the business is prepared when the change is necessary.
- While TCP/IP is used to connect to and communicate with the Internet, other protocols are used for specific Internet applications.
- For instance, **HTTP** (***Hypertext Transfer Protocol***) and **HTTPS** (***Secure Hypertext Transfer Protocol***) are protocols used to display Web pages, and **FTP** (***File Transfer Protocol***) is a protocol used to transfer files over the Internet. Protocols used to deliver e-mail over the Internet include **SMTP** (***Simple Mail Transfer Protocol***) and **POP3** (***Post Office Protocol***).

Fig: How TCP/IP works

- TCP/IP networks (like the Internet) use packet switching.



1. Each message is split into packets.

Hi Jim,

Hope you are doing well and will be finished with finals soon. We're firming up the plans for our Yellowstone trip and so I wanted to check with you to let you know our plans so far and see if you have any additions/corrections.

Itinerary:
May 29: USC group leaves
May 29: CU group leaves
May 30: Meet at Yellowstone campground
June 4: All groups depart

We're excited about the trip on this end! We should touch base next week to firm up camping gear and make sure we don't duplicate unnecessarily.

Talk to you soon.

Sue

2. The packets are addressed to the same destination.

From: SueG@usc.edu
To: JimS@cu.edu

From: SueG@usc.edu
To: JimS@cu.edu

From: SueG@usc.edu
To: JimS@cu.edu

3. The packets may travel the same or different routes to the destination.

4. The packets are reassembled into the message at the destination.

Hi Jim,

Hope you are doing well and will be finished with finals soon. We're firming up the plans for our Yellowstone trip and so I wanted to check with you to let you know our plans so far and see if you have any additions/corrections.

Itinerary:
May 29: USC group leaves
May 29: CU group leaves
May 30: Meet at Yellowstone campground
June 4: All groups depart

We're excited about the trip on this end! We should touch base next week to firm up camping gear and make sure we don't duplicate unnecessarily.

Talk to you soon.

Sue

SUE'S PC
0¢
0¢
0¢
University of Colorado (CU)
University of Southern California (USC)
JIM'S PC

NETWORKING HARDWARE/DEVICES

Introduction

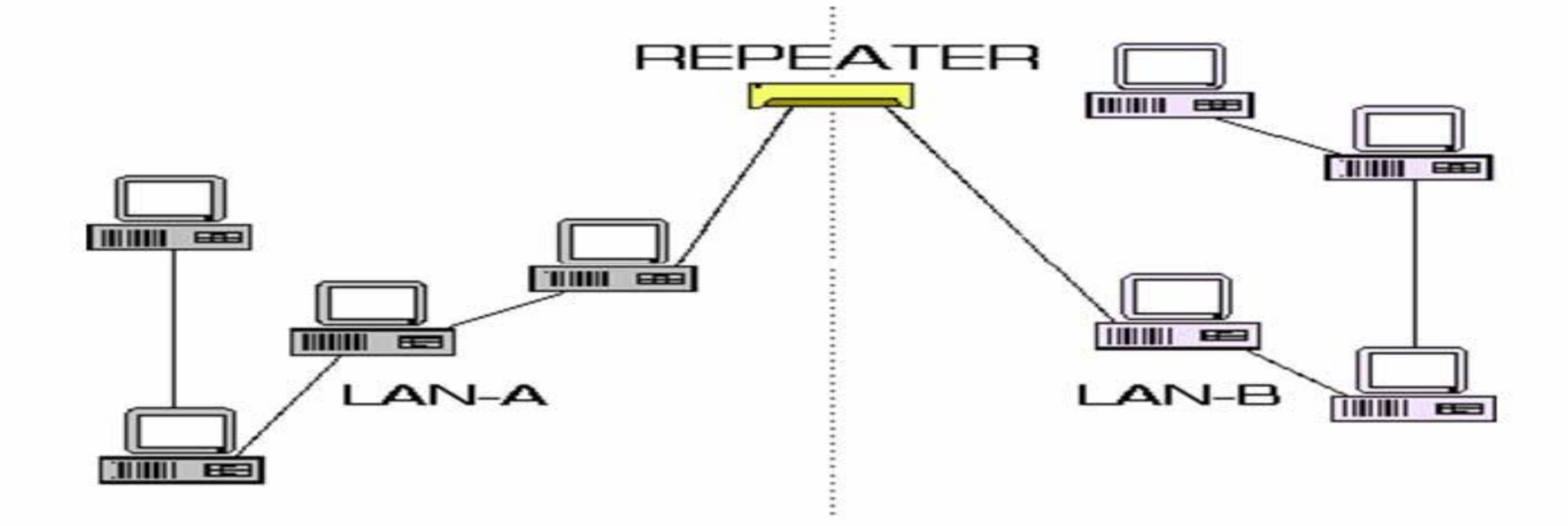
- Various types of hardware are necessary to create a computer network, to connect multiple networks together, or to connect a computer or network to the Internet.
- The most common types of networking hardware used in home and small office networks are:
    - Network Interface Card (NIC)
    - Repeater
    - Bridge
    - Hub
    - Switch
    - Router
    - Gateway

Network Interface Card (NIC)

- A ***Network Interface Card*** (**NIC**) is a hardware device through which the computer connects to a network. It works at both the data link layer and physical layer of the OSI reference model.
- At the data link layer, NIC converts the data packets into data frames, adds the ***Media Access address*** (**MAC address**) to data frames.
- At the physical layer, it converts the data into signals and transmits it across the communication medium.

Repeater

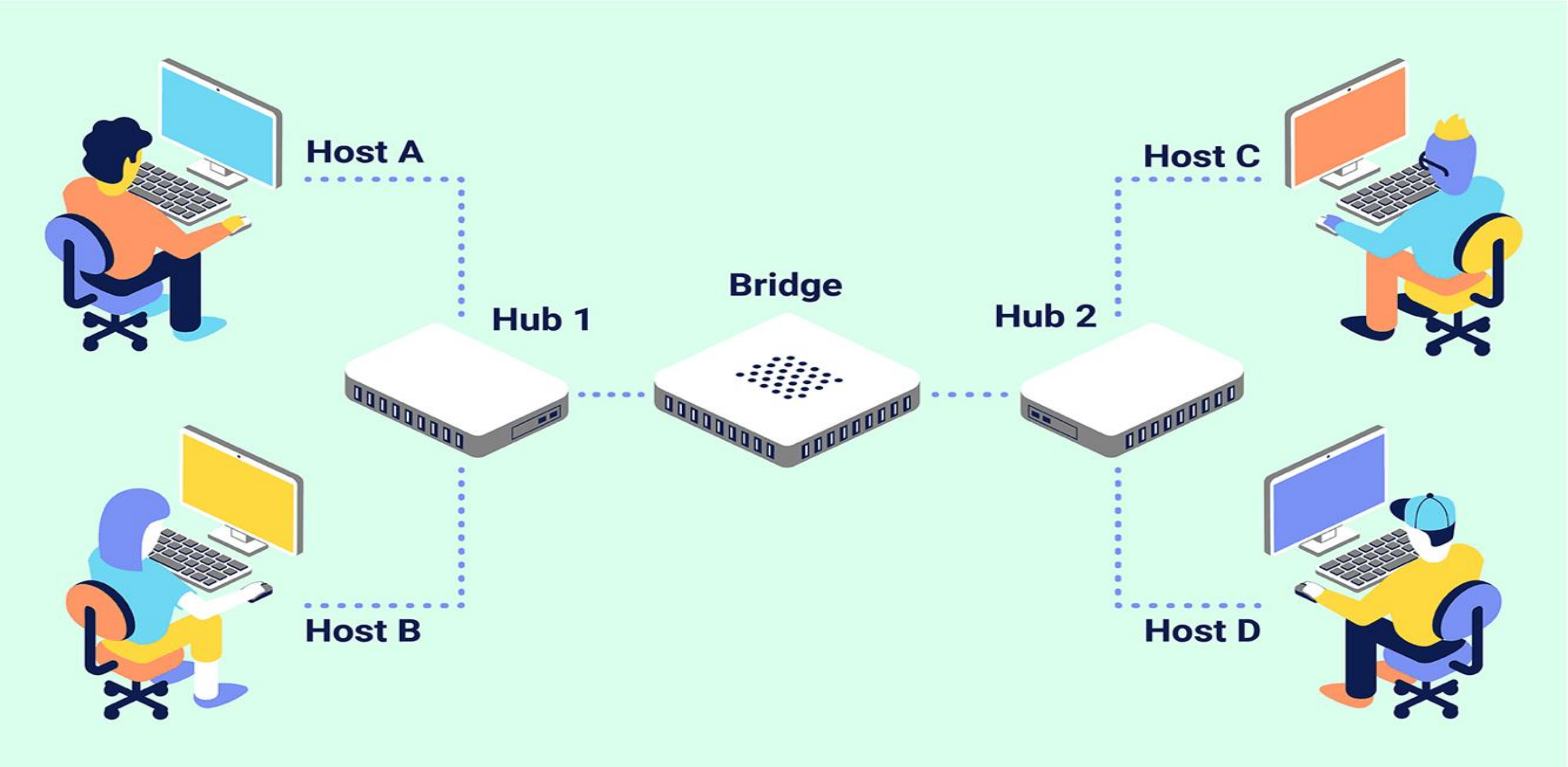
- ***Repeaters*** are used to extend LAN. It has only two ports and can connect only two segments of the network. It retimes and regenerates the signals to proper amplitudes and sends them to the other segments. Also, it cannot connect dissimilar network.
- The repeater then sends the refreshed signal. It can extend the physical length of a LAN.
- ***Repeaters*** require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row. Repeaters work only at the physical layer of the OSI network model.



Bridge

- ***Bridge*** is used to connect two LAN segments like a repeater; it forwards complete and correct frames to the other segment. It works in both the physical and the data link layer.
- As a physical layer device, it regenerates the signal it receives. As a data link layer device, the bridge can check the physical (MAC) address contained in the frame. A bridge has a filtering capabilities i.e. it can check the destination address of a frame and decide if the frame should be forwarded or dropped.
- A bridge reads the outermost section of data on the data packet, to tell where the message is going. It reduces the traffic on other network segments, since it does not send all packets.
- ***Bridges*** can be programmed to reject packets from particular networks. Bridges forward all broadcast messages.
- Bridges do not normally allow connection of networks with different architectures.
- Only a special bridge called a ***translation bridge*** will allow two networks of different architectures to be connected.

Fig: Bridge



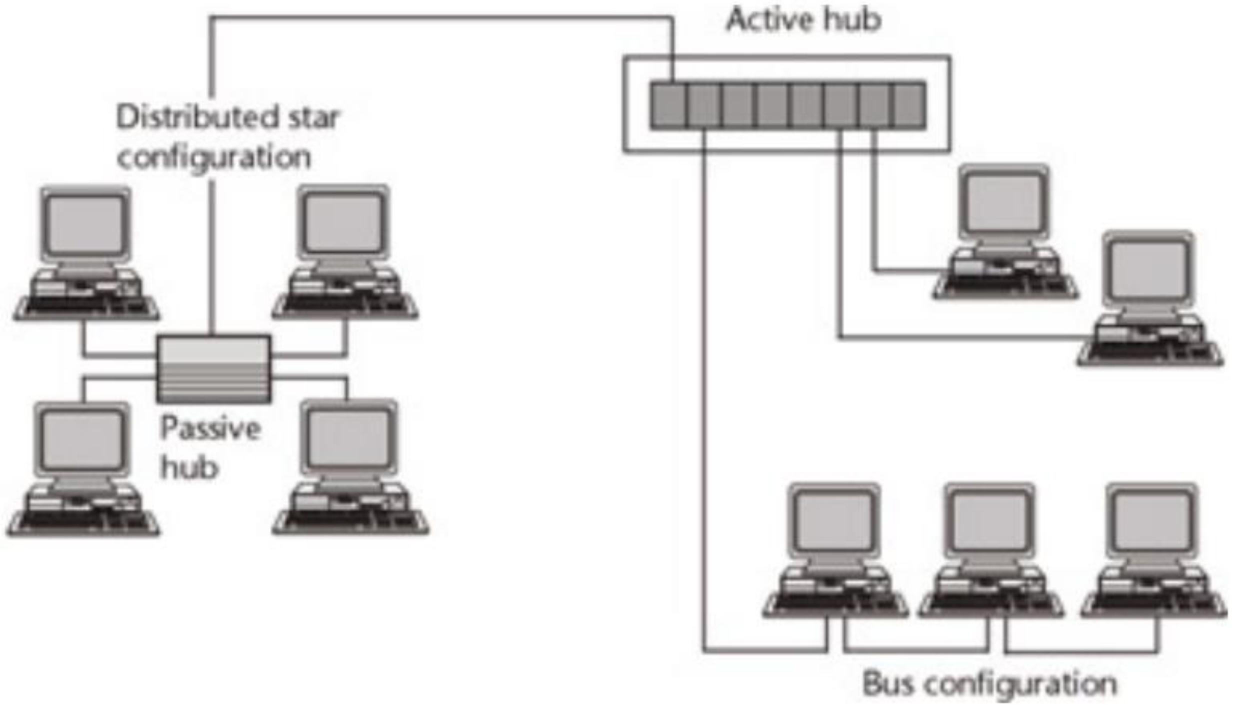
Hub

- It is a device that centrally connects devices in a computer network.
- There are **three types of a hub*:***
  - ***Active hubs*** amplify and regenerate the incoming electrical signals before broadcasting them. They have their own power supply and serves both as a repeater as well as connecting center. Due to their regenerating capabilities, they can extend the maximum distance between nodes, thus increasing the size of LAN.
  - ***Passive hubs*** connects nodes in a star configuration by collecting wiring from nodes. They broadcast signals onto the network without amplifying or regenerating them. As they cannot extend the distance between nodes, they limit the size of the LAN.
  - ***Intelligent hubs*** are active hubs that provide additional network management facilities. They can perform a variety of functions of more intelligent network devices like network management, switching, providing flexible data rates etc.

Hub (Contd.)

- Every computer is directly connected with the hub. When data packets arrives at hub, it broadcast them to all the LAN cards in a network and the destined recipient picks them and all other computers discard the data packets.
- Hub has four, eight, sixteen and more ports and one port is known as ***uplink port***, which is used to connect with the next hub.
- Hubs work at the physical layer of the OSI (Open System Interconnection) model.
- The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

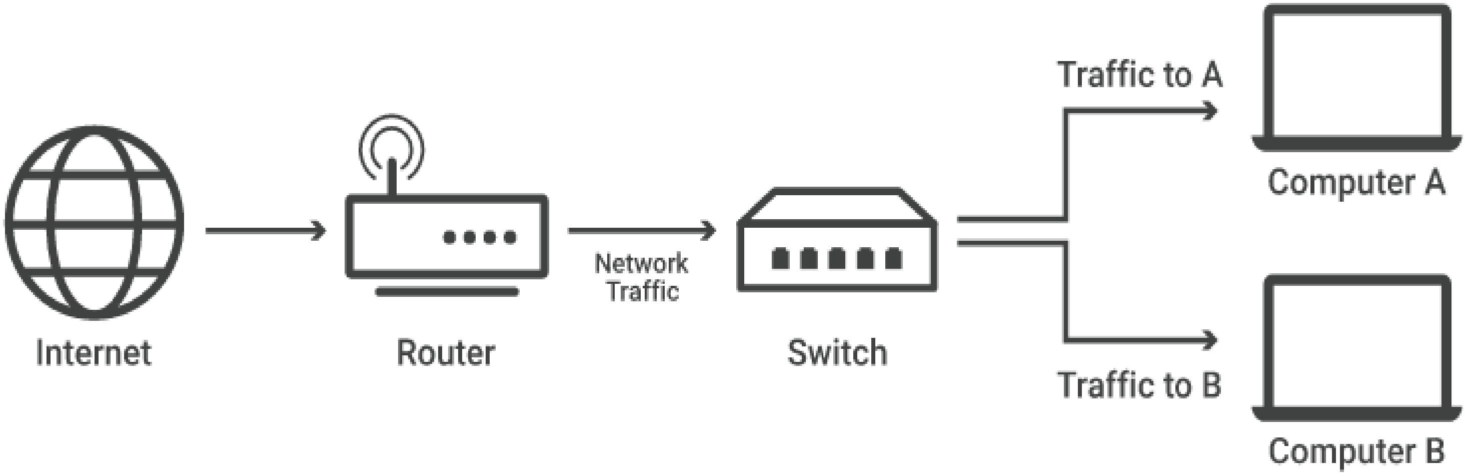
Fig: Hub


Active hub
Distributed star configuration
Passive hub
Bus configuration

Switch

- Like hub, ***switch*** also connects multiple computers in a network or different segments of the same network.
- ***Switches*** work at the Data Link Layer of the OSI reference model. Hence, switches consider data as frames and not as signals. Unlike the hubs, a switch does not broadcast the data to all the computers; it sends the data packets only to the destined computer.
- A ***switch*** receives a signal as a data frame from a source computer on a port, checks the MAC address of the frame, forwards the frame to the port connected to the destination computer having the same MAC addresses.

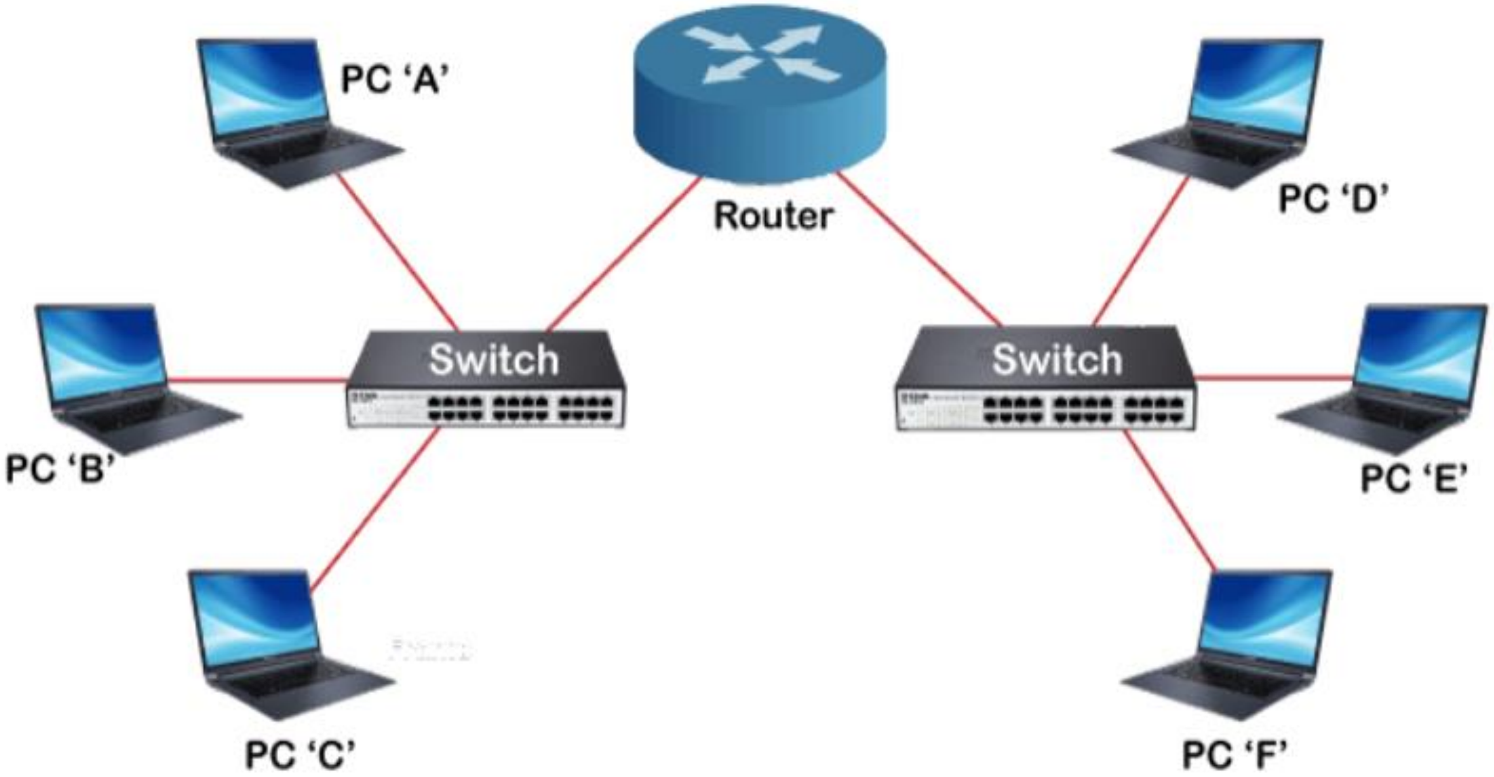
Fig: Switch


Internet
Router
Network Traffic
Switch
Traffic to A
Computer A
Traffic to B
Computer B

Router

- A ***router*** is a communication device that is used to connect two logically and physically different networks, two LANs, two WANs and a LAN with WAN.
- The main function of the router is to sorting and the distribution (i.e. ***routing***) of the data packets to their destinations based on their IP addresses.
- Routers provides the connectivity between the enterprise businesses, ISPs and in the internet infrastructure, router is a main device. Every router has routing software, which is known as **I**nternetwork **O**perating **S**ystem (**IOS**).
- Router operates at the network layer of the OSI model. Router does not forward broadcast the data packets. Routers connect two or more logical subnets, each having a different network address.
- A router determines which way is the shortest or fastest in a network, and routes packets accordingly based on the IP addresses.

Fig: Router

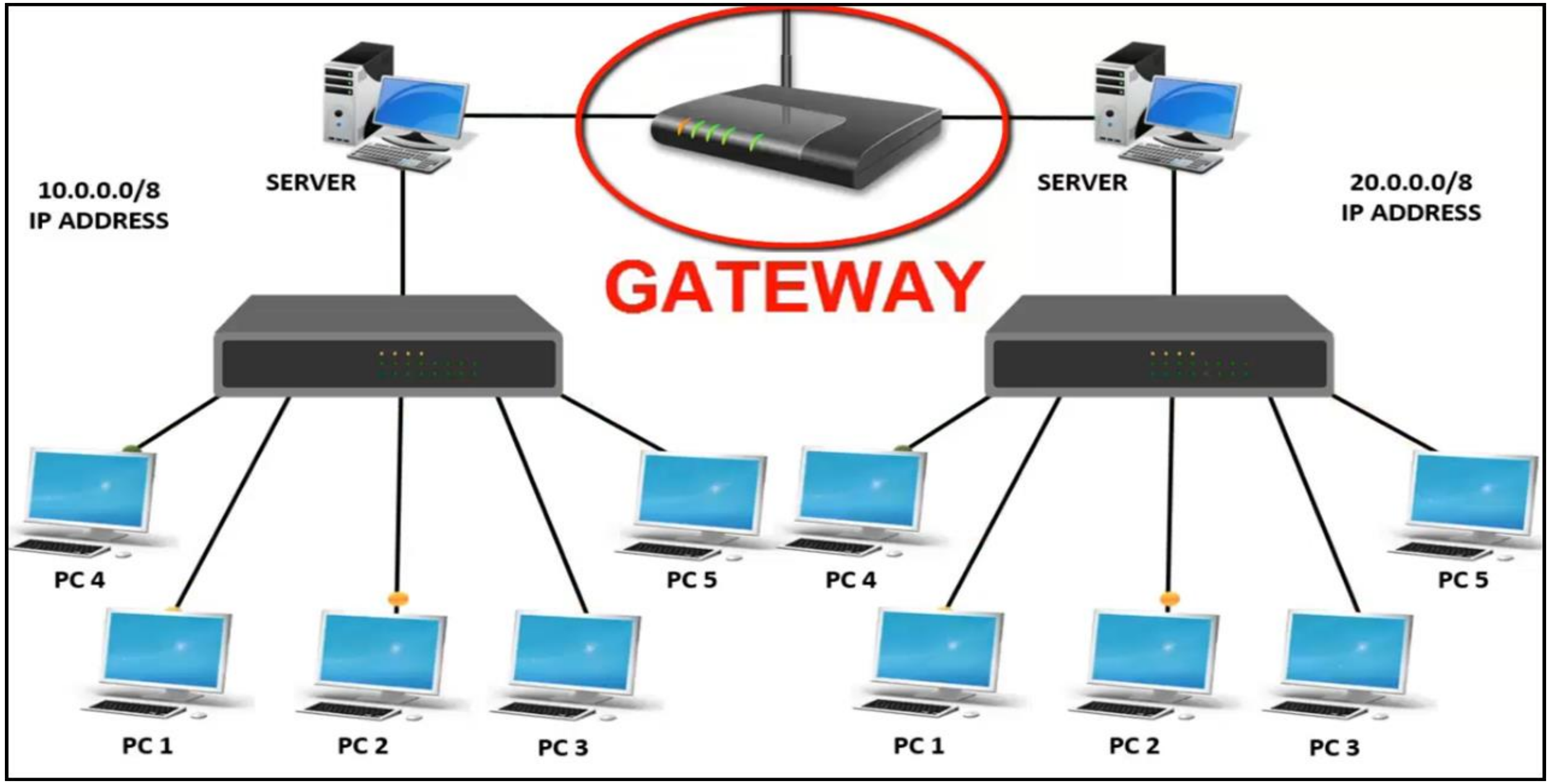


Connection of networks through Router

Gateway

- ***Gateway*** is a generic term used to represent devices that connect two dissimilar networks. A gateway at the transport layer converts protocols among communications networks.
- It can accept a packet formatted for one protocol and convert it to a packet formatted for another protocol. An application gateway can translate messages from one format to the other.
- A ***gateway*** can be implemented in hardware, software, or in both hardware and software. Generally, gateway is implemented by software installed within a router.

Fig: Gateway


GATEWAY
SERVER
10.0.0.0/8
IP ADDRESS
SERVER
20.0.0.0/8
IP ADDRESS
PC 4
PC 5
PC 1
PC 2
PC 3
PC 4
PC 5
PC 1
PC 2
PC 3

WIRELESS NETWORKING

Introduction

- ***Wireless technology***, as the name suggests, is used to establish a wire-free connection or communication between two or more devices. In contrast, to the wired technology where data is encoded as electric current and signals travel through wires, in wireless technology data is encoded on electromagnetic waves that travel through air.

- The ***wireless technology*** is used for broadcasting in radio and television communication, for communication using mobile phones and pagers, for connecting components of computers using Bluetooth technology, for Internet connection using Wi-Fi, Wireless LAN, PDA, and in remote controls for television, doors etc.

Benefits of wireless network

- Businesses can experience many benefits from a wireless network, this includes:
  - **Convenience:**

    Access your network resources from any location within your wireless network’s coverage area or from any Wi-Fi hotspot.
  - **Mobility:**

    We are no longer tied to our desk, as we were with a wired connection. You and your employees can go online in conference room meetings.
  - **Productivity:**

    Wireless access to the internet and to your company’s key applications and resources helps your staff get the job done and encourages collaboration.
  - **Easy Setup:**

    You don’t have to string cables, so installation can be quick and cost-effective.
  - **Expandable:**

    You can easily expand wireless network with existing equipment, while a wired network might require additional wiring.
  - **Security:**

    Advances in wireless networks provide robust security protections.
  - **Cost:**

    Because wireless networks eliminate or reduce wiring costs, they can cost less to operate than wired networks.

Types of wireless network

- **Bluetooth Technology:**

  The different components of the computer like the keyboard, printer, monitor etc., are connected to the computer case via wires. ***Bluetooth technology*** is used to connect the different components wirelessly. A printer placed in a room may be connected to a computer placed in a different room using Bluetooth technology. Using ***Bluetooth*** does away with the wires required to connect the components to the computer and allows portability of components within a small area lying within the Bluetooth range.

- **Wireless LAN:**
  - ***Wireless LAN*** has some benefits over the wired LANs. In wireless LANs, there is flexibility to move the computers and devices within the network. It can connect computers where cabling is not possible. It is easy to expand by using an access point. Since, no physical medium is physical medium is required, Wireless LANs are easy to install.
  - In ***wireless LAN***, data is transmitted using radio or infrared waves, there is no attenuation or distortion of the signal due to electromagnetic interference. Wireless LANs are used at home to connect devices on different floors or to set up a home network, to provide connectivity in public places like airports, railway stations, college campus, and hotels etc., where travelling users can access the network. Wireless LANs can also be connected to a WAN thus providing access to Internet to the user. ***IEEE 802.11*** is a standard for wireless LAN.

Types of wireless network (Contd.)

- **Wireless WAN:**
  - The radio network used for cellular telephone is an example of wireless WAN. ***Wireless WANs*** allow the users to access the Internet via their mobile devices. This provides flexibility to the user access the Internet from any location where wireless connectivity exists.
  - Almost all wireless networks are connected to the wired network at the back-end to provide access to Internet. Wireless networks also offer many challenges, like, the compatibility among different standards promoted by different companies, congested networks in case of low bandwidth, the high infrastructure and service cost, data security, battery storage capability of wireless device, and health risk.

THANK YOU!