1. NETWORK HARDWARE

Network hardware has 2 main dimensions : Transmission technology

Scale

Transmission Technology

- In transmission technology there are 2 types. **broadcast** links and **point-to-point** links.
- Point-to-point links connect individual pairs of machines. To go from the source to the destination on a network made up of point-to-point links, short messages, called **packets** is used.
- Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called **unicasting**.
- On a broadcast network, the communication channel is shared by all the machines on the network; packets sent by any machine are received by all the others. An address field within each packet specifies the intended recipient. Upon receiving a packet, a machine checks the address field. If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.
- A wireless network is a common example of a broadcast link, with communication shared over a coverage regionthat depends on the wireless channel and the transmitting machine.
- Broadcast systems usually also allow the possibility of addressing a packet to *all* destinations by using a special code in the address field. When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called **broadcasting**. Some broadcast systems also support transmission to a subset of the machines, which known as **multicasting**.

Scale:

Distance is important as a classification metric because different technologies are used at different scales.

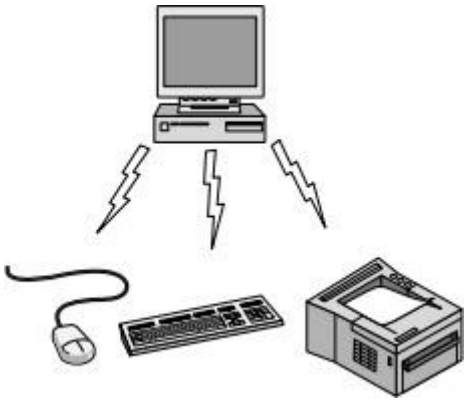
Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

At the top are the personal area networks, networks that are meant for one person. Beyond these come longer-range networks. These can be divided into local, metropolitan, and wide area networks, each with increasing scale.

1.1 Personal Area Networks:

PANs (**Personal Area Networks**) let devices communicate over the range of a person.

- A common example is a wireless network that connects a computer with its peripherals. In the simplest form, Bluetooth networks use the master-slave paradigm.



- The system unit (the PC) is normally the master, talking to the mouse, keyboard, etc., as slaves. The master tells the slaves what addresses to use, when they can broadcast, how long they can transmit, what frequencies they can use, and so on. Bluetooth can be used in other settings, too.
- It is often used to connect a headset to a mobile phone without cords and it can allow your digital music player to connect to your car merely being brought within range.
- A completely different kind of PAN is formed when an embedded medical device such as a pacemaker, PANs can also be built with other technologies that communicate over short ranges, such as RFID on smartcards insulin pump, or hearing aid talks to a user-operated remote control.

1.2 Local Area Network

- A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory. LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information. When LANs are used by companies, they are called **enterprise networks**.
- Each computer talks to a device in the ceiling through a device called AP(Access Point) or base station relays packets between the wireless computers and also between them and the Internet. There is a standard for wireless LANs called **IEEE 802.11**, popularly known as **WiFi**, which has become very widespread. It runs at speeds anywhere from 11 to hundreds of Mbps.

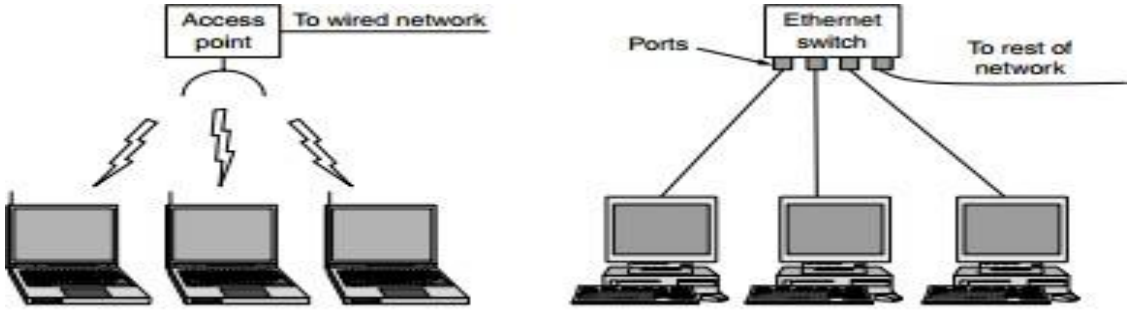


Figure 1-8. Wireless and wired LANs. (a) 802.11. (b) Switched Ethernet.

- Wired LANs use a range of different transmission technologies. Most of them use copper wires, but some use optical fiber. LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance. The most commonly used wired LANs is IEEE802.3, called as **Ethernet.**

Switched Ethernet

- Each computer speaks the Ethernet protocol and connects to a box called a **switch** with a point-to-point link. A switch has multiple **ports**, each of which can connect to one computer.
- The job of the switch is to relay packets between computers that are attached to it, using the address in each packet to determine which computer to send it to.
- To build larger LANs, switches can be plugged into each other using their ports. It is also possible to divide one large physical LAN into two smaller logical LANs.
- Depending on the how the channel is allocated, it is divided into static and dynamic designs.
  - ❖ **Static allocation:** A typical static allocation would be to divide time into discrete intervals and use a round-robinalgorithm, allowing each machine to broadcast only when its time slot comes up.
  - ❖ **Dynamic allocation:** Dynamic allocation can be done by either centralized or decentralized.

    Centralized channel: There is a single entity, for example, the base station in cellular

    networks.
- Decentralized channel: There is no central entity; each machine must decide for itself whether to transmit.
- Many devices are already capable of being **networked**. These include computers, entertainment devices such as TVs and DVDs, phones and other consumer electronics such as cameras, appliances like clock radios, and infrastructure like utility meters and thermostats.

Home Network:

- Home networks can be just as another LAN
  - ❖ First, the networked devices have to be very easy to install. Wireless routers are the most returned consumerelectronic item.
  - ❖ Second, the network and devices have to be foolproof in operation.

- ❖ Third, low price is essential for success.
- ❖ Fourth, it must be possible to start out with one or two devices and expand the reach of the network gradually.
- ❖ Fifth, security and reliability will be very important

- According to the convenience and cost favours, the home networks can be wired or wireless. Security favours thewired networking.
- **Power-line networks** let devices that plug into outlets broadcast information throughout the house.

1.3 Metropolitan Area Networks:

- A **MAN** (**Metropolitan Area Network**) covers a city. The best-known examples of MANs are the cabletelevision networks available in many cities.
- Initially these were designed locally, and then companies started to expand to wire up the entire cities. The nextstep was television programming and even entire channels designed for cable only.
- When the Internet began attracting a mass audience, the cable TV network operators began to realize that withsome changes to the system, they could provide two-way Internet service in unused parts of the spectrum.

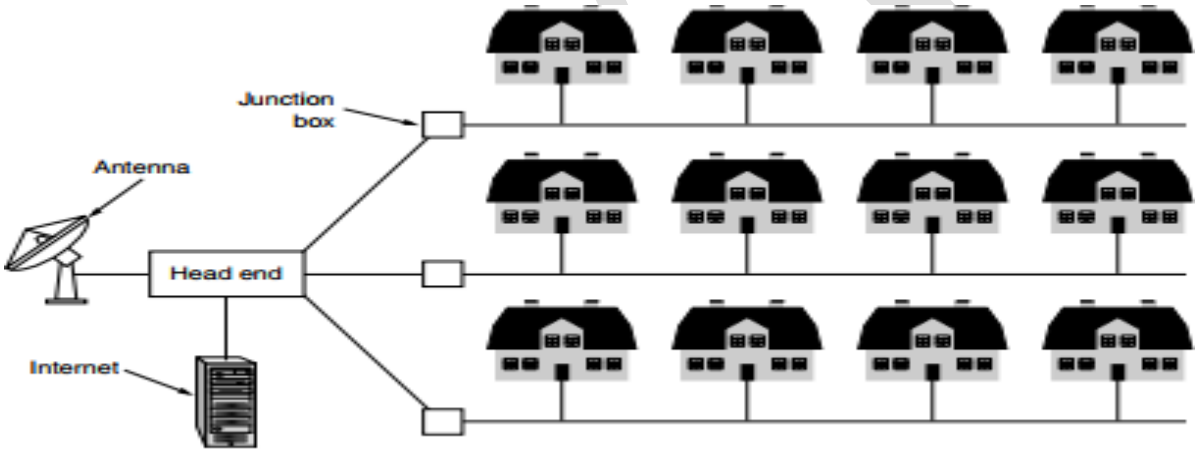
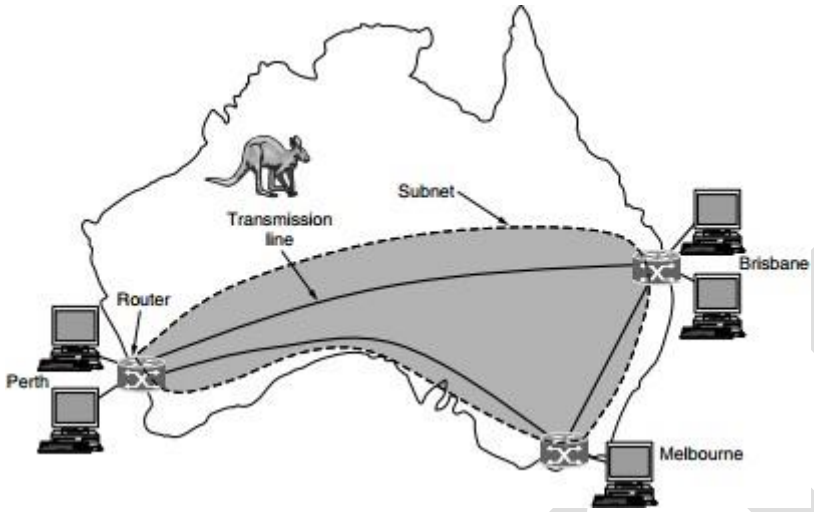


Figure 1-9. A metropolitan area network based on cable TV.

- Both the television signals and Internet is being fed into the centralized **cable headend** for subsequentdistribution to people's homes.
- Recent developments in high speed wireless Internet access have resulted in another MAN, which has beenstandardized as IEEE 802.16 and is popularly known as **WiMAX**.

1.4 Wide Area Networks

A **WAN** (**Wide Area Network**) spans a large geographical area, often a country or continent.



The fig shows the network that connects offices in Perth, Melbourne and Brisbane. Each offices contain the computers and these are called machine **hosts** in the traditional usage. The rest of the network that connects these hosts is then called the **communication subnet**, or just **subnet.** The job of the subnet is to carry messages from host to host.

- The subnet consists of two distinct components: transmission lines and switching elements.
  - ❖ **Transmission lines** move bits between machines.They can be made of copper wire, optical fiber, or even radio links.
  - ❖ **Switching elements**, or just **switches**, are specialized computers that connect two or more transmission lines.When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them. These switching computers have been called by various names in the past; the name **router** is now most commonly used.
- The two varieties of WAN

i) WAN using a VPN(virtual private network)
ii) WAN using ISP network

- ❖ **WAN using a VPN(virtual private network)**

  A company might connect its offices to the Internet This allows connections to be made between the offices as virtual links that use the underlying capacity of the Internet. This is called VPN.

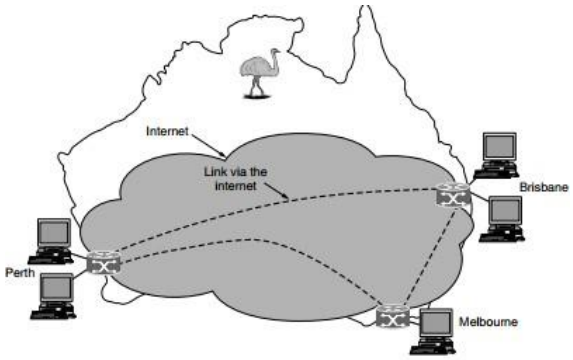


Figure 1-11. WAN using a virtual private network.

Compared to the dedicated arrangement, a VPN has the usual advantage of virtualization, which is that it provides flexible reuse of a resource.

❖ **WAN using ISP network**

The subnet operator is known as a **network service provider** and the offices are its customers.. The subnet operator will connect to other customers too, as long as they can pay and it can provide service. Such a subnet operator is called an **ISP** (**Internet Service Provider**) and the subnet is an **ISP network.**

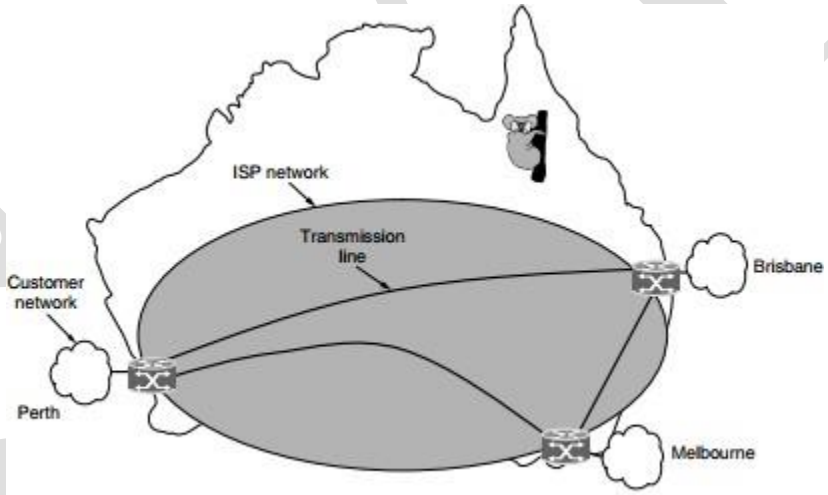


Figure 1-12. WAN using an ISP network.

- In most WANs, the network contains many transmission lines, each connecting a pair of routers. If two routers that do not share a transmission line wish to communicate, they must do this indirectly, via other routers. The network makes the decision as to which path to use is called the **routing algorithm**. Each router makes the decision as to where to send a packet next is called the **forwarding algorithm**.

Satellite System

- It is one of wireless WAN technologies. Each computer on the ground has an antenna through which it can send data to and receive data from to a satellite in orbit. All computers can hear the output *from* the

satellite, and in some cases they can also hear the upward transmissions of their fellow computers *to* the satellite as well. Satellite networks are inherently broadcast and are most useful when the broadcast property is important.

Cellular Telephone Network

- Another example of a WAN that uses wireless technology. There are so many generations in the cellular telephonenetwork.
- The first generation was analog and for voice only. The second generation was digital and for voice only. The third generation is digital and is for both voice and data. Each cellular base station covers a distance much larger than a wireless LAN, with a range measured in kilometers rather than tens of meters.
- The base stations are connected to each other by a backbone network that is usually wired. The data rates of cellular networks are often on the order of 1 Mbps, much smaller than a wireless LAN that can range up to on the order of 100 Mbps.

1.5 Internetworks:

- A collection of interconnected networks is called an **internetwork** or **internet.** The Internet uses ISP networks to connect enterprise networks, home networks, and many other networks.
- The term ‘‘subnet’’ refers to the collection of routers and communication lines owned by the network operator. A network is formed by the combination of a subnet and its hosts. Connecting a LAN and a WAN or connecting two LANs is the usual way to form an internetwork.
- The general name for a machine that makes a connection between two or more networks and provides the necessary translation, both in terms of hardware and software, is a **gateway.** Gateways are distinguished by the layer at which they operate in the protocol hierarchy.

1.2 NETWORK SOFTWARE

1.2.1 Protocol hierarchies

- To reduce the design complexity, most networks are organized as a stack of **layers** or **levels**, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
- The purpose of each layer is to offer certain services to the higher layers while shielding those layers from the details of how the offered services are actually implemented.
- A **protocol** is an agreement between the communicating parties on how communication is to proceed.

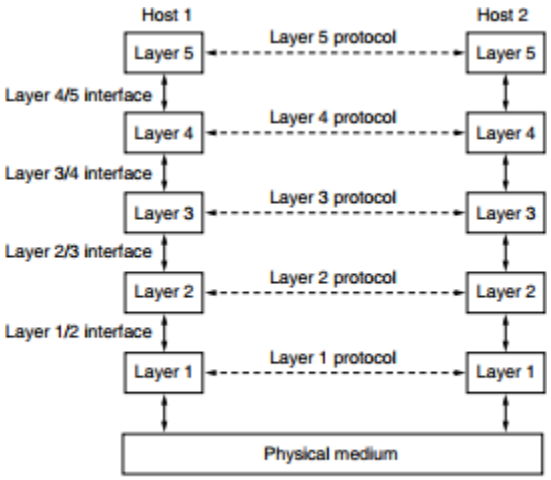
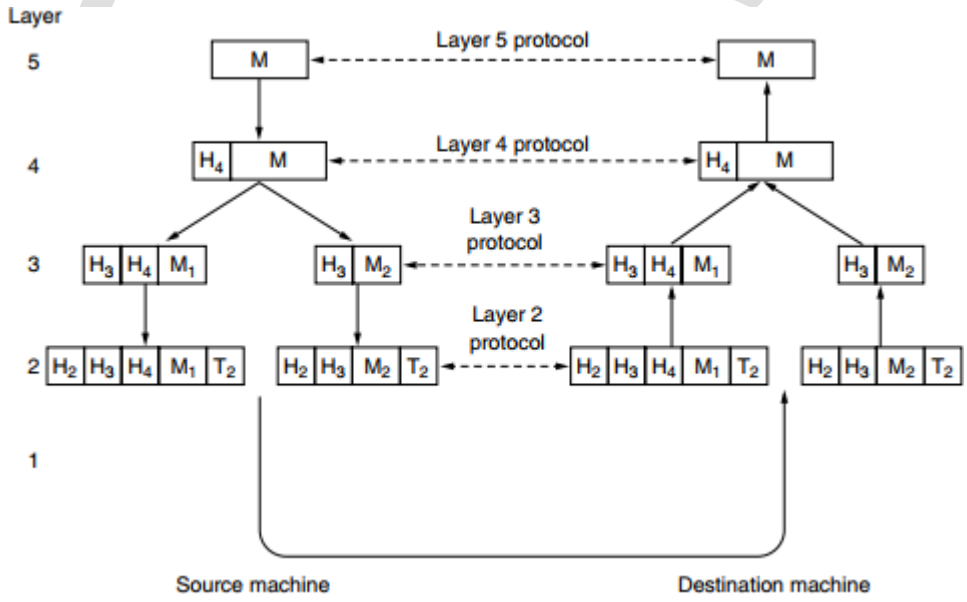


Figure 1-13. Layers, protocols, and interfaces.

- The entities comprising the corresponding layers on different machines are called **peers**. The peers may be software processes, hardware devices, or even human beings. No data are directly transferred from layer *n* on one machine to layer *n* on another machine. It is transferred through the physical medium(actual communication occurs). Virtual communication is shown by dotted lines and physical communication by solid lines.
- Between each pair of adjacent layers is an **interface**. The interface defines which primitive operations and services the lower layer makes available to the upper one.
- A set of layers and protocols is called a **network architecture**. The specification of an architecture must contain enough information to allow an implementer to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol. A list of the protocols used by a certain system, one protocol per layer, is called a **protocol stack.**



- The above diagram is the example of providing communication to the top layer of 5 layer network.
- A message, *M*, is produced by an application process running in layer 5 and given to layer 4 for transmission.
- Layer 4 puts a **header** in front of the message to identify the message and passes the result to layer 3. The header includes control information, such as addresses, to allow layer 4 on the destination machine to deliver the message.
- Layer 3 decides which of the outgoing lines to use and passes the packets to layer 2. Layer 2 adds to each piece not only a header but also a trailer, and gives the resulting unit to layer 1 for physical transmission.
- At the receiving machine the message moves upward, from layer to layer, with headers being stripped off as it progresses.

1.2.2 Design Issues For the Layers

Some of the design issues are

i) Reliability ii) Evolution of the network iii) Resource Allocation iv) Security

- **Reliability**
  - ❖ One mechanism for finding errors in received information uses codes for **error detection**. Information that is incorrectly received can then be retransmitted until it is received correctly. **error correction**, where the correct message is recovered from the possibly incorrect bits that were originally received.
  - ❖ Another reliability issue is finding a working path through a network. The process of selecting a path for traffic in a network or between or across multiple networks is called **routing.**
- **Evolution of network**
  - ❖ Since the networks grow larger and new designs emerge in the existing networks, key structuring mechanism used to support the change by dividing the overall problem called, **protocol layering** is implemented**.**
  - ❖ Every layer needs a mechanism for identifying the senders and receivers that are involved in a particular message. This mechanism is called **addressing** or **naming**, in the low and high layers, respectively.
  - ❖ The mechanism which involves in doing disassembling, transmitting, and then reassembling messages in overall network is called **Internetwork.** Designs that continue to work well when the network gets large are said to be **scalable**.
- **Resource Allocation**
  - ❖ Networks provide a service to hosts from their underlying resources, such as the capacity of transmission lines(bandwidth).

Statistical Multiplexing

- ❖ Sharing the resources based on the statistics of demand. It can be applied at low layers for a single link, or at high layers for a network or even applications that use the network.

- **Flow Control**
  - ❖ Flow control is a technique used to regulate data transfer between computers or other nodes in a network. Flowcontrol ensures that the transmitting device does not send more data to the receiving device than it can handle.
- **Congestion**
  - ❖ When too many computers want to send the data and the network cannot handle it all. Thos overloading ofcomputers are called congestion. This makes the end users' network slow.
- **Quality of service(QoS)**
  - ❖ QoS is the use of mechanisms or technologies that work on a network to control traffic and ensure theperformance of critical applications with limited network capacity.
- **Security**
  - ❖ **Confidentiality:** The data is only available to authorized parties. When information has been kept confidential, itmeans that it has not been compromised by other parties.
  - ❖ **Authentication:** Authentication is used by a client when the client need to know that the server is system itclaims to be. In authentication, the user or computer has to prove its identity to the server or client.
  - ❖ **Integrity:** Integrity means guarding against improper information modification or destruction and includesensuring information non repudiation and authencity.

1.2.3 Connection Oriented Versus Connectionless Service:

- **Connection oriented:** The service user first establishes a connection, uses the connection, and then releases the connection.
  - ❖ The essential aspect of a connection is that it acts like a tube: the sender pushes objects (bits) in at one end, and the receiver takes them out at the other end.
  - ❖ A **circuit** is another name for a connection with associated resources, such as a fixed bandwidth.
  - ❖ Reliable connection-oriented service has two minor variations: message sequences and byte streams. In the former variant, the message boundaries are preserved. When two 1024-byte messages are sent, they arrive as two distinct 1024- byte messages, never as one 2048-byte message.
  - ❖ In the latter, the connection is simply a stream of bytes, with no message boundaries. When 2048 bytes arrive at the receiver, there is no way to tell if they were sent as one 2048-byte message, two 1024-byte messages, or 2048 1-byte messages.
- **Connectionless Service:** Each message (letter) carries the full destination address, and each one is routed

throughthe intermediate nodes inside the system independent of all the subsequent messages.

- A **packet** is a message at the network layer. When the intermediate nodes receive a message in full before sending it on to the next node, this is called **store-and-forward s witching.** The alternative, in which the onward transmission of a message at a node starts before it is completely received by the node, is called **cut-through s witching.**
- **Voice over IP:** For some applications, the transit delays introduced by acknowledgements are unacceptable. One such application is digitized voice traffic for **voice over IP**. It is less disruptive for telephone users to hear a bit of noise on the line from time to time than to experience a delay waiting for acknowledgements.
- Unreliable (meaning not acknowledged) connectionless service is often called **datagram** service. The six different types of service are

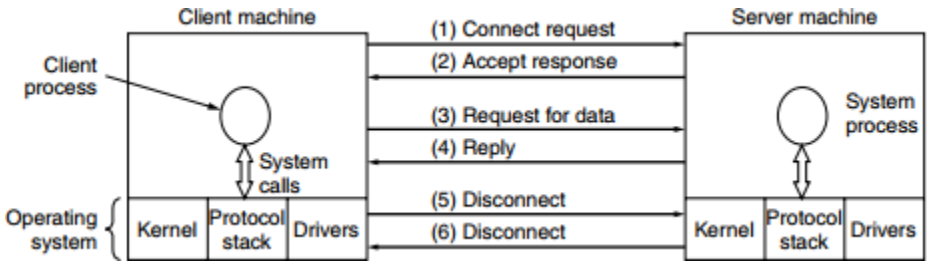
	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Movie download
	Unreliable connection	Voice over IP
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Text messaging
	Request-reply	Database query

1.2.4 Service Primitivies

- A service is formally specified by a set of **primitives** (operations) available to user processes to access the service. These primitives tell the service to perform some action or report on an action taken by a peer entity. The set of primitives available depends on the nature of the service being provided. The primitives for connection- oriented service are different from those of connectionless service.

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
ACCEPT	Accept an incoming connection from a peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

- First, the server executes LISTEN to indicate that it is prepared to accept incoming connections. Next, the client process executes CONNECT to establish a connection with the server. The CONNECT call needs to specify who to connect to.



- Then the client executes SEND to transmit its request (3) followed by the execution of RECEIVE to get the reply. The arrival of the request packet at the server machine unblocks the server so it can handle the request. After it has done the work, the server uses SEND to return the answer to the client (4). When the client is done, it executes DISCONNECT to terminate the connection (5). When the server gets the packet, it also issues a DISCONNECT of its own, acknowledging the client and releasing the connection (6).

1.2.5 The Relationship of Services to Protocols

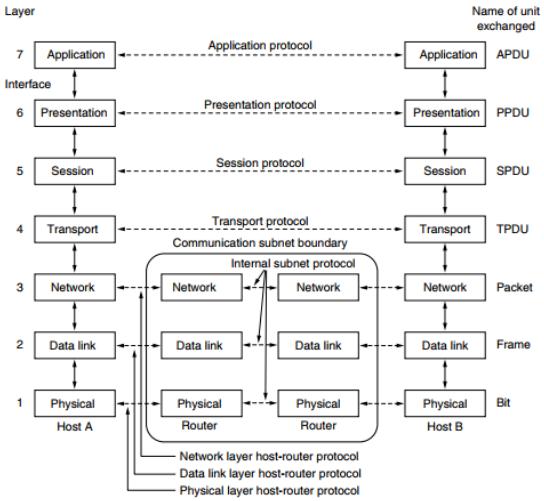
- **Service:** A *service* is a set of primitives (operations) that a layer provides to the layer above it. The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented. A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.
- **Protocol:** A Protocol is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer. Entities use protocols to implement their service definitions.

1.3 Reference Models

There are two important network architectures.

i) OSI reference model
ii) TCP/IP reference model

1.3.1 The OSI Reference Model



The OSI model has seven layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.

2. Each layer should perform a well-defined function.

3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.

4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

- **The Physical Layer**
  - ❖ The **physical layer** is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit it is received by the other side as a 1 bit, not as a 0 bit.
- **The Data Link Layer**
  - ❖ The main task of the **data link layer** is to transform a raw transmission facility into a line that appears free of undetected transmission errors. The sender breaks up the input data into **data frame** and transmit the frames sequentially.
  - ❖ If the service is reliable, the receiver confirms correct receipt of each frame by sending back an **acknowledgement frame**. The medium access control sublayer deals how to control access to the shared channel.
- **The Network Layer**
  - ❖ The **network layer** controls the operation of the subnet. A key design issue is determining how packets are routedfrom source to destination. Routes can be based on static tables that are ‘‘wired into’’ the network

and rarely changed, or more often they can be updated automatically to avoid failed components. Handling congestion is also the responsibility of the network layer.

- **The Transport Layer**

❖ The basic function of the **transport layer** is to accept data from above it, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. The transport layer also determines what type of service to provide to the session layer, and, ultimately, to the users of the network. The transport layer is a true end-to-end layer; it carries data all the way from the source to the destination.

- **The Session Layer**

❖ The session layer allows users on different machines to establish **sessions** between them. Sessions offer various services, including **dialog control** , **token management** (preventing two parties from attempting the same criticaloperation simultaneously), and **synchronization.**

- **The Presentation Layer**

❖ The **presentation layer** is concerned with the syntax and semantics of the information transmitted. The presentation layer manages these abstract data structures and allows higher-level data structures (e.g., banking records) to be defined and exchanged.

- **The Application Layer**

❖ The **application layer** contains a variety of protocols that are commonly needed by users. One widely used application protocol is **HTTP** (**HyperText Transfer Protocol**),

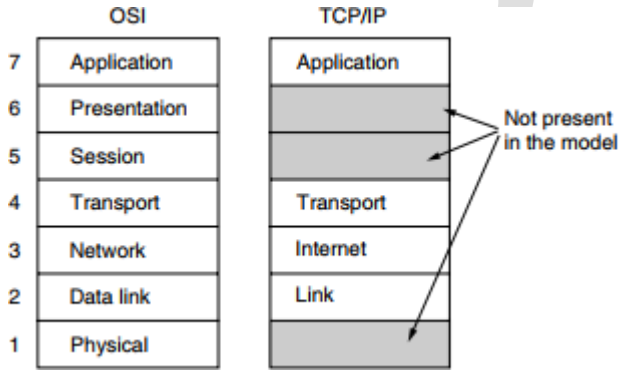
1.3.2 The TCP/IP Reference Model

- **The Link Layer**

❖ The **link layer** describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer.

- **The Internet Layer**

❖ The **internet layer** is the linchpin that holds the whole architecture together.



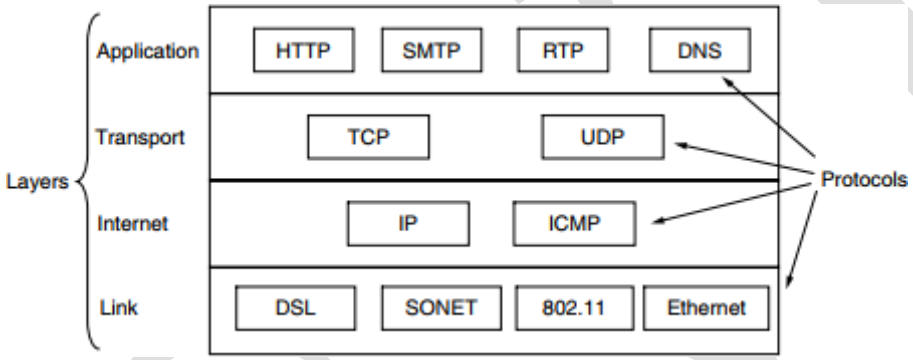
- Its job is to permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network). They may even arrive in a completely different order than they were sent.
- The internet layer defines an official packet format and protocol called **IP** (**Internet Protocol**), plus a companion protocol called **ICMP** (**Internet Control Message Protocol**) that helps it function.

- **The Transport Layer**

- The layer above the internet layer in the TCP/IP model is now usually called the **transport layer**. Two end-to- end transport protocols have been defined here. The first one, **TCP** (**Transmission Control Protocol**), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet.
- The second protocol in this layer, **UDP** (**User Datagram Protocol**), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own.

- **The Application Layer**

- On top of the transport layer is the **application layer**. It contains all the higher-level protocols.



1.3.3 A Comparison of OSI and TCP/IP Reference Models

Parameters	OSI Model	TCP/IP Model
Full Form	Open Systems Interconnection	Transmission Control Protocol/ Internet Protocol
Layers	It has 7 layers	It has 4 layers
Usage	It is low in usage	It is mostly used.
Approach	It is vertically approached	It is horizontally approached
Delivery	Delivery of package is guaranteed.	Delivery is not guaranteed
Replacement	Changes can be easily done	Replacing the tools is not easy.
Reliability model	Less reliable than TCP/IP model	It is more reliable than OSI

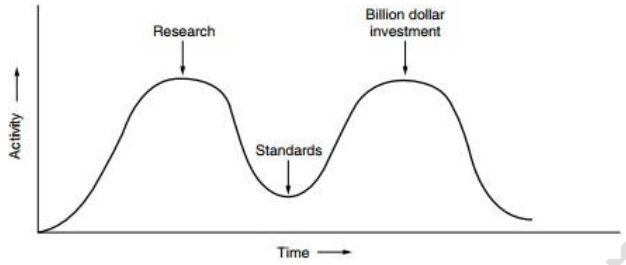
1.3.4 A Critique of OSI Model and Protocols

A critique of OSI Model and Protocols are

a) Bad Timing b) Bad Technology c) Bad Implementation d) Bad politics

Bad Timing

- The time at which a standard is established is absolutely critical to its success.



- When the subject is first discovered, there is a burst of research activity in the form of discussions, papers, and meetings. After a while this activity subsides, corporations discover the subject, and the billion-dollar wave of investment hits.
- If they are written too early (before the research results are well established), the subject may still be poorly understood; the result is a bad standard. If they are written too late, so many companies may have already made major investments in different ways of doing things that the standards are effectively ignored.

Bad Technology

The choice of seven layers was a bad one as two of the layers (session and presentation) are nearly empty, whereas two other ones (data link and network) are overfull. Another problem with OSI is that some functions, such as addressing, flow control, and error control, reappear again and again in each layer.

Bad Implementation

The initial implementations were huge, unwieldy, and slow.

Bad Politics

OSI, was widely thought to be the creature of the European telecommunication ministries, the European Community, and later the U.S. Government.

1.3.6 A Critique of TCP/IP Reference Model

1) The model does not clearly distinguish the concepts of services, interfaces, and protocols.
2) The TCP/IP model is not at all general and is poorly suited to describing any protocol stack other than TCP/IP.
3) The link layer is not really a layer at all in the normal sense of the term as used in the context of layered protocols.

4) The TCP/IP model does not distinguish between the physical and data link layers.

1.4 The Physical Layer

The physical layer is the first and lowest layer of the OSI communication model.

Its function is to transport data using electrical, mechanical or procedural interfaces.

1.4.1 Guided Transmission Medium

The purpose of the physical layer is to transport bits from one machine to another. Various physical media can be used for the actual transmission.

1.4.1.1 Magnetic Media

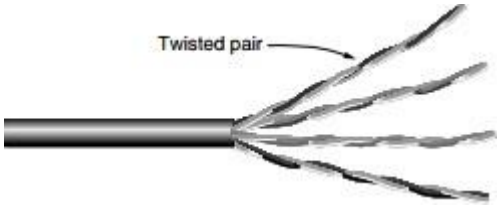
One of the most common ways to transport data from one computer to another is to write them onto magnetic tape or removable media (e.g., recordable DVDs), physically transport the tape or disks to the destination machine, and read them back in again.

Common types of magnetic media are, audio reel to reel cassettes tapes, hard disk drives, floppy disks etc..

1.4.1.2 Twisted Pairs

- A twisted pair consists of two insulated copper wires, typically about 1 mm thick. The wires are twisted together in a helical form, just like a DNA molecule. Twisting is done because two parallel wires constitute a fine antenna.
- When the wires are twisted, the waves from different twists cancel out, so the wire radiates less effectively. A signal is usually carried as the difference in voltage between the two wires in the pair. This provides better immunity to external noise because the noise tends to affect both wires the same, leaving the differential unchanged.
- The most common application of the twisted pair is the telephone system. Nearly all telephones are connected to the telephone company (telco) office by a twisted pair. Both telephone calls and ADSL Internet access run over these lines.
- Twisted pairs can be used for transmitting either analog or digital information. The bandwidth depends on the thickness of the wire and the distance traveled, but several megabits/sec can be achieved for a few kilometres

Varieties of Twisted pair Cabling



The garden variety deployed in many office buildings is called **Category 5** cabling, or ‘‘Cat 5.

A category 5 twisted pair consists of two insulated wires gently twisted together. Four such pairs are typically grouped in a plastic sheath to protect the wires and keep them together. To reach higher speeds, 1-Gbps Ethernet uses all four pairs in both directions simultaneously.

Full duplex

Links that can be used in both directions at the same time, like a two-lane road, are called **full-duplex** links.

Half duplex

Links that can be used in either direction, but only one way at a time, like a single-track railroad line, called **half-duplex** links.

Simplex

Links that allow traffic in only one direction, like a one-way street are called **simplex** links.

Category 3

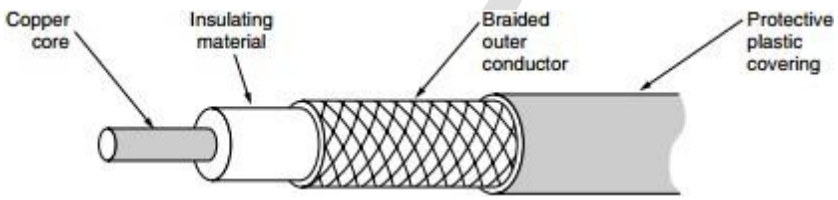
Cable uses a same connector, but has more twists per meter. More twists result in less crosstalk and a better-quality signal over longer distances, making the cables more suitable for high-speed computer communication, especially 100-Mbps and 1-Gbps Ethernet LANs.

Category 6 and Category 7

New wiring use these categories. It has more specifications to handle signals with greater bandwidths. In category 6, wiring types are referred to as UTP(Unshielded Twisted Pair). Category 7 cables have shielding on individual twisted pair. Shielding reduces the susceptibility to external interference and crosstalk with other nearby cables to meet demanding performance specifications.

1.4.1. 3 Coaxial Cable

- Coaxial cable has better shielding and greater bandwidth than unshielded twisted pairs, so it can span longer distances at higher speeds.
- Two kinds of coaxial cable are widely used. One kind, 50-ohm cable, is commonly used when it is intended for digital transmission from the start. The other kind, 75-ohm cable, is commonly used for analog transmission and cable television.

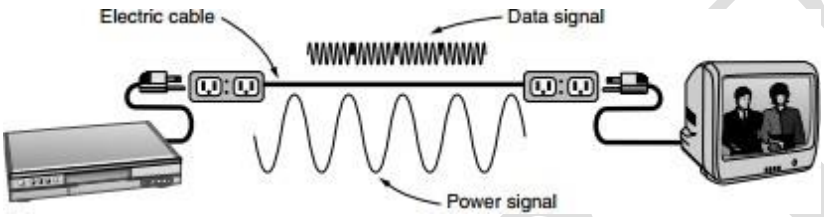


- A coaxial cable consists of a stiff copper wire as the core, surrounded by an insulating material. The insulator is encased by a cylindrical conductor, often as a closely woven braided mesh. The outer conductor is covered in a protective plastic sheath.

- The bandwidth possible depends on the cable quality and length. Coaxial cables used to be widely used within thetelephone system for long-distance lines but have now largely been replaced by fiber optics on longhaul routes. Coax is still widely used for cable television and metropolitan area networks.

1.4.1.4 Power Lines

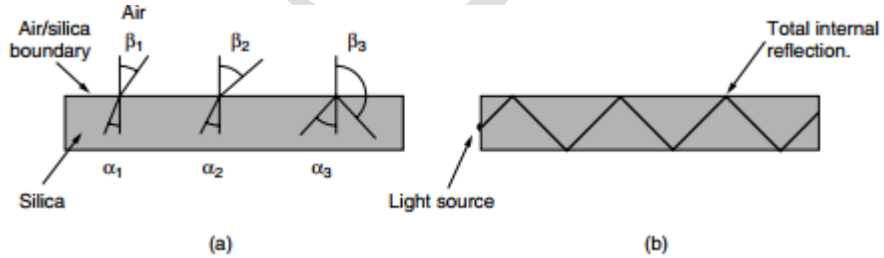
- Power lines deliver electrical power to houses, and electrical wiring within houses distributes the power to electrical outlets.
- Power lines have been used by electricity companies for low-rate communication such as remote metering. The convenience of using power lines for networking should be like simply plug a TV and a receiver into the wall, because they need power, and they can send and receive movies over the electrical wiring.



- Electrical signals are sent at 50–60 Hz and the wiring attenuates the much higher frequency (MHz) signals needed for high-rate data communication. The electrical properties of the wiring vary from one house to the next and change as appliances are turned on and off, which causes data signals to bounce around the wiring.

1.4.1.5 Fiber Optics

- Fiber optics are used for long-haul transmission in network backbones, highspeed LANs (although so far, copper has always managed catch up eventually), and high-speed Internet access such as **FttH** (**Fiber to the Home**).
- An optical transmission system has three key components: the light source, the transmission medium, and the detector. The transmission medium is an ultra-thin fiber of glass. The detector generates an electrica l pulse when light falls on it.
- By attaching a light source to one end of an optical fiber and a detector to the other, we have a unidirectional data transmission system that accepts an electrical signal, converts and transmits it by light pulses, and then reconverts the output to an electrical signal at the receiving end.



Fig(a): When a light ray passes from one medium to another—for example, from fused silica to air—the ray is

refracted (bent) at the silica/air boundary. A light ray incident on the boundary at an angle α1 emerging at an angle β1. The amount of refraction depends on the properties of the two media (in particular, their indices of refraction)

Fig (b): The light is refracted back into the silica; none of it escapes into the air. Thus, a light ray incident at or above the critical angle is trapped inside the fiber. The fig shows the only one trapped ray, but since any light ray incident on the boundary above the critical angle will be reflected internally, many different rays will be bouncing around at different angles. Each ray is said to have a different mode, so a fiber having this property is called a **multimode fiber**.

Single mode fiber

if the fiber's diameter is reduced to a few wavelengths of light the fiber acts like a wave guide and the light can propagate only in a straight line, without bouncing, yielding a **single-mode fiber.** Single- mode fibers are more expensive but are widely used for longer distances.

Transmission of Light Through Fiber

Optical fibers are made of glass, which, in turn, is made from sand, an inexpensive raw material available in unlimited amounts. The attenuation of light through glass depends on the wavelength of the light. It is defined as the ratio of input to output signal power.

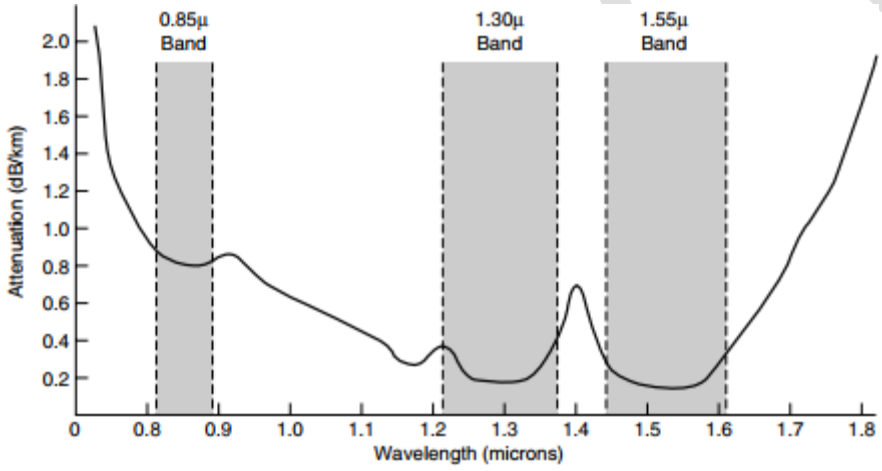


Figure 2-7. Attenuation of light through fiber in the infrared region.

The figure shows the near- infrared part of the spectrum. Visible light has slightly shorter wavelengths, from 0.4 to 0.7 microns. The true metric purist would refer to these wavelengths as 400 nm to 700 nm. Three wavelength bands are most commonly used at present for optical communication. They are centered at 0.85, 1.30, and 1.55 microns, respectively. All three bands are 25,000 to 30,000 GHz wide. The 0.85- micron band was used first. It has higher attenuation and so is used for shorter distances. The last two bands have good attenuation properties (less than 5% loss per kilometer). The 1.55- micron band is now widely used with erbium-doped amplifiers that work directly in the optical domain.

Chromatic Dispersion

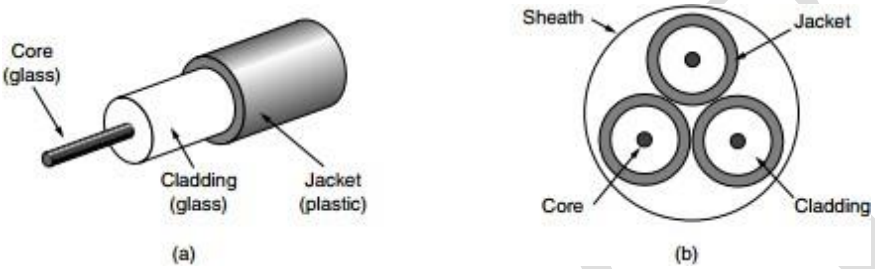
Light pulses sent down a fiber spread out in length as they propagate.

Soliton:

A soliton is a pulse that can collide with another similar pulse and still retain its shape after the collision, again in the presence of both dispersion and non-linearities.

1.4.1.6 Fiber Cables

- Fiber optic cables are similar to coax, except without the braid. At the center is the glass core through which the light propagates. In multimode fibers, the core is typically 50 microns in diameter, about the thickness of a human hair. In single-mode fibers, the core is 8 to 10 microns.



- The core is surrounded by a glass cladding with a lower index of refraction than the core, to keep all the light in the core. Next comes a thin plastic jacket to protect the cladding. Fibers are typically grouped in bundles, protected by an outer sheath.
- Fibers can be connected in three different ways. First, they can terminate in connectors and be plugged into fiber sockets. Connectors lose about 10 to 20% of the light, but they make it easy to reconfigure systems.
- Second, they can be spliced mechanically. Mechanical splices just lay the two carefully cut ends next to each other in a special sleeve and clamp them in place. Alignment can be improved by passing light through the junction and then making small adjustments to maximize the signal.
- Third, two pieces of fiber can be fused (melted) to form a solid connection. A fusion splice is almost as good as a single drawn fiber, but even here, a small amount of attenuation occurs. For all three kinds of splices, reflections can occur at the point of the splice, and the reflected energy can interfere with the signal.

Item	LED	Semiconductor laser
Data rate	Low	High
Fiber type	Multi-mode	Multi-mode or single-mode
Distance	Short	Long
Lifetime	Long life	Short life
Temperature sensitivity	Minor	Substantial
Cost	Low cost	Expensive

Figure 2-9. A comparison of semiconductor diodes and LEDs as light sources.

Comparison of Fiber Optics and Copper Wire

Advantages of Fiber Optics:

- It can handle higher bandwidths than copper.
- Fiber optic cables have low attenuation.
- Fiber optics cables are not affected by electromagnetic interferences and power fluctuations.
- Fiber optic cables are much more secured.
- Fiber cables are thin and light weight.
- The life cycle of fiber cables is 30 to 50 years, which is much higher than copper cables.

Disadvantages of Fiber Optics:

- It is a newer technology with not much expertise.
- Copper cables and connectors are much cheaper than fiber optic cables and connectors.
- Propagation of signals in fiber optic cables is unidirectional.

1.5 WIRELESS TRANSMISSION

Wireless communications has many important applications besides providing connectivity to users from any place.

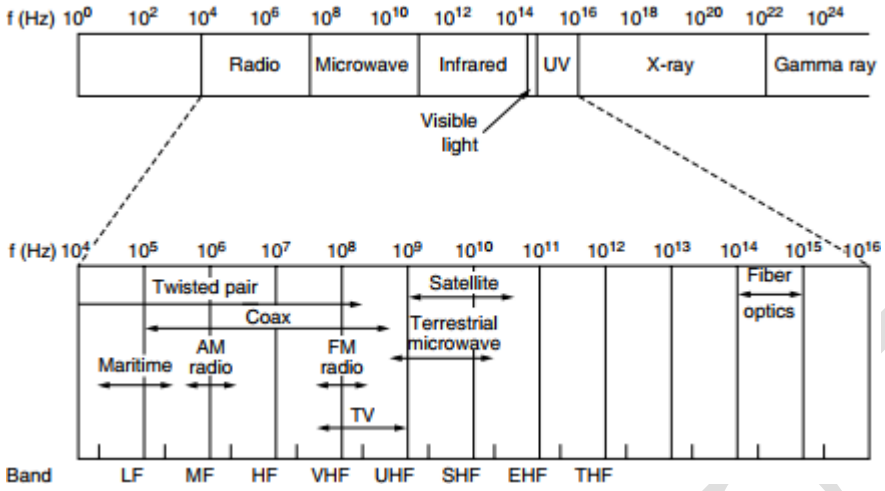
1.5.1 The Electromagnetic Spectrum

- When electrons move, they create electromagnetic waves that can propagate through space.
- The number of oscillations per second of a wave is called its **frequency**, *f*, and is measured in **Hz.** The distance between two consecutive maxima (or minima) is called the **wavelength,** represented by lambda.
- In a vacuum, all electromagnetic waves travel at the same speed, no matter what their frequency. This speed, usually called the **speed of light**, *c*, is approximately 3 × 108 m/sec, or about 1 foot (30 cm) per nanosecond.

The fundamental relation between f, λ, and c (in a vacuum) is

$$\lambda f = c$$

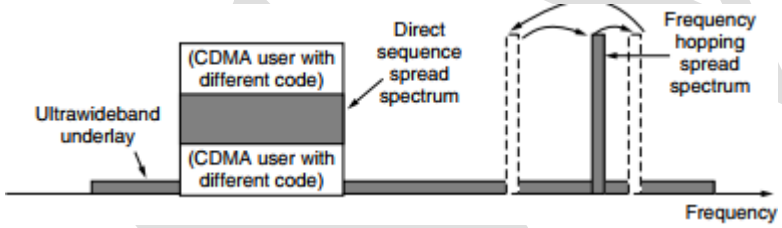
- The radio, microwave, infrared, and visible light portions of the spectrum can all be used for transmitting information by modulating the amplitude, frequency, or phase of the waves. Ultraviolet light, X-rays, and gamma rays would be even better, due to their higher frequencies, but they are hard to produce and modulate, do not propagate well. The terms LF, MF, and HF refer to Low, Medium, and High Frequency, respectively.



- Most transmissions use a relatively narrow frequency band (i.e., $\Delta f / f << 1$). In **frequency hopping spread spectrum**, the transmitter hops from frequency to frequency hundreds of times per second. It is pop ular for military communication because it makes transmissions hard to detect and next to impossible to jam. This technique is used commercially, for example, in Bluetooth and older versions of 802.11.

Direct Sequence spread spectrum

A second form of spread spectrum, **direct sequence spread spectrum**, uses a code sequence to spread the data signal over a wider frequency band. It is widely used commercially as a spectrally efficient way to let multiple signals share the same frequency band. These signals can be given different codes, a method called **CDMA** (**Code Division Multiple Access**)



It forms the basis of 3G mobile phone networks and is also used in GPS (Global Positioning System).

UWB(UltraWideBand)

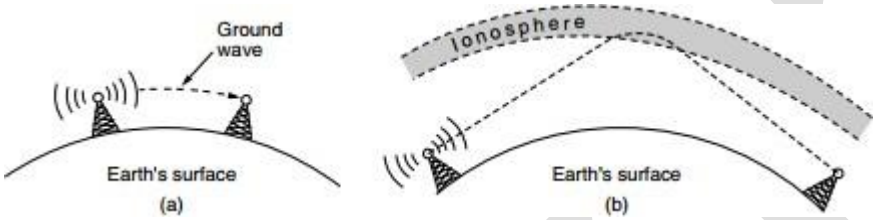
UWB sends a series of rapid pulses, varying their positions to communicate information. The rapid transitions lead to a signal that is spread thinly over a very wide frequency band. UWB is defined as signals that have a bandwidth of at least 500 MHz or at least 20% of the center frequency of their frequency band. It can tolerate a substantial amount of relatively strong interference from other narrowband signals, because it is spread across wide band of frequencies.

1.5.2 Radio Transmission

- Radio frequency (RF) waves are easy to generate, can travel long distances, and can penetrate buildings easily, so they are widely used for communication, both indoors and outdoors. Radio waves also are omni

directional, meaning that they travel in all directions from the source, so the transmitter and receiver do not have to be carefully aligned physically.

- The properties of radio waves are frequency dependent. At low frequencies, radio waves pass through obstacles well, but the power falls off sharply with distance from the source—at least as fast as $1/r^2$ in air—asthe signal energy is spread more thinly over a larger surface. This attenuation is called **path loss.**
- At high frequencies, radio waves tend to travel in straight lines and bounce off obstacles. Path loss still reduces power, though the received signal can depend strongly on reflections as well. High- frequency radio waves are also absorbed by rain and other obstacles to a larger extent than are low-frequency ones. At all frequencies, radio waves are subject to interference from motors and other electrical equipment.



From fig(a): In the VLF, LF, and MF bands, radio waves follow the ground. These waves can be detected for perhaps 1000 km at the lower frequencies, less at the higher ones. AM radio broadcasting uses the MF band.

Fig(b) In the HF and VHF bands, the ground waves tend to be absorbed by the earth. However, the waves that reach the ionosphere, a layer of charged particles circling the earth at a height of 100 to 500 km, are refracted by it and sent back to earth.

1.5.3 Microwave Transmission

- Microwaves travel in a straight line. Thus, repeaters are needed periodically. The distance between repeaters is square root of the tower height. For 100- meter-high towers, repeaters can be 80 km apart. Microwaves do not pass through buildings well.
- Some waves may be refracted off low- lying atmospheric layers and may take slightlylonger to arrive than the direct waves. The delayed waves may arrive out of phase with the direct wave and thus cancel the signal. This effect is called **multipath fading.**
- Bands up to 10 GHz are now in routine use. These waves are only a few centimetres long and are absorbed by rain. Microwave communication is so widely used for long-distance telephone communication, mobile phones, television distribution. It does not require to lay down cables. By buying a small plot of ground every 50 km and putting a microwave tower on it, one can bypass the telephone system entirely. Microwave is also relatively inexpensive.

Politics of ElectroMagnetic Spectrum

National governments allocate spectrum for AM and FM radio, television, and mobile phones, as well as for telephone companies, police, maritime, navigation, military, government, and many other competing users.

3 algorithms are widely used.

Beauty Contest

Oldest algorithm requires each carrier to explain why its proposal serves the public interest best. Government officials then decide which of the nice stories they enjoy most.

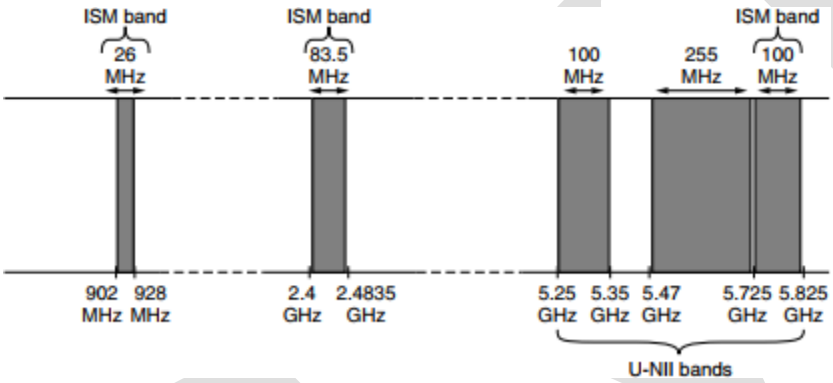
Lottery

Second algorithm which holds lottery among the interested companies. The problem with that idea is that companies with no interest in using the spectrum can enter the lottery.

Auction

Random companies has been severely criticized by many, which led to algorithm 3: **auction** off the bandwidth to the highest bidder.

A completely different approach to allocating frequencies is to not allocate them at all. Accordingly, most governments have set aside some frequency bands, called the **ISM** (**Industrial, Scientific, Medical**) bands for unlicensed usage. To minimize interference between these uncoordinated devices, the FCC mandates that all devices in the ISM bands limit their transmit power.



The 900-MHz band was used for early versions of 802.11, but it is crowded. The 2.4-GHz band is available in most countries and widely used for 802.11b/g and Bluetooth, though it is subject to interference from microwave ovens and radar installations. The 5-GHz part of the spectrum includes **U-NII** (**Unlicensed National Information Infrastructure**) bands.

One exciting development in the U.S. is the FCC decision in 2009 to allow unlicensed use of **white spaces** around 700 MHz. White spaces are frequency bands that have been allocated but are not being used locally. The only difficulty to use the white spaces, unlicensed devices must be able to detect any nearby licensed transmitters, including wireless microphones.

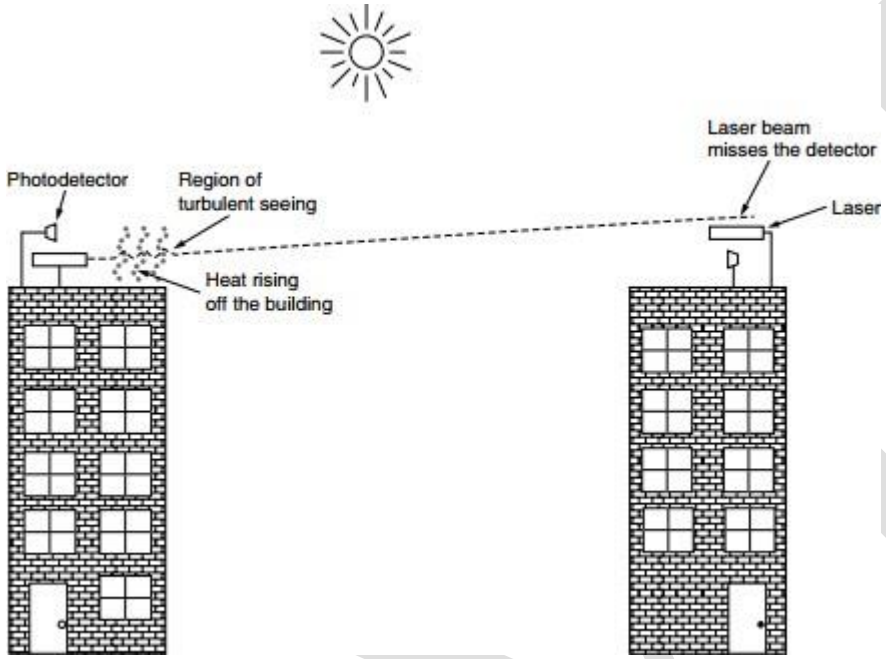
1.5.4 InfraRed Transmission

- Unguided infrared waves are widely used for short-range communication. The remote controls used for televisions, VCRs, and stereos all use infrared communication.
- They are relatively directional, cheap, and easy to build but have a major drawback: they do not pass through solid objects. It means that an infrared system in one room of a building will not interfere with a similar system in adjacent rooms or buildings.

- Infrared communication has a limited use on the desktop, for example, to connect notebook computers and printers with the **IrDA** (**Infrared Data Association**) standard, but it is not a major player in the communication game.

1.5.5 Light Transmission

A more modern application is to connect the LANs in two buildings via lasers mounted on their rooftops. Optical signaling using lasers is inherently unidirectional, so each end needs its own laser and its own photo detector.



To avoid unnecessary wiring for only limited days, the organizers placed the laser on the roof, and tested in the night which worked perfectly. At 9 A.M. on a bright, sunny day, the link failed completely and stayed down all day. The problem is that because heat from the sun during the daytime caused convection currents to rise up from the roof of the building. This turbulent air diverted the beam and made it dance around the detector, much like a shimmering road on a hot day. Communicating with visible light in this way is inherently safe and creates a low-speed network in the immediate vicinity of the display.