Module-I

INTRODUCTION

- Each of the past three centuries was dominated by a single new technology.
- The 18th century was the era of the great mechanical systems accompanying the Industrial Revolution.
- The 19th century was the age of the steam engine.
- During the 20th century, the technology was information gathering, processing, and distribution. Ex: Telephone networks, invention of radio and computer industry, communication satellites, Internet.
- The 21st century Networks are Human-to-Human, Machine-to-Machine.
- **Computer Network:** A collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information. The connection need not be via a copper wire; fiber optics, microwaves, infrared and communication satellites can also be used. Networks come in many sizes, shapes and forms, as we will see later. They are usually connected together to make larger networks, for example **Internet.**
- **Uses of Computer Networks**

A) **Business Applications:** Resource Sharing, Client-Server-mail, video conferencing

- Many companies have a substantial number of computers. For example, a company may have separate computers to monitor production, keep track of inventories, and do the payroll. Initially, each of these computers may have worked in isolation from the others, but at some point, management may have decided to connect them to be able to extract and correlate information about the entire company.

1. **Resource sharing:** The main task of the connectivity of resources is resource sharing. For example, a high-volume networked printer may be installed instead of large collection of individual printers.
2. **Information Sharing:** large and medium-sized company and many small companies are vitally dependent on computerized information. This can be done by a simple client server model connected by network as illustrated in Fig.1.4.

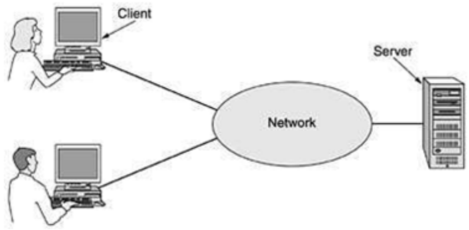


Figure 1.4 A network with two clients and one server

In client-server model in detail, two processes are involved, one on the client machineand one on the server machine. Communication takes the form of the client process sending a message over the network to the server process. The client process then waits for a reply message. When the server process gets the request, it performs the requested work or looks up the requested data and sends back a reply. These messagesare shown in Fig. 1.5.

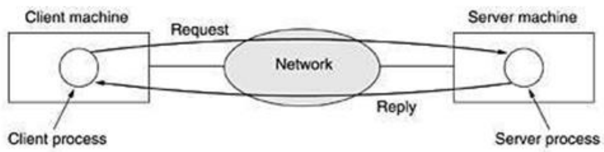


Figure 1.5 Client-server model involves requests and replies

3. **Connecting People:** another use of setting up a computer network has to do with people rather than information or even computers. It is achieved through Email, Video Conferencing.
4. **E-commerce:** many companies is doing business electronically with other companies, especially suppliers and customers, and doing business with consumers over the Internet.

B) **Home Applications:** Shopping, Digital library, email, game playing, TV,Twitter, Instagram

The computer network provides better connectivity for home applications via desktop computers, laptops, iPads, iPhones. Some of the more popular uses of the Internet for home users are as follows:

1. Access to remote information.
2. Person-to-person communication (peer-to-peer).
   i. Peer-to-peer - there are no fixed clients and servers.
   ii. Audio and Video sharing
3. Interactive entertainment.
4. Electronic commerce.

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books on-line
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products on line
P2P	Peer-to-peer	File sharing

Table 1.2 some forms of e-commerce

C) **Mobile Users:** Notebook Computer,Hotspots,Text Messaging,GPS

As wireless technology becomes more widespread, numerous other applications are likely to emerge. Wireless networks are of great value to fleets of trucks, taxis, delivery vehicles, and repairpersons for keeping in contact with home. Wireless networks are also important to the military.

Although wireless networking and mobile computing are often related, they are not identical, as Table 1.3 shows. Here we see a distinction between fixed wireless and mobile wireless. Even notebook computers are sometimes wired. For example, if a traveler plugs a notebook computer into the telephone jack in a hotel room, he has mobility without a wirelessnetwork.

Wireless	Mobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	Portable office; PDA for store inventory

Table 1.3 Combinations of wireless networks and mobile computing

Another area in which wireless could save money is utility meter reading. If electricity, gas, water, and other meters in people's homes were to report usage over a wireless network, there would be no need to send out meter readers.

D) Social Issues: Phishing,network neutrality(Traffic treated as equal)

The widespread introduction of networking has introduced new social, ethical, and political problems. A popular feature of many networks is newsgroups or bulletin boards whereby people can exchange messages with like-minded individuals. As long as the subjectsare restricted to technical topics or hobbies like gardening, not too many problems will arise.

The following are the issues in society due to the misbehave or misconduct of computernetworks.

1. Network neutrality
2. Digital Millennium Copyright Act
3. Profiling users
4. Phishing

NETWORK HARDWARE

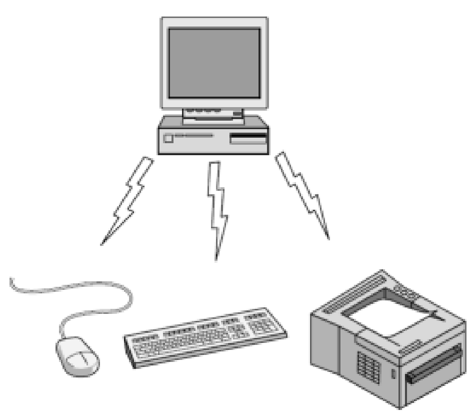
- ❖ There is no generally accepted taxonomy into which all computer networks fit, but two dimensions stand out as important: transmission technology and scale.
- ❖ There are two transmission technologies: Broadcast links and Point-to-Point links.
- ❖ **Point-to-point** links connect individual pairs of machines. To go from the source to the destination on a network made up of point-to-point links, short messages, called **packets** in certain contexts, may have to first visit one or more intermediate machines.
- ❖ Often multiple routes of different lengths are possible, so finding good ones is important in point-to-point networks.
- ❖ Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called **unicasting**. Example browsing a website.
- ❖ **Broadcast links**: single communication channel shared by all machines, example wireless network.
- ❖ 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.
- ❖ Some broadcast systems also support transmission to a subset of the machines, which known as **multicasting**.

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

Classification of interconnected processors by scale.

PANs (Personal Area Networks):

- ❖ Let devices communicate over the range of a person.
- ❖ For example a wireless network that connects a computer with its peripherals, without using wireless, this connection must be done with cables.
- ❖ So many new users have a hard time finding the right cables and plugging them into the right place.
- ❖ To help these users, some companies got together to design a short-range wireless network called Bluetooth to connect these components without wires.
- ❖ The idea is that if your devices have Bluetooth, then you need no cables. You just put them down, turn them on, and they work together. For many people, this ease of operation is a big plus.
- ❖ In the simplest form, Bluetooth networks use the **master-slave paradigm** of
- ❖ Fig. 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.
- ❖ It connects a headset to a mobile phone without cords and it can allow your digital music player

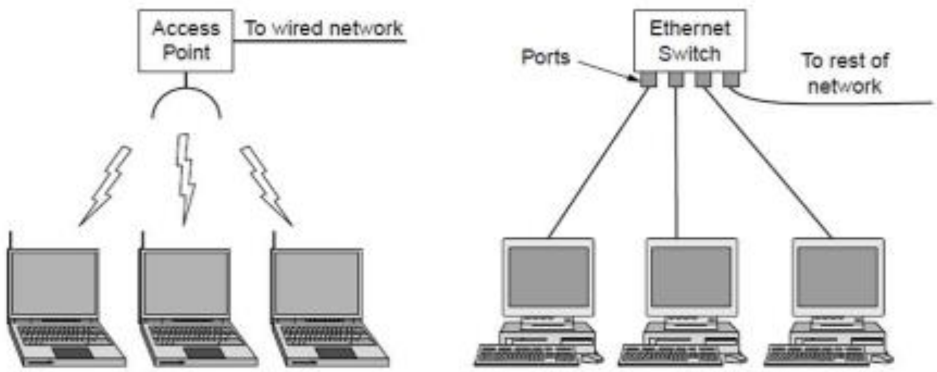


Bluetooth PAN configuration

LAN (Local Area Network):

- ❖ It is a privately owned network that operates within and nearby a single building like a home, office or factory.

- When LANs are used by companies, they are called enterprise networks.
- Wireless LANs(IEEE 802.11) /Wireless Fidelity (WiFi): It is used in homes, older office buildings, cafeterias, and other places where it is too much trouble to install cables.
- In these systems, every computer has a radio modem and an antenna that it uses to communicate with other computers.



Wireless and wired LANs. (a) 802.11. (b) Switched Ethernet.

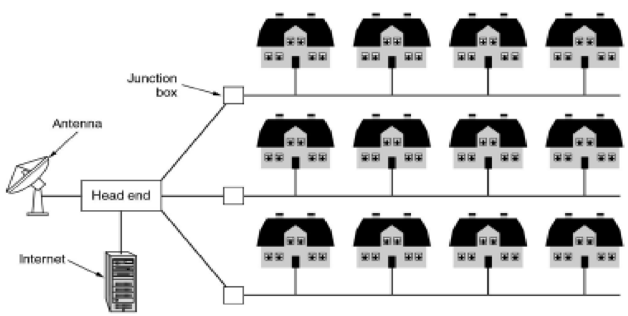
- An AP (Access Point), wireless router, or base station, relays packets between the wireless computers and also between them and the Internet.
- Wireless LAN operates at a speed of 11 to 100's Mbps.
- Wired LANs use a range of different transmission technologies. Most of them use copper wires, but some use optical fiber. LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance.
- Wired LANs run at speeds of 100 Mbps to 1 Gbps, have low delay and few errors. Newer LANs can operate at up to 10 Gbps. It is just easier to send signals over a wire or through a fiber than through the air.
- The topology wired LANs is built from point-to-point links. IEEE 802.3, called **Ethernet**, is, by far, the most common type of wired LAN. Fig. (b) **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.
- Both wireless and wired broadcast networks can be divided into static and dynamic designs, depending on how the channel is allocated.

- Static allocation would be to divide time into discrete intervals and use a round-robin algorithm, allowing each machine to broadcast only when its time slot comes up.
- Static allocation wastes channel capacity when a machine has nothing to say during its allocated slot, so most systems attempt to allocate the channel dynamically (i.e., on demand).
- Dynamic allocation methods for a common channel are either centralized or decentralized.
- **Centralized channel allocation: T**here is a single entity, for example, the base station in cellular networks, which determines who goes next. It might do this by accepting multiple packets and prioritizing them according to some internal algorithm.

- **Decentralized channel allocation:** there is no central entity; each machine must decide for itself whether to transmit.

MAN (**Metropolitan Area Network**):

- It covers a city and best-known example is cable television networks available in many cities. These systems grew from earlier community antenna systems used in areas with poor over-the-air television reception. In those early systems, a large antenna was placed on top of a nearby hill and a signal was then piped to the subscribers' houses.
- At first, these were locally designed, ad hoc systems. The next step was television programming and even entire channels designed for cable only. Often these channels were highly specialized, such as all news, all sports, all cooking, all gardening, and so on.
- When the Internet began attracting a mass audience, the cable TV network operators began to realize that with some changes to the system, they could pro- vide two-way Internet service in unused parts of the spectrum.
- In figure, both television signals and Internet being fed into the centralized **cable headend** for subsequent distribution to people's homes.
- Recent developments in high- speed wireless Internet access have resulted in another MAN, which has been standardized as IEEE 802.16 and is popularly known as **WiMAX**



A metropolitan area network based on cable TV.

WAN (**Wide Area Network**):

- It Spans a large geographical area, often a country or continent.
- In most WANs, the subnet consists of two distinct components: transmission lines and switching elements.
- **Transmission lines** (copper wire, optical fiber, or even radio links) move bits between machines.
- Switching elements (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.
- The routers will usually connect different kinds of networking technology. The networks inside the offices may be switched Ethernet, for example, while the long-distance transmission lines may be SONET links.

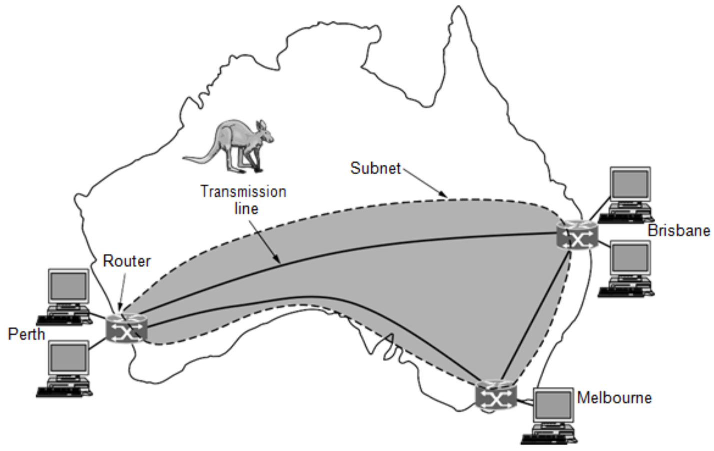


Figure 1-10. WAN that connects three branch offices in Australia.

❖ VPN (Virtual Private Network): it provides flexible reuse of a resource (Internet connectivity).
❖ It has disadvantage, which is a lack of control over the underlying resources and mileage may vary with internet speed.

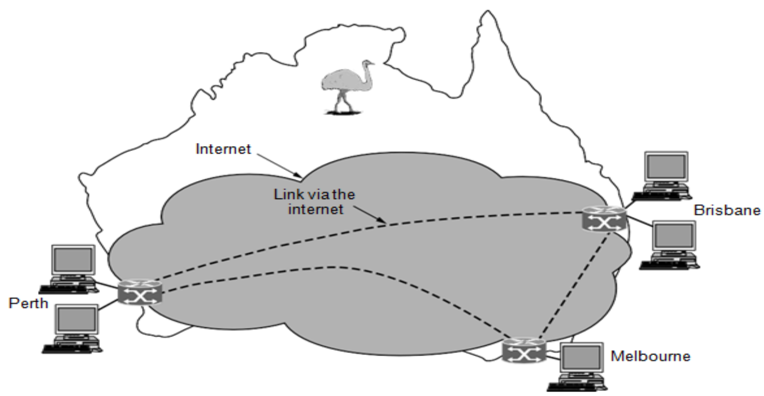


Figure 1-11. WAN using a virtual private network.

❖ 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.
❖ A subnet operator is called an **ISP** (**Internet Service Provider**) and the subnet is an **ISP network**. Its customers who connect to the ISP receive Internet service.

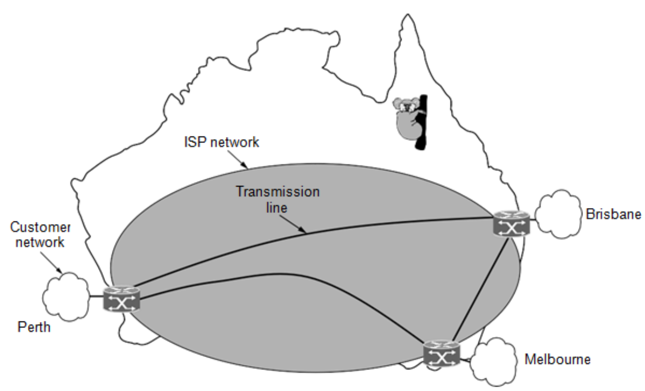


Figure 1-12. WAN using an ISP network.

❖ How the network makes the decision as to which path to use is called the **routing algorithm**.

- How each router makes the decision as to where to send a packet next is called the **forwarding algorithm**.
- Examples of WAN make heavy use of wireless technologies i.e. satellite systems.
- The cellular telephone network is another example of a WAN that uses wireless technology.
- 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.

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.
- There are two rules of thumb that are useful. First, if different organizations have paid to construct different parts of the network and each maintains its part, we have an internetwork rather than a single network.
- Second, if the underlying technology is different in different parts (e.g., broadcast versus point-to-point and wired versus wireless), we probably have an internetwork.
- Gateways are distinguished by the layer at which they operate in the protocol hierarchy.

NETWORK SOFTWARE:

Protocol Hierarchies:

- To reduce their 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. In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.

- When layer *n* on one machine carries on a conversation with layer *n* on another machine, the rules and conventions used in this conversation are collectively known as the layer *n* protocol. Basically, a **protocol** is an agreement between the communicating parties on how communication is to proceed.

- **A five-layer network is illustrated:**

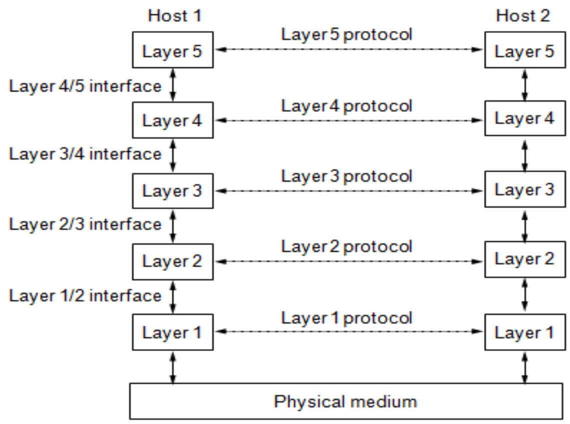


Figure 1-13. Layers, protocols, and interfaces.

- In reality, no data are directly transferred from layer *n* on one machine to layer *n* on another machine. Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached.
- Below layer 1 is the **physical medium** through which actual communication occurs. Virtual communication is shown by dotted lines and physical communication by solid lines.
- **Interface:** defines which primitive operations and services the lower layer makes available to the upper one.
- Clear- cut interfaces also make it simpler to replace one layer with a completely different protocol or implementation.
- A set of layers and protocols is called network **architecture.** The specification of 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**.

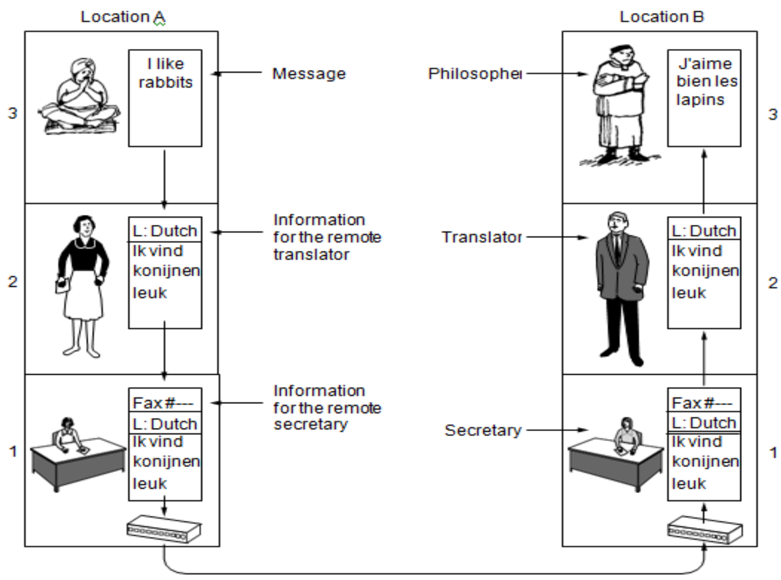


Figure 1-14. The philosopher-translator-secretary architecture.

- In this example, M is split into two parts, M_1 and M_2, that will be transmitted separately.
  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. None of the headers for layers below n are passed up to layer n.

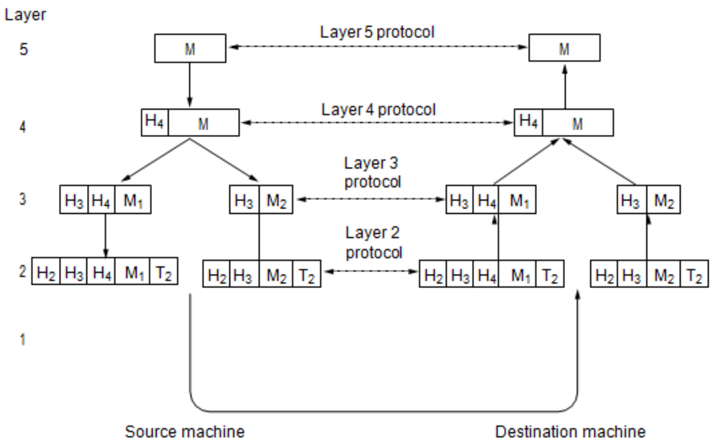


Figure 1-15. Example information flow supporting virtual communication in layer 5.

Design Issues for the Layers:

Some of the key design issues that occur in computer networks are present in several layers. The following are briefly mention some of the more important ones.

- ***Identifying senders and receivers*** - some form of addressing is needed in order tospecify a specific source and destination.
- ***Rules for data transfer*** - The protocol must also determine the direction of dataflow, how many logical channels the connection corresponds to and what their priorities are. Many networks provide at least two logical channels per connection,one for normal data and one for urgent data.
- ***Error control*** – when circuits are not perfect, both ends of the connection must agree on which error-detecting and error-correcting codes is being used.
- ***Sequencing*** - protocol must make explicit provision for the receiver to allow the pieces to be reassembled properly.
- ***Flow Control*** - how to keep a fast sender from swamping a slow receiver with data.This is done by feedback-based (receiver to sender) or agreed-on transmission rate.

- ***Segmentation and reassembly*** - several levels are the inability of all processes to accept arbitrarily long messages. It leads to mechanisms for disassembling, transmitting, and then reassembling messages.
- ***Multiplexing and demultiplexing*** – to share the communication medium by severalusers.
- ***Routing*** - When there are multiple paths between source and destination, a route must be chosen.

Connection-Oriented Versus Connectionless Service:

- ❖ Connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection.
- ❖ Connection acts like a tube: the sender pushes objects (bits) in at one end, and the receiver takes them out at the other end. In most cases the order is preserved so that the bits arrive in the order they were sent.
- ❖ In some cases when a connection is established, the sender, receiver, and subnet conduct a **negotiation** about the parameters to be used, such as max message size, QoS required etc. Typically, one side makes a proposal and the other side can accept it, reject it, or make a counter- proposal.
- ❖ **Connectionless** service is modeled after the postal system. Each message (letter) carries the full destination address, and each one is routed through the intermediate nodes inside the system independent of all the subsequent messages.
- ❖ There are different names for messages in different contexts; 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 switching**.
- ❖ 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 switching**.
- ❖ Unreliable (meaning not acknowledged) connectionless service is often called **datagram** service, in analogy with telegram service, which also does not return an acknowledgement to the sender.

	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

Figure 1-16. Six different types of service.

Service Primitives (Operations):

- ❖ These primitives tell the service to perform some action or report on an action taken by peer entity.

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

Figure 1-17. Six service primitives that provide a simple connection-oriented service.

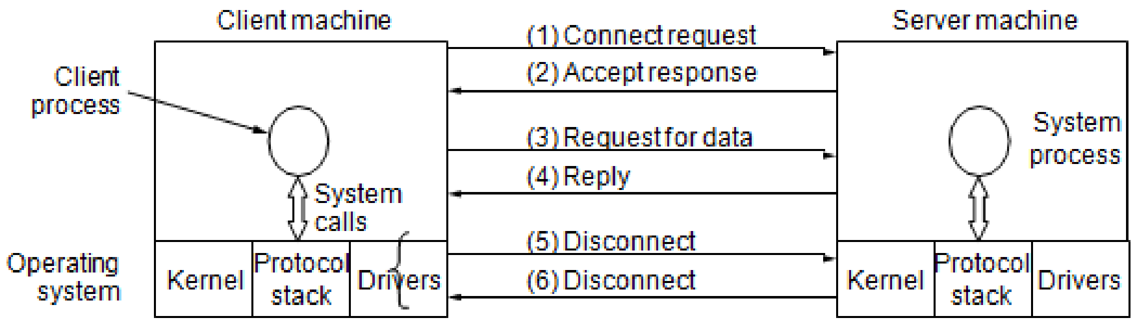


Figure 1-18. A simple client-server interaction using acknowledged datagram's.

- ❖ First, the server executes LISTEN to indicate that it is prepared to accept in coming connections. A common way to implement LISTEN is to make it a blocking system call. After executing the primitive, the server process is blocked untila request for connection appears.
- ❖ Next, the client process executes CONNECT to establish a connection with the server. The CONNECT call needs to specify who to connect to, so it might have a parameter giving the server's address. Client is suspended until there is a response.
- ❖ When the packet arrives at the server, the operating system sees that the packet is requesting a connection. It checks to see if there is a listener, and if so it unblocks the listener. The server process can then establish the connection with the ACCEPT call.
- ❖ The next step is for the server to execute RECEIVE to prepare to accept the first request. Normally, the server does this immediately upon being released from the LISTEN, before the acknowledgement can get back to the client. The RECEIVE call blocks the server.
- ❖ Then the client executes SEND to transmit its request followed by the execution of RECEIVE to get the reply.
- ❖ When the client is done, it executes DISCONNECT to terminate the connection.

The Relationship of Services to Protocols

- ❖ **A *service*** is a set of primitives (operations) thata layer provides to the layer above it. I t defines what operations the layer is prepared to perform on behalf of its users. 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.
- ❖ A service is like an abstract data type or an object in an object-oriented language. It defines operations that can be performed on an object but does not specify how these operationsare implemented.

- **A *protocol,*** in contrast, 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.
- In contrast, a protocol relates to the *implementation* of the ser- vice and as such is not visible to the user of the service.

Figure 1-19. The relationship between a service and a protocol.

REFERENCE MODELS

The OSI Reference Model

- This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers (Day and Zimmermann, 1983).
- It was revised in 1995 (Day, 1995). The model is called the ISO OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems.
- 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.

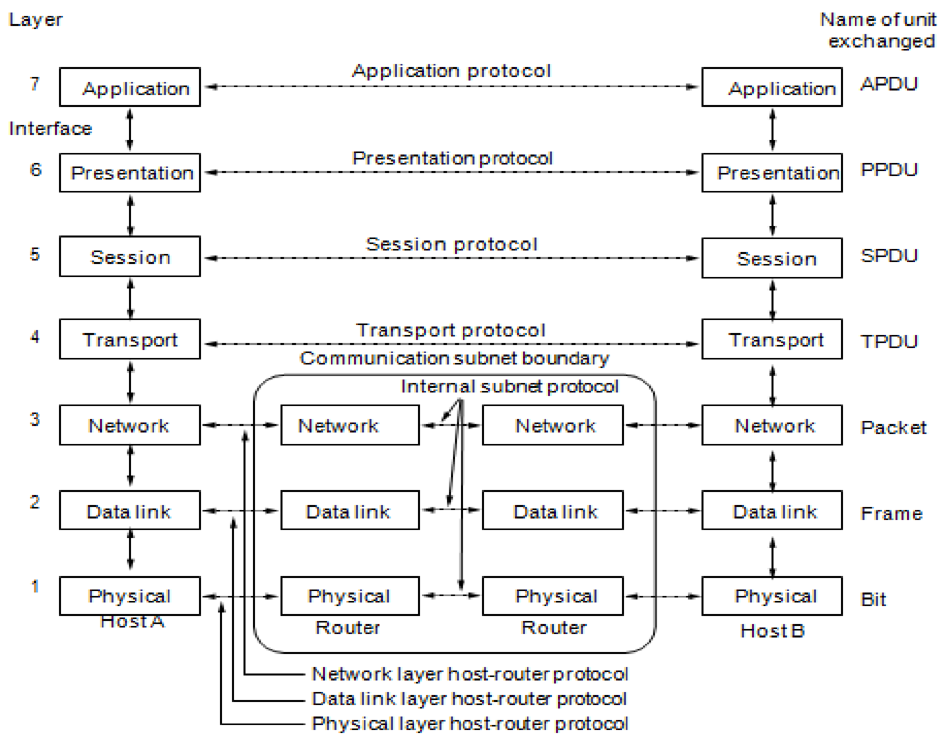


Figure 1-20. The OSI reference model.

The Physical Layer

- ❖ This **layer** is concerned with transmitting raw bits sequence of 0’s and 1’s over a communication channel.
- ❖ The design issues are deal with mechanical, electrical, and timing interfaces, as well as the physical transmission medium, which lies below the physical layer.

The Data Link Layer

- ❖ This layer transforms a raw transmission facility into a line that appears free of undetected transmission errors.
- ❖ It accomplishes this task by having the sender break up the input data into **data frames** (typicallya few hundred or a few thousand bytes) and transmits the frames sequentially.
- ❖ If the service is reliable, the receiver confirms correct receipt of each frame by send- ing back an **acknowledgement frame**.
- ❖ Another issue in the data link layer is how to keep a fast transmitter from drowning a slow receiver in data. Some traffic regulation mechanisms are used.
- ❖ **Medium access control** sub layer deals with how to control access to the shared channel.

The Network Layer

- ❖ Controls the operation of the subnet.
- ❖ A key design issue is determining how packets are routed from 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.
- ❖ If too many packets are present in the subnet at the same time, they will get in one another’s way,

forming bottlenecks. Handling congestion is also a responsibility of the network layer.

- Heterogeneous networks to be interconnected.

The Transport Layer

- It 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.
- It also determines what type of service to provide to the session layer, ultimately, to the users of the network.
- The most popular type of transport connection is an error-free point-to-point channel that delivers messages or bytes in the order in which they were sent.
- It also provides the service of transporting of isolated messages with no guarantee about the order of delivery, and the broadcasting of messages to multiple destinations.
- 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

- It allows users on different machines to establish sessions between them.
- Sessions offer various services, including dialog control (keeping track of whose turn it is to transmit), token management(preventing two parties from attempting the same critical operation simultaneously), and synchronization (check pointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery).

The Presentation Layer

- **This layer** is concerned with the syntax and semantics of the information transmitted.
- In order to make it possible for computers with different internal data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used ‘‘on the wire.’’
- 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

- **It c**ontains a variety of protocols that are commonly needed by users.
- One widely used application protocol is **HTTP** (**HyperText Transfer Protocol**), which is the basis for the World Wide Web. When a browser wants a Web page, it sends the name of the page it wants to the server hosting the page using HTTP. The server then sends the page back.
- Other application protocols are used for file transfer, electronic mail, and network news.

The TCP/IP Reference Model

- This reference Model is a four-layered suite of communication protocols, developed by the DoD

(Department of Defence) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP.

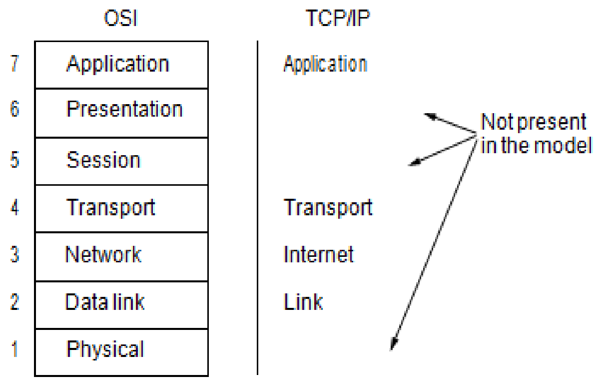


Figure 1-21. The TCP/IP reference model.

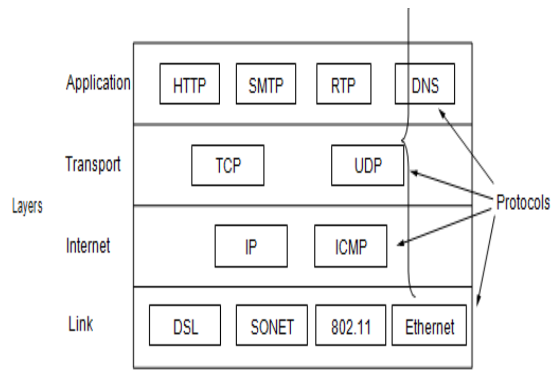


Figure 1-22. The TCP/IP model with some protocols we will study.

The Link Layer

- ❖ It describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer.
- ❖ It is not really a layer at all, in the normal sense of the term, but rather an interface between hosts and transmission links.

The Internet Layer

- ❖ Its job is to permit hosts to inject packets into any network and have they travel independently to the destination.
- ❖ Packet may arrive in a completely different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired.
- ❖ This 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 job of the internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly a major issue here, as is congestion (though IP has not proven effective at avoiding congestion).

The Transport Layer

- ❖ It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer.
- ❖ Two end-to-end transport protocols have been defined here TCP,UDP.
- ❖ **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.
- ❖ It segments the incoming byte stream into discrete messages and passes each one on to the internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream.
- ❖ TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more

messages than it can handle.

- ❖ 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.
- ❖ It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video.

The Application Layer

- ❖ It contains all the higher-level protocols. The file transfer (FTP), and electronic mail (SMTP). Domain Name System (DNS), for mapping host names onto their net- work addresses, HTTP, the protocol for fetching pages on the World Wide Web, RTP, the protocol for delivering real-time media such as voice or movies.

A Comparison of the OSI and TCP/IP Reference Models

- ❖ Three concepts are central to the OSI model:

1. **Services:** It tells layer's semantics, what the layer does, not how entities above it access it or how the layer works.
2. **Interfaces:** It specifies what the parameters are and what results to expect.
3. **Protocols:** provides the offered services.

- ❖ The TCP/IP model did not originally clearly distinguish between services, interfaces, and protocols, although people have tried to retrofit it after the fact to make it more OSI-like.
- ❖ The protocols in the OSI model are better hidden than in the TCP/IP model and can be replaced relatively easily as the technology changes.
- ❖ As a consequence, the proto- cols in the OSI model are better hidden than in the TCP/IP model and can be replaced relatively easily as the technology changes.
- ❖ With TCP/IP the reverse was true: the protocols came first, and the model was really just a description of the existing protocols. There was no problem with the protocols fitting the model.
- ❖ The OSI model has seven layers and the TCP/IP model has four. Both have (inter)network, transport, and application layers, but the other layers are different.
- ❖ The OSI model supports both connectionless and connection- oriented communication in the network layer, but only connection-oriented communication in the transport layer, where it counts
- ❖ The TCP/IP model supports only one mode in the network layer (connectionless) but both in the transport layer, giving the users a choice.

PHYSICAL LAYER: GUIDED TRANSMISSION MEDIA

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.
- Although this method is not as sophisticated as using a geosynchronous communication satellite, it is often more cost effective, especially for applications in which high bandwidth or cost per bit transported is the key factor.
- An industry-standard Ultrium tape can hold 800 gigabytes. A box 60 □ 60 □ 60 cm can hold about 1000 of these tapes, for a total capacity of 800 terabytes, or 6400 terabits (6.4 petabits).
- A boxof tapes can be delivered anywhere in the United States in 24 hours by Federal Express and other companies. The effective bandwidth of this transmission is 6400 terabits/86,400 sec, or a bit over 70 Gbps.
- If the destination is only an hour away by road, the bandwidth is increased to over 1700 Gbps. No computer net- work can even approach this. Of course, networks are getting faster, but tape den- sities are increasing, too.
- The cost of an Ultrium tape is around $40 when bought in bulk. A tape can be reused at least 10 times , So the tape cost is maybe $4000 per box per usage.

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.
- Twisted pairs can run several kilometers without amplification, but for longer distances the signal becomes too attenuated and repeaters are needed.
- The bandwidth depends on the thickness of the wire and the distance traveled, but several megabits/sec can be achieved for a few kilometers in many cases.

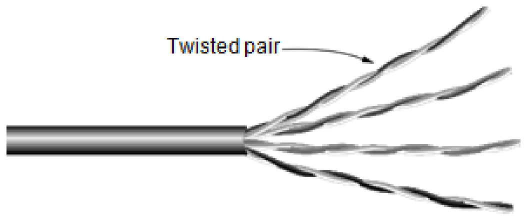


Figure 2-3. Category 5 UTP cable with four twisted pairs.

- ❖ Twisted-pair cabling comes in several varieties. A ''Cat 5"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.
- ❖ Links that can be used in both directions at the same time, like a two-lane road, are called **full-duplex** links.
- ❖ links that can be used in either direction, but only one way at a time, like a single-track railroad line are called **half-duplex** links.
- ❖ Links that allow traffic in only one direction, like a one-way street. They are called **simplex** links.
- ❖ Cat 5 replaced earlier Category 3 cables, 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 or even Category 7 has more stringent specifications to handle signals with greater band-widths.

3. **Coaxial Cable**

- ❖ It has better shielding and greater bandwidth than unshielded twisted pairs, so it can span longer distances at higher speed.
- ❖ There are two kinds, 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 construction and shielding of the coaxial cable give it a good combination of high bandwidth and excellent noise immunity. The bandwidth possible depends on the cable quality and length.
- ❖ Coaxial cables used to be widely used within the telephone system for long-distance lines but have now largely been replaced by fiber optics on long- haul routes. Coax is still widely used for cable television and metropolitan area networks, however.

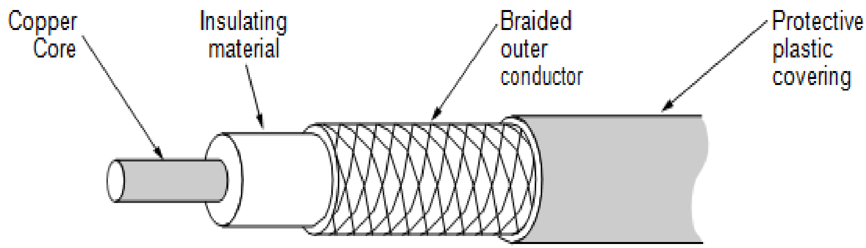


Figure 2-4. A coaxial cable.

4. **Power Lines**

- Power lines deliver electrical power to houses, and electrical wiring within houses distributes the power to electrical outlets. Its been used by electricity companies for low-rate communication such as re- mote metering for many years, as well in the home to control devices.
- Simply plug a TV and a receiver into the wall, which you must do anyway because they need power, and they can send and receive movies over the electrical wiring.
- The difficulty with using household electrical wiring for a network is that it was designed to distribute power signals.
- Electrical signals are sent at 50–60 Hz and the wiring attenuates the much higher frequency (MHz) signals needed for high-rate data communication.
- Transient currents when appliances switch on and off create electrical noise over a wide range of frequencies.
- Despite these difficulties, it is practical to send at least 100 Mbps over typical household electrical wiring by using communication schemes that resist impaired frequencies and bursts of errors.

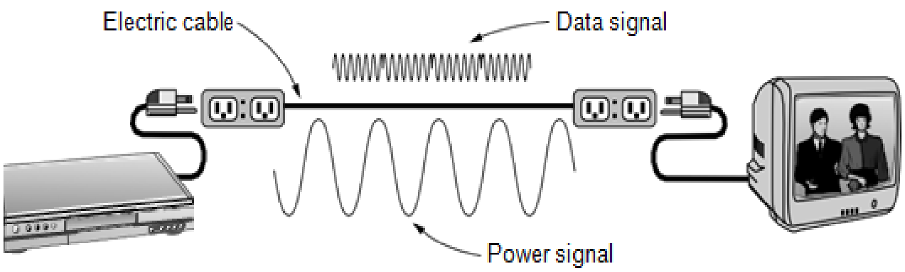


Figure 2-5. A network that uses household electrical wiring.

5. **Fiber Optics**

- In contrast, the achievable bandwidth with fiber technology is in excess of 50,000 Gbps (50 Tbps) and we are nowhere near reaching these limits.
- The current practical limit of around 100 Gbps is due to our inability to convert between electrical and opti- cal signals any faster.
- Fiber optics are used for long-haul transmission in network backbones, high-speed LANs 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.

- Conventionally, a pulse of light indicates a 1 bit and the absence of light indicates a 0 bit. The transmission medium is an ultra-thin fiber of glass. The detector generates an electrical pulse when light falls on it.

Transmission of Light through Fiber:

Optical fibers are made of glass, which, in turn, is made from sand, an in expensive raw material available in unlimited amounts.

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 coreis 8 to 10 microns.

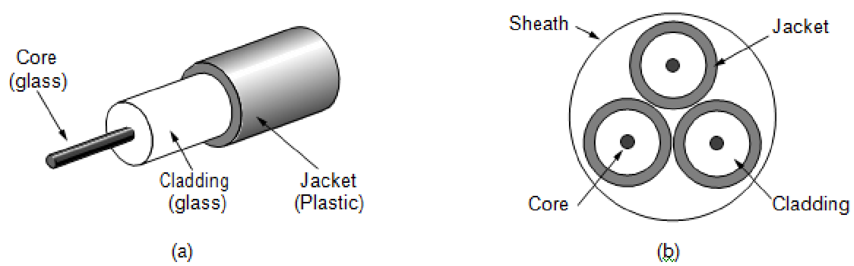


Figure 2-8. (a) Side view of a single fiber. (b) End view of a sheath with three fibers.

- 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.

WIRELESS TRANSMISSION

The Electromagnetic Spectrum

- When electrons move, they create electromagnetic waves that can propagate through space . These waves were predicted by the British physicist James Clerk Maxwell in 1865 and first observed by the German physicist Heinrich Hertz in 1887.
- 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** □ (lambda).
- When an antenna of the appropriate size is attached to an electrical circuit, the electromagnetic waves can be broadcast efficiently and received by a receiver some distance away.
- In a vacuum, all electromagnetic waves travel at the same speed, no matter what their frequency as called **speed of light**, *c*, is approximately 3 □ 10^8 m/sec, or about 1 foot (30 cm) per nanosecond.
- The fundamental relation between *f*, □, and *c* (in a vacuum) is □*f* □*c*

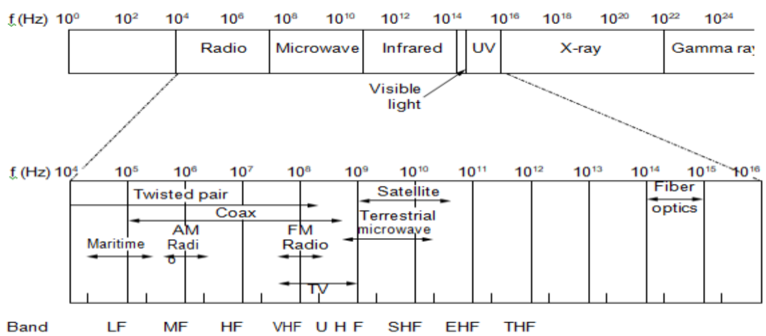


Figure 2-10. The electromagnetic spectrum and its uses for communication.

- In **frequency hopping spread spectrum**, the transmitter hops from frequency to frequency hundreds of times per second. It is popular for military communication because it makes transmissions hard to detect and next to impossible to jam.
- **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.

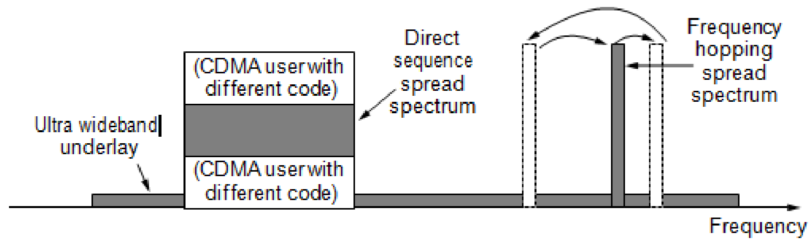


Figure 2-11. Spread spectrum and ultra-wideband (UWB) communication.

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 omnidirectional, 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—as the signal energy is spread more thinly over a larger surface. This attenuation is called **path loss**.

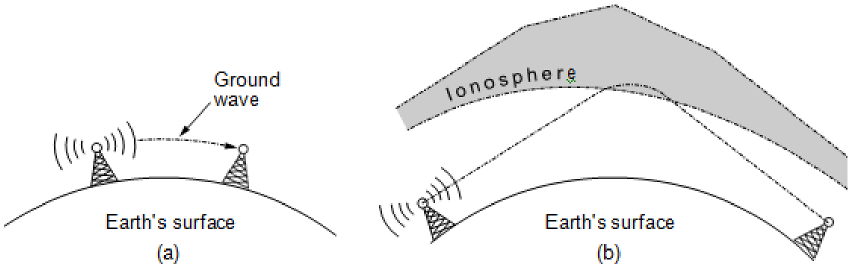


Figure 2-12. (a) In the VLF, LF, and MF bands, radio waves follow the curvature of the earth. (b) In the HF band, they bounce off the ionosphere.

Microwave Transmission

- Before fiber optics, for decades these microwaves formed the heart of the long-distance tele- phone transmission system.
- In fact, MCI, one of AT&T's first competitors after it was deregulated, built its entire system with microwave communications passing between towers tens of kilometers apart. Even the company's name reflected this (MCI stood for Microwave Communications, Inc.).
- Microwaves travel in a straight line, so if the towers are too far apart, the earth will get in the way.
- Unlike radio waves at lower frequencies, microwaves do not pass through buildings well. In addition, even though the beam may be well focused at the transmitter, there is still some divergence in space.
- The demand for more and more spectrum drives operators to yet higher frequencies. Bands up to 10 GHz are now in routine use, but at about 4 GHz a new problem sets in: absorption by water.
- Microwave communication is so widely used for long-distance telephone communication, mobile phones, television distribution, and other pur- poses that a severe shortage of spectrum has developed.
- Microwave is also relatively inexpensive. Putting up two simple towers and putting antennas on each one may be cheaper than burying 50 km of fiber through a congested urban area or up over a mountain, and it may also be cheaper than leasing the telephone company's fiber,

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.
- On the other hand, the fact that infrared waves do not pass through solid walls well is also a plus. It means that an infrared system in one room of a building will not interfere with a similar system in adjacent rooms or buildings: you cannot control your neighbor's television with your remote control.
- Furthermore, security of infrared systems against eavesdropping is better than that of radio systems precisely for this reason.

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

Light Transmission

- Unguided optical signaling or free-space optics has been in use for centuries.

- Optical signaling using lasers is inherently unidirectional, so each end needs its own laser and its own Photodetector. This scheme offers very high bandwidth at very low cost and is relatively secure because it is difficult to tap a narrow laser beam.
- The laser's strength, a very narrow beam, is also its weakness here. Aiming a laser beam 1 mm wide at a target the size of a pin head 500 meters away requires the marksmanship of a latter-day Annie Oakley.

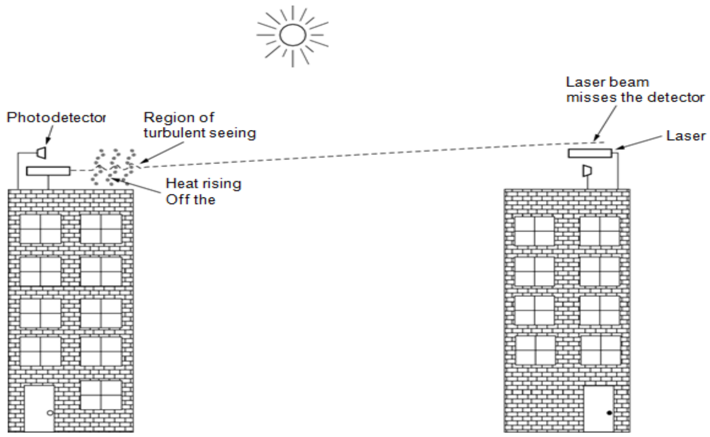


Figure 2-14. Convection currents can interfere with laser communication systems. A bidirectional system with two lasers is pictured here.

- To add to the difficulty, wind and temperature changes can distort the beam and laser beams also cannot penetrate rain or thick fog, although they normally work well on sunny days.
- Unguided optical communication may seem like an exotic networking technology today, but it might soon become much more prevalent.
- Communicating with visible light in this way is inherently safe and creates a low-speed network in the immediate vicinity of the display.