Dayananda Sagar Academy of Technology & Management

(An Autonomous Institute under VTU)

Opp. Art of Living, Udayapura, Kanakapura Road,Bangalore – 560082

Department of Information Science & Engineering

Accredited by NAAC A+ and Accredited by NBA, New Delhi

Academic Year: 2024-2025

Computer Networks -BCS502

Module-1: Introduction to Data Communications Notes

Dr. Rajesh L,

Associate Professor

ISE, DSATM

Module 1: Introduction to Networks

Syllabus:

Introduction: Data Communications, Networks, Network Types, Networks Models: Protocol Layering, TCP/IP Protocol suite, The OSI model, Introduction to Physical Layer: Transmission media, Guided Media, Unguided Media: Wireless. Switching: Packet Switching and its types.

Textbook: Behrouz A. Forouzan, Data Communications and Networking, Ch. 1.1 - 1.3, 2.1 - 2.3, 7.1 – 7.3, 8.3.

1.1 Data Communications

When we communicate, we are sharing information. This sharing can be local or remote. The term "Telecommunication" means communication at a distance. "Tele" in Greek means far. The term "data" refers to information presented whatever form is agreed upon by the parties creating and using data.

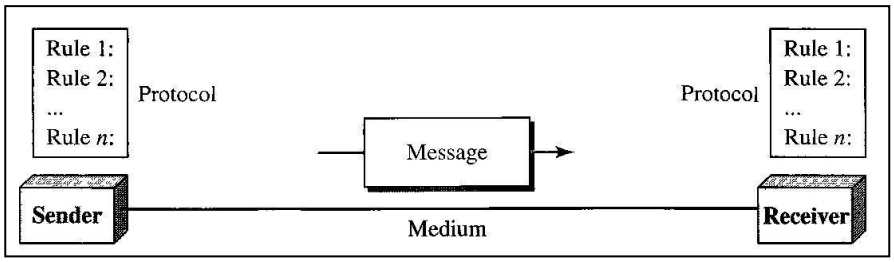
Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

The effectiveness of a data communications system depends on **four fundamental characteristics**

1. **Delivery**. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy**. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. **Timeliness**. The system must deliver data in a timely manner. Data delivered late are useless.
4. **Jitter**. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

Components

A data communications system has five components:



1. **Message**. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2. **Sender**. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. **Receiver**. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. **Transmission medium**. The transmission medium is the physical path by which a message travels from sender to receiver.

5. **Protocol**. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

Data Representation

Information today comes in different forms such as text, numbers, images, audio, and video.

Text

In data communications, text is represented as a bit pattern, a sequence of bits (0s or 1s). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world.

Numbers

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations.

Images

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution. After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the valueof the pattern depend on the image. There are several methods to represent color images. One method is called RGB, so calledbecause each color is made of a combination of three primary

colors: red, green, and blue.

Audio

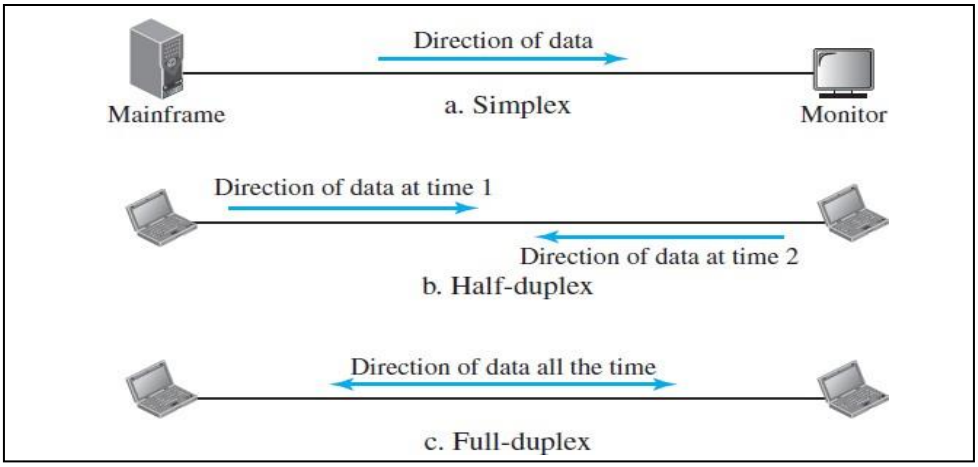
Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.

Video

Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex as shown in figure.



Simplex

- In simplex mode, the communication is unidirectional. Only one of the two devices on a link can transmit; the other can only receive.
- Keyboards and traditional monitors are examples of simplex devices.
- The simplex mode can use the entire capacity of the channel to send data in onedirection.

Half-Duplex

- In half-duplex mode, each station can both transmit and receive, but not at the same time.
- When one device is sending, the other can only receive, and vice versa.
- In a half-duplex transmission, the entire capacity of a channel is taken over by whicheverof the two devices is transmitting at the time.
- Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

- The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

Full-Duplex

- In full-duplex mode (also, called duplex), both stations can transmit and receive simultaneously.
- In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction.
- One common example of full-duplex communication is the telephone network. The full-duplex mode is used when communication in both directions is required all the time.

1.2 Networks

1.Network

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

2. Distributed Processing

A task is divided among multiple computers, instead of one single large machine being responsible for all aspects of a process; separate computers (usually a personal computer or workstation) handle a subset.

Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

1.Performance

- Performance can be measured in many ways, including transit time and response time.
- Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response.
- The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.
- Performance is often evaluated by two networking metrics: throughput and delay. We often need more throughput and less delay.

2. Reliability

In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

3. Security

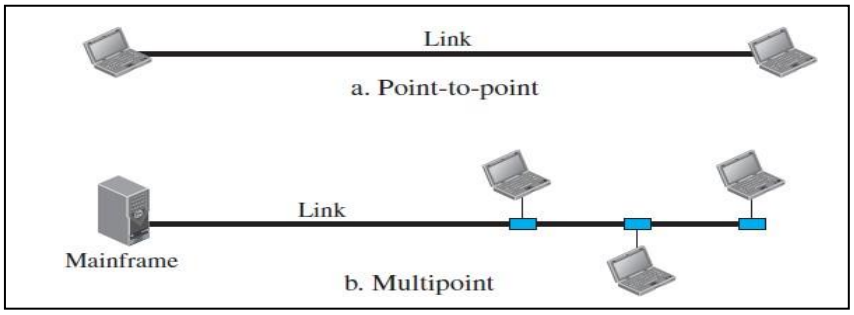
Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

1.3 Physical Structures

Types of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another.

1. Point-to-Point A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices.



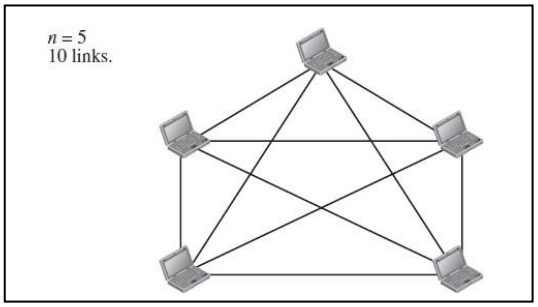
2. Multipoint A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally.

Physical Topology

- The term physical topology refers to the way in which a network is laid out physically.
- Two or more devices connect to a link; two or more links form a topology.

1. Mesh Topology

- In a mesh topology, every device has a dedicated point-to-point link to every other device.
- We need **n(n-1)** physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2.
- In other words, we can say that in a mesh topology, we need **n(n - 1) / 2** duplex-modelinks.



Advantages

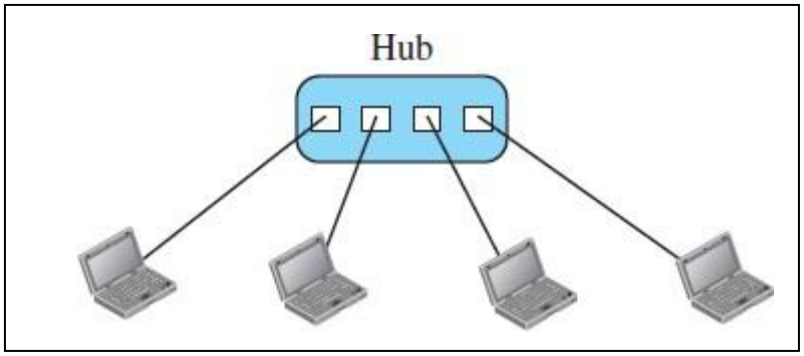
1. The use of dedicated links guarantees that each connection can carry its own data load.
2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
3. There is the advantage of privacy or security.
4. Point-to-point links make fault identification and fault isolation easy.

Disadvantages

1. Difficulty in installation and reconnection.
2. The sheer bulk of the wiring can be greater than the available space.
3. The hardware required will be expensive.

2. Star Topology

- Each device has a dedicated point-to-point link only to a central controller, usually calleda hub.
- The controller acts as a medium for exchange



Advantages:

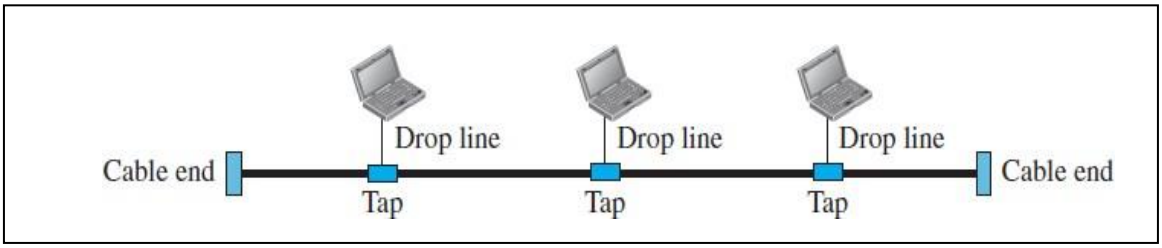
1. A star topology is less expensive than a mesh topology.
2. Other advantages include robustness. If one link fails, only that link is affected

Disadvantages:

1. If the hub goes down, the whole system is dead.
2. Each node must be linked to a central hub. More cabling is required.

3. Bus Topology

- A bus topology is multipoint.
- One long cable acts as a backbone to link all the devices in a network.



- Nodes are connected to the bus cable by drop lines and taps.
- As a signal travels along the backbone, some of its energy is transformed into heat. The
- It becomes weaker and weaker as it travels. Hence there is a limit on the number of taps and the distance between those taps.

Advantages:

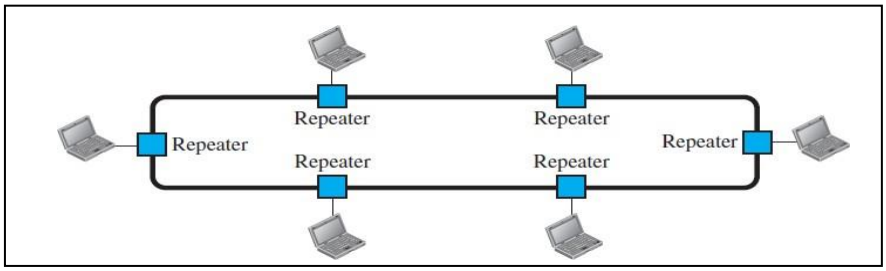
1. Advantages of a bus topology include ease of installation.
2. In a bus, redundancy is eliminated.

Disadvantages:

1. Difficult reconnection and fault isolation.
2. Signal reflection at the taps can cause degradation in quality.
3. A fault or break in the bus cable stops all transmission.

4. Ring Topology

- Each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reachesits destination.
- Each device in the ring incorporates a repeater, to regenerate the bits and passes them along.



Advantages:

1. A ring is relatively easy to install and reconfigure.
2. To add or delete a device requires changing only two connections.
3. In addition, fault isolation is simplified

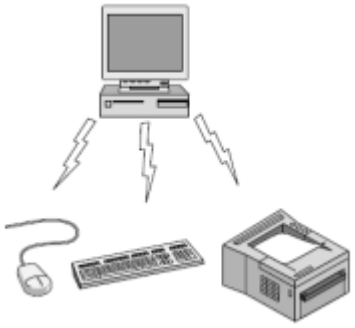
Disadvantages:

1. Unidirectional traffic can be a disadvantage.

1.4 Network Types

Personal Area Networks

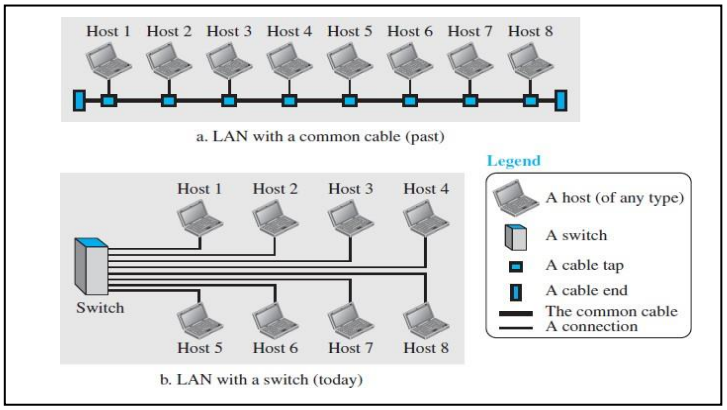
PANs (Personal Area Networks) let devices communicate over the range of a person. A common example is a wireless network that connects a computer with its peripherals. Almost every computer has an attached monitor, keyboard, mouse, and printer. Many new users have a hard time finding the right cables and plugging them into the right little holes (even though they are usually color coded) that most computer vendors offer the option of sending a technician to the user's home to do it. To help these users, some companies got together to design a short-range wireless network called Bluetooth to connect these components without wires.



In the simplest form, Bluetooth networks use the master-slave paradigm of Figure. 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.

Local Area Network

- A local area network (LAN) is usually privately owned and connects some hosts in a single office, building, or campus.
- Each host in a LAN has an identifier, an address that uniquely defines the host in the LAN.
- A packet sent by a host to another host carries both the source host's and the destination host's addresses.



- In the past, all hosts in a network were connected through a common. Today, most LANs use a smart connecting switch.

Metropolitan Area Networks

A MAN (Metropolitan Area Network) covers a city. The best-known examples of MANs are the 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. Recent developments in highspeed wireless Internet access have resulted in another MAN, which has been standardized as IEEE 802.16 and is popularly known as WiMAX.

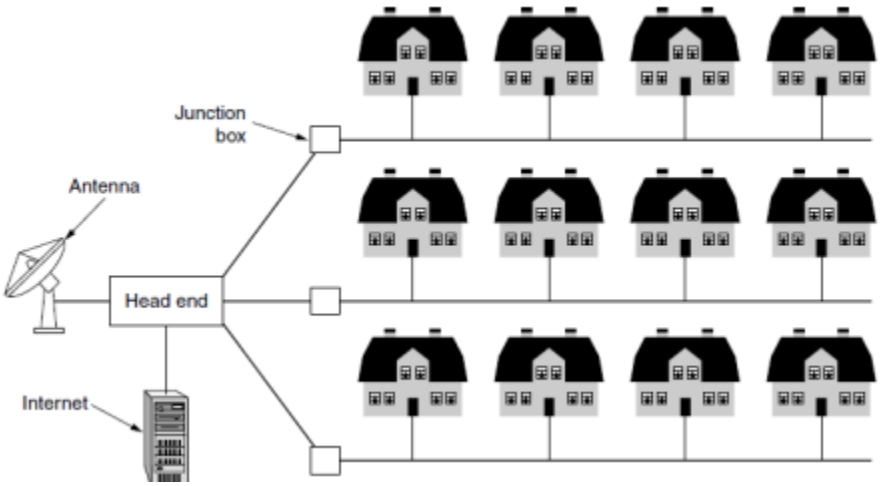


Figure. A metropolitan area network based on cable TV.

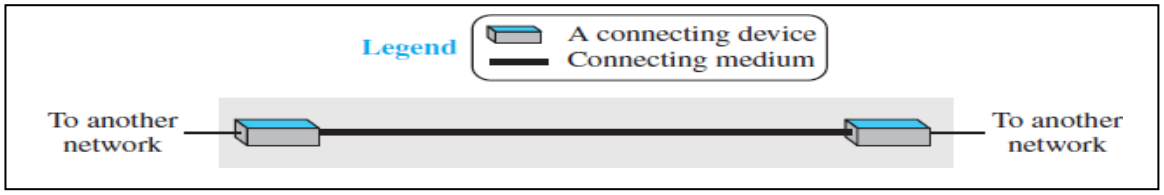
Wide Area Network

- A **wide area network (WAN)** is also an interconnection of devices capable of communication.
- A LAN is normally limited in size, spanning an office, a building, or a campus; a WANhas a wider geographical span, spanning a town, a state, a country, or even the world.
- WAN is normally created and run by communication companies and leased by an organization that uses it.
- We see two distinct examples of WANs today: point-to-point WANs and switchedWANs.

1. Point-to-Point WAN

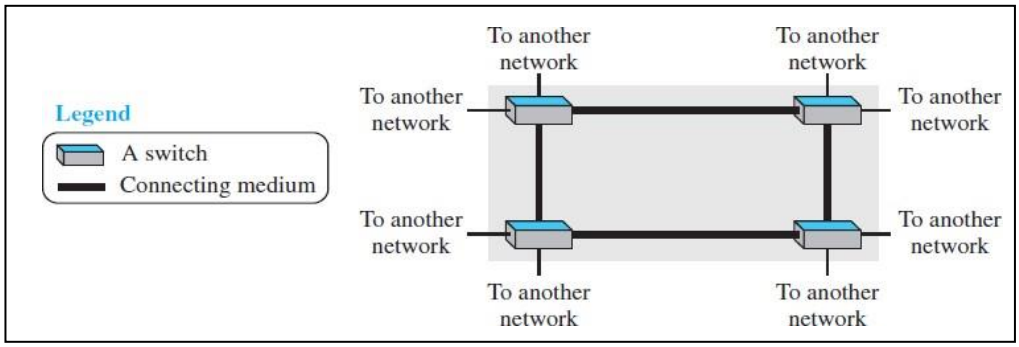
A point-to-point WAN is a network that connects two communicating devices through a

transmission media (cable or air).



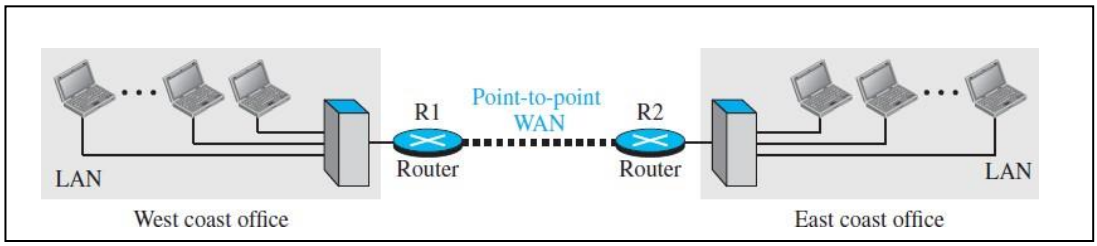
2. Switched WAN

- A switched WAN is a network with more than two ends.
- A switched WANis used in the backbone of global communication today.
- A switched WAN is a combination of several point-to-point WANs that are connected by switches.



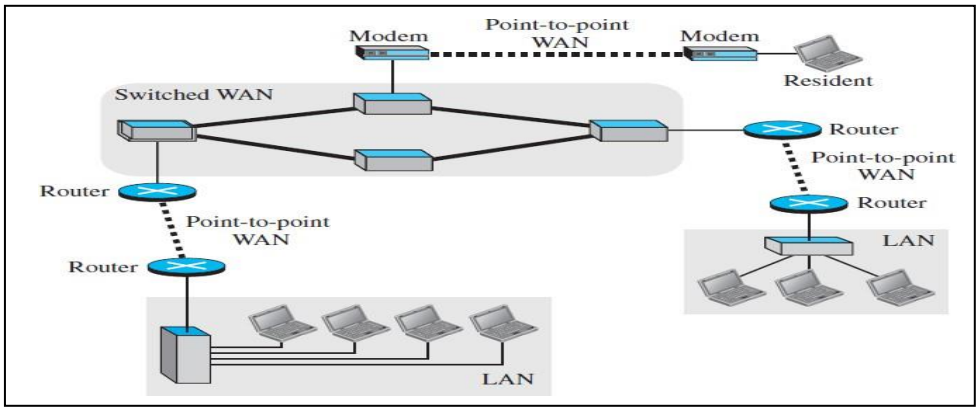
Internetwork

Today, it is very rare to see a LAN or a WAN in isolation; they are connected to one another. When two or more networks are connected, they make an **internetwork,** or **internet.**



When a host in the west coast office sends a message to another host in the same office, the router blocks the message, but the switch directs the message to the destination. On the other hand, when a host on the west coast sends a message to a host on the east coast, router R1 routes the packet to router R2, and the packet reaches the destination.

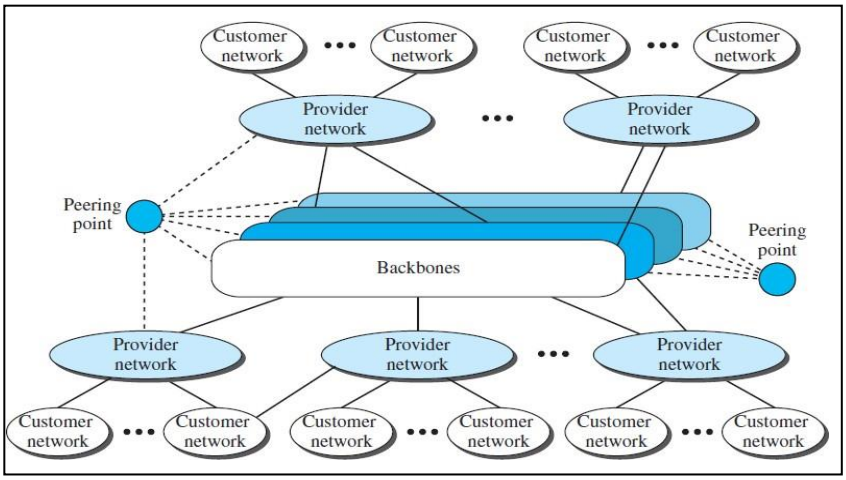
Figure shows another internet with several LANs and WANs connected. One of the WANs is a switched WAN with four switches.



The Internet

- An internet (note the lowercase *i*) is two or more networks that can communicate with each other. The most notable internet is called the **Internet** (uppercase *I)*, and is composed of thousands of interconnected networks.
- Figure shows a conceptual (not geographical) view of the Internet. The figure shows the Internet as several backbones, provider networks, and customer networks.
- At the top level, the *backbones* are large networks owned by some communication companies such as Sprint, Verizon (MCI), AT&T, and NTT. The backbone networks are connected through some complex switching systems, called ***peering points*.**
- At the second level, there are smaller networks, called ***provider networks*** that use the services of the backbones for a fee. The provider networks are connected to backbones and sometimes to other provider networks. The ***customer networks*** are networks at the edge of the Internet that actually use the services provided by the Internet. They pay fees to provider networks for receiving services.

- Backbones and provider networks are also called **Internet Service Providers (ISPs).** The backbones are often referred to as ***international ISPs;*** the provider networks are often referred to as ***national* or *regional ISPs*.**



Accessing the Internet

The Internet today is an internetwork that allows any user to become part of it. The user, however, needs to be physically connected to an ISP. The physical connection is normally done through a point-to-point WAN.

1. ***Using Telephone Networks***

Today most residences and small businesses have telephone service, which means they are connected to a telephone network. Since most telephone networks have already connected themselves to the Internet, one option for residences and small businesses to connect to the Internet is to change the voice line between the residence or business and the telephone center to a point-to-point WAN. This can be done in two ways.

A. ***Dial-up service.*** The first solution is to add to the telephone line a modem that converts data to voice. The software installed on the computer dials the ISP and imitates making a telephone connection. Unfortunately, the dial-up service is very slow, and when the line is used for Internet connection, it cannot be used for telephone (voice) connection. It is only useful for small residences.

B. ***DSL Service.*** Since the advent of the Internet, some telephone companies have upgraded their telephone lines to provide higher speed Internet services to residences or small businesses. The DSL service also allows the line to be used simultaneously for voice and data communication.

2. ***Using Cable Networks***

More and more residents over the last two decades have begun using cable TV services instead of antennas to receive TV broadcasting. The cable companies have been upgrading their cable networks and connecting to the Internet. A residence or a small business can be connected to the Internet by using this service. It provides a higher speed connection, but the speed varies depending on the number of neighbors that use the same cable.

3. ***Using Wireless Networks*** Wireless connectivity has recently become increasingly popular. A household or a small business can use a combination of wireless and wired connections to access the Internet. With the growing wireless WAN access, a household or a small business can be connected to the Internet through a wireless WAN.

4. ***Direct Connection to the Internet***

A large organization or a large corporation can itself become a local ISP and be connected to the Internet. This can be done if the organization or the corporation leases ahigh-speed WAN from a carrier provider and connects itself to a regional ISP. For example, a large university with several campuses can create an internetwork and then connect the internetwork to the Internet.

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

1.5 Networks Models

Protocol Layering

In data communication and networking, a protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively.

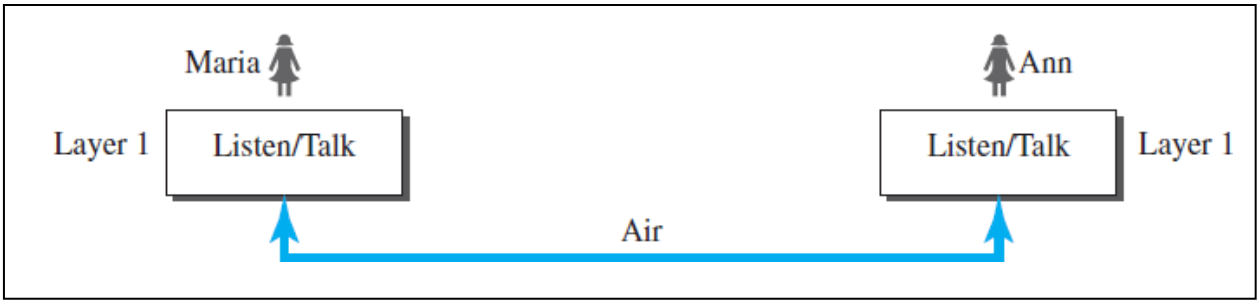
- When communication is simple, we may need only one simple protocol;
- When the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or **protocol layering.**

Scenarios

Let us develop two simple scenarios to better understand the need for protocol layering.

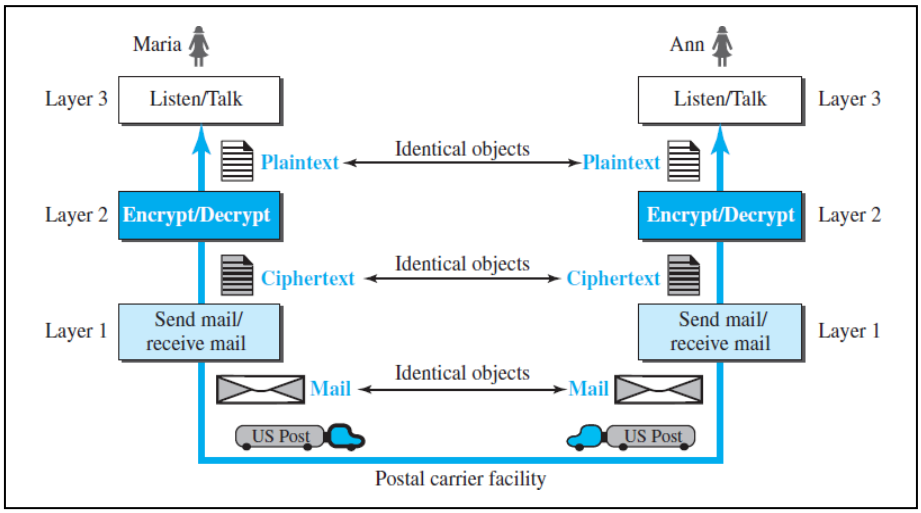
First Scenario

In the first scenario, communication is so simple that it can occur in only one layer. Assume Maria and Ann are neighbors with a lot of common ideas. Communication between Maria and Ann takes place in one layer, face to face, in the same language, as shown in Figure.



Second Scenario

- In the second scenario, it is assumed that the two friends are located in different cities. They decide to continue their conversation using regular mail through the post office.
- They agree on an encryption/decryption technique to avoid intervention.
- The sender of the letter encrypts it to make it unreadable by an intruder; the receiver of the letter decrypts it to get the original letter
- We assume that Ann and Maria each have three machines (or robots) that can performthe task at each layer.



Sender Side

- Let us assume that Maria sends the first letter to Ann.
- Maria talks to the machine at the third layer as though the machine is Ann and is listening to her. The third layer machine listens to what Maria says and creates the plaintext (a letter in English), which is passed to the second layer machine.
- The second layer machine takes the plaintext, encrypts it, and creates the cipher text, which is passed to the first layer machine.
- The first layer machine, presumably a robot, takes the cipher text, puts it in an envelope, adds the sender and receiver addresses, and mails it.

Receiver Side

- At Ann's side, the first layer machine picks up the letter from Ann's mail box, recognizing the letter from Maria by the sender address. The machine takes out the ciphertext from the envelope and delivers it to the second layer machine.

- The second layer machine decrypts the message, creates the plaintext, and passes the plaintext to the third-layer machine.
- The third layer machine takes the plaintext and reads it as though Maria is speaking.

One of the advantages of protocol layering is that it allows us to separate the services from the implementation.

Another advantage of protocol layering is that communication does not always use only two end systems; there are intermediate systems that need only some layers, but not all layers.

Principles of Protocol Layering

First Principle

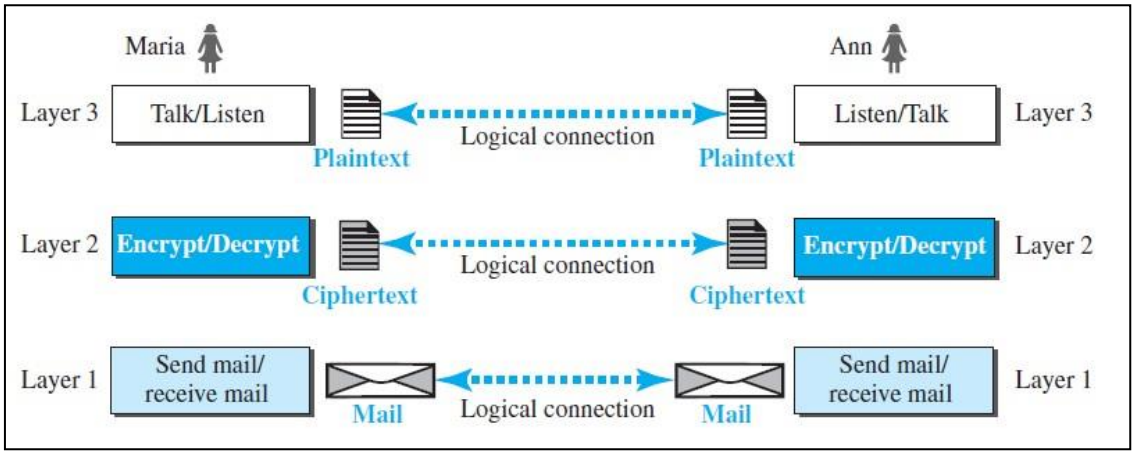
The first principle dictates that if we want bidirectional communication, each layer should be able to perform two opposite tasks, one in each direction.

Second Principle

The second principle that we need to follow in protocol layering is that the two objects under each layer at both sites should be identical.

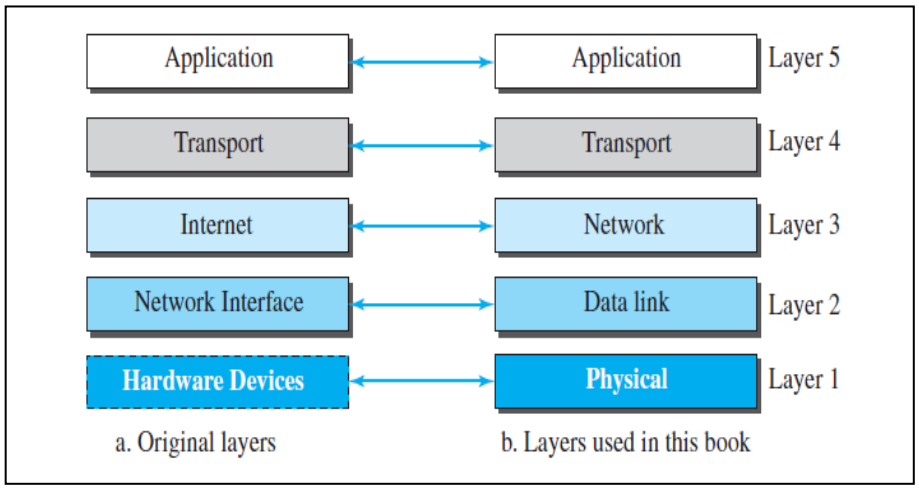
Logical Connections

Logical connection between each layer will be as shown in Figure. This means that we have layer-to-layer communication.



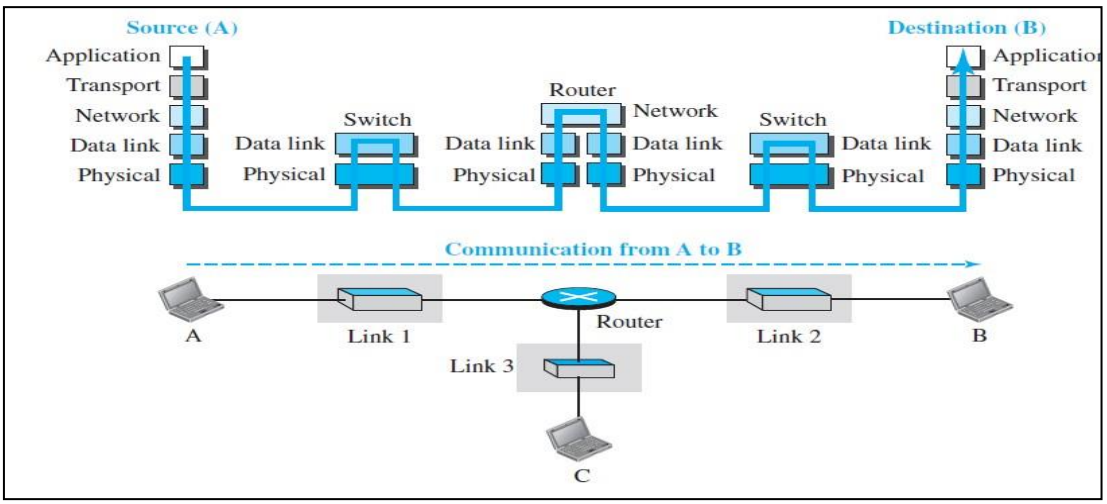
TCP/IP PROTOCOL SUITE

- TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today.
- It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality.
- The term *hierarchical* means that each upper level protocol is supported by the services provided by one or more lower level protocols.
- TCP/IP is thought of as a five-layer model. Figure shows configurations.



Layered Architecture

To show how the layers in the TCP/IP protocol suite are involved in communication between two hosts, we assume that we want to use the suite in a small internet made up of three LANs (links), each with a link-layer switch. We also assume that the links are connected by one router, as shown in Figure.



- Let us assume that computer A communicates with computer B. As the figure shows, we have five communicating devices in this communication: source host(computer A), the link-layer switch in link 1, the router, the link-layer switch in link 2,and the destination host (computer B).

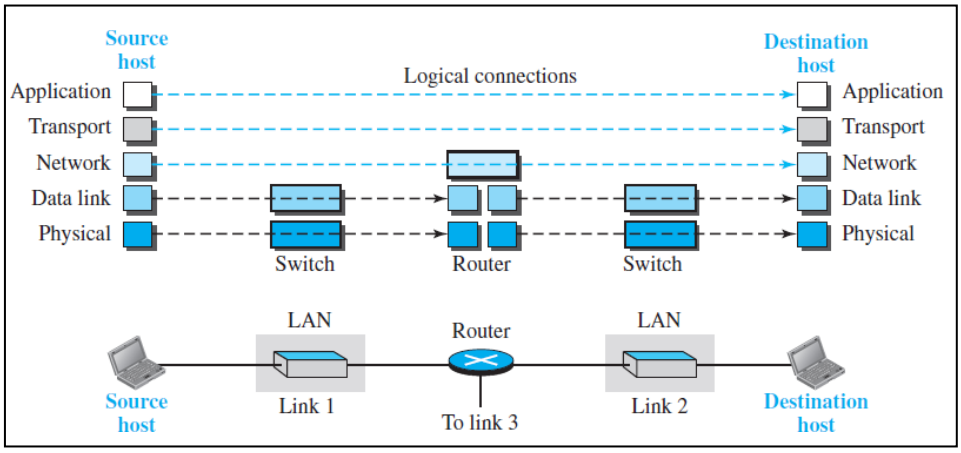
- The two hosts are involved in all five layers; the source host needs to create a message in the application layer and send it down the layers so that it is physically sent to the destination host. The destination host needs to receive the communication at the physical layer and then deliver it through the other layers to the application layer.

- The router is involved in only three layers; there is no transport or application layer in a router as long as the router is used only for routing. Although a router is always involved in one network layer, it is involved in *n* combinations of link and physical layers in which*n* is the number of links the router is connected to. The reason is that each link may use its own data-link or physical protocol.

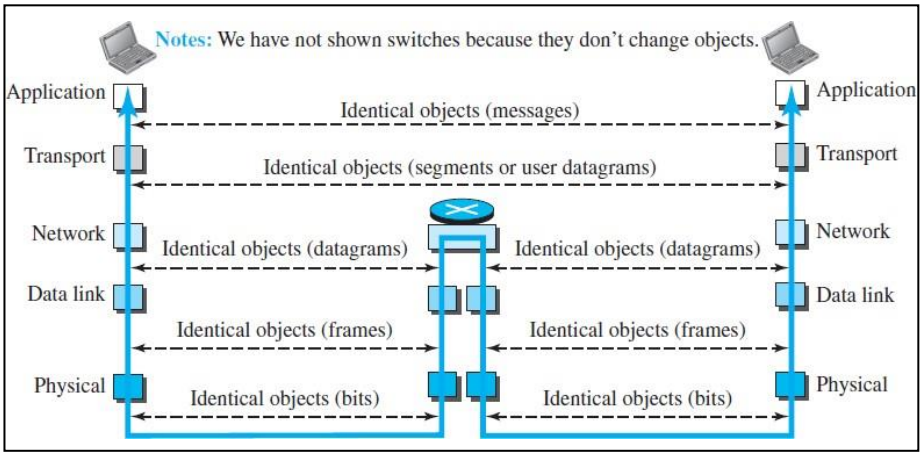
- A link-layer switch in a link, however, is involved only in two layers, data-link and physical.

Layers in the TCP/IP Protocol Suite

Figure shows logical connections in our simple internet.



- The duty of the application, transport, and network layers is end-to-end. However, the duty of the data-link and physical layers is hop-to-hop, in which a hop is a host or router.
- In the top three layers, the data unit (packets) should not be changed by any router or link-layer switch. In the bottom two layers, the packet created by the host is changed onlyby the routers, not by the link-layer switches.
- Figure shows the second principle discussed previously for protocol layering. We show the identical objects below each layer related to each device.



Description of Each Layer

Physical Layer

- The physical layer is responsible for carrying individual bits in a frame across the link.
- The communication between two devices at the physical layer is still a logical communication because there is another, hidden layer, the transmission media, under the physical layer.

- Two devices are connected by a transmission medium (cable or air).
- The transmission medium does not carry bits; it carries electrical or optical signals. So, the bits received in a frame from the data-link layer are transformed and sent through the transmission media.

Data-link Layer

- The data-link layer is responsible for moving the packet through the link.
- TCP/IP does not define any specific protocol for the data-link layer. It supports all the standard and proprietary protocols.
- The data-link layer takes a datagram and encapsulates it in a packet called a *frame*.
- Each link-layer protocol may provide a different service.
- Some link-layer protocols provide complete error detection and correction, some provideonly error correction.

Network Layer

- The network layer is responsible for creating a connection between the source computer and the destination computer.
- The network layer is responsible for host-to-host communication and routing the packet through possible routes.
- The network layer in the Internet includes the main protocol, Internet Protocol (IP) that defines the format of the packet, called a datagram at the network layer. IP also defines the format and the structure of addresses used in this layer. IP is also responsible for routing a packet from its source to its destination.
- IP is a connectionless protocol that provides no flow control, no error control, and no congestion control services.
- The network layer also includes unicast (one-to-one) and multicast (one-to-many) routing protocols.
- A routing protocol does not take part in routing (it is the responsibility of IP),but it creates forwarding tables for routers to help them in the routing process.
- The network layer also has some auxiliary protocols that help IP in its delivery and routing

tasks.

1. The Internet Control Message Protocol (ICMP) helps IP to report some problems when routing a packet.
2. The Internet Group Management Protocol (IGMP) is another protocol that helps IP in multitasking.
3. The Dynamic Host Configuration Protocol (DHCP) helps IP to get the network-layer address for a host.
4. The Address Resolution Protocol (ARP) is a protocol that helps IP to find the link-layer address of a host or a router when its network-layer address is given.

Transport Layer

- The logical connection at the transport layer is also end-to-end.
- The transport layer at the source host gets the message from the application layer, encapsulates it in a transport layer packet (called a *segment* or a *user datagram* in different protocols) and sends it, through the logical (imaginary) connection, to the transport layer at the destination host.
- There are a few transport-layer protocols in the Internet, each designed for some specific task.
- The main protocol, Transmission Control Protocol (TCP), is a connection-oriented protocol that first establishes a logical connection between transport layers at two hosts before transferring data.
- It creates a logical pipe between two TCPs for transferring a stream of bytes.
- TCP provides flow control, error control, and congestion control to reduce the loss of segments due to congestion in the network.
- The other common protocol, User Datagram Protocol (UDP), is a connectionless protocolthat transmits user datagrams without first creating a logical connection.
- A new protocol, Stream Control Transmission Protocol (SCTP) is designed to respond to new applications that are emerging in the multimedia.

Application Layer

- As Figure shows, the logical connection between the two application layers is end to-end.

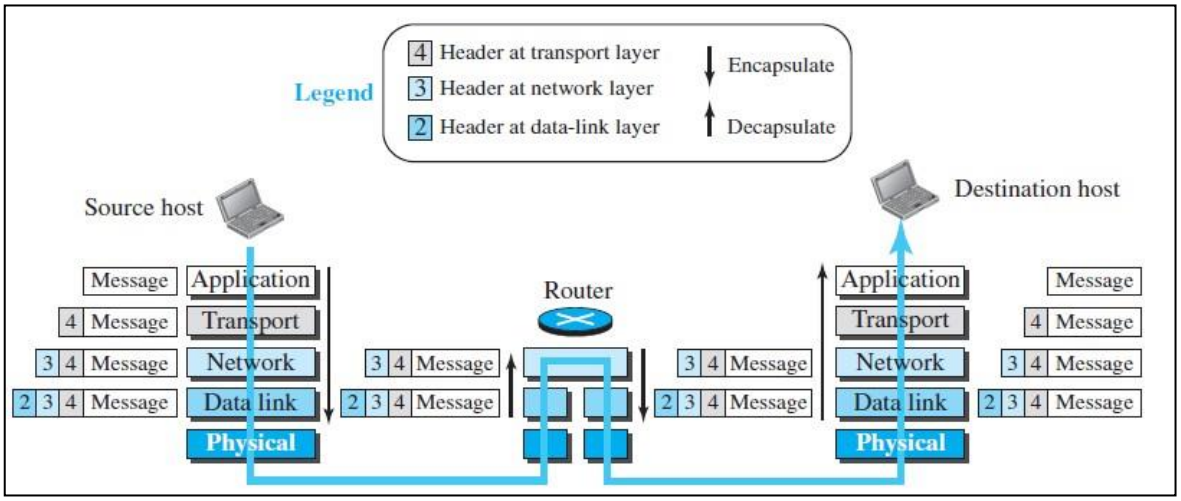
- Communication at the application layer is between two *processes.*
- To communicate, a process sends a request to the other process and receives a response.

  Process-to-process communication is the duty of the application layer.
- The application layer in the Internet includes many predefined protocols, but a user can also create a pair of processes to be run at the two hosts.

1. The Hypertext Transfer Protocol (HTTP) is a vehicle for accessing the World Wide Web (WWW).
2. The Simple Mail Transfer Protocol (SMTP) is the main protocol used in electronic mail (e-mail) service.
3. The File Transfer Protocol (FTP) is used for transferring files from one host to another.
4. The Terminal Network (TELNET) and Secure Shell (SSH) are used for accessinga site remotely.
5. The Simple Network Management Protocol (SNMP) is used by an administrator to manage the Internet at global and local levels.
6. The Domain Name System (DNS) is used by other protocols to find the network-layer address of a computer.
7. The Internet Group Management Protocol (IGMP) is used to collect membership in a group.

Encapsulation and Decapsulation

One of the important concepts in protocol layering in the Internet is encapsulation/decapsulation.



Encapsulation at the Source Host

At the source, we have only encapsulation.

- At the application layer, the data to be exchanged is referred to as a *message*. The message is passed to the transport layer.
- The transport layer takes the message as the payload and adds the transport layer header to the payload, which contains the identifiers of the source and destination application programs, plus some more information that is needed for the end-to end delivery of the message, such as flow, error control, or congestion control. The result is the transport- layer packet, which is called the *segment* (in TCP) and the *user datagram* (in UDP).
- The transport layer then passes the packet to the network layer.
- The network layer takes the transport-layer packet as data or payload and adds its own header to the payload.
- The header contains the addresses of the source and destination hosts and some more information used for error checking of the header, fragmentation information, and so on.
- The result is the network-layer packet, called a *datagram*. The network layer then passes the packet to the data-link layer.
- The data-link layer adds its own header, which contains the link-layer addresses of the host or the next hop (the router). The result is the link-layer packet, which is called a *frame*. The frame is passed to the physical layer for transmission.

Decapsulation and Encapsulation at the Router

At the router, we have both decapsulation and encapsulation because the router is connected to two or more links.

- After the set of bits are delivered to the data-link layer, this layer decapsulates the datagram from the frame and passes it to the network layer.
- The network layer only inspects the source and destination addresses in the datagram header and consults its forwarding table to find the next hop to which the datagram is to be delivered.
- The datagram is then passed to the data-link layer of the next link. The data-link layer of the next link encapsulates the datagram in a frame and passes it to the physical layer for transmission.

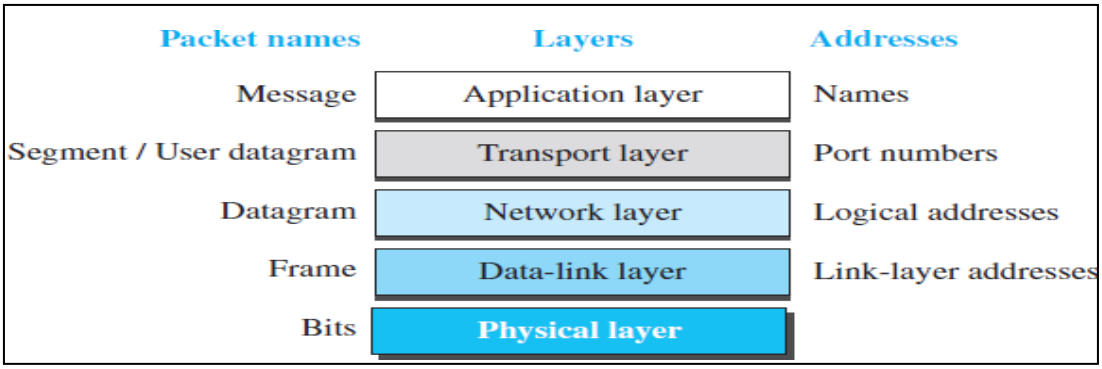
Decapsulation at the Destination Host

At the destination host, each layer encapsulates the packet received and delivers the payload to the next-higher layer protocol until the message reaches the application layer. It is necessary to say that decapsulation in the host involves error checking.

Addressing

- Any communication that involves two parties needs two addresses: source address and destination address.

- Although it looks as if we need five pairs of addresses, one pair per layer, we normally have only four because the physical layer does not need addresses; the unit of data exchange at the physical layer is a bit, which definitely cannot have an address.

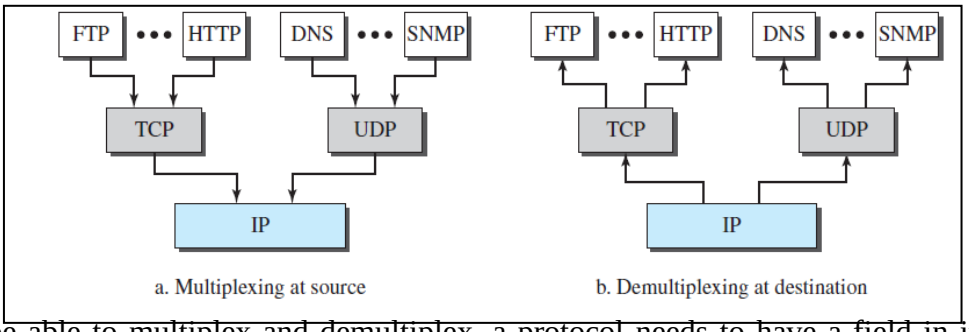


- Figure shows the addressing at each layer

1. At the application layer, we normally use names to define the site that provides services, such as *someorg.com*, or the e-mailaddress, such as *somebody@coldmail.com*.
2. At the transport layer, addresses are called port numbers, and these define the application-layer programs at the source anddestination. Port numbers are local addresses that distinguish between several programs running at the same time.
3. At the network-layer, the addresses are global, with the whole Internet as the scope.
4. The link-layer addresses, sometimes called MAC addresses, are locally defined addresses, each of which defines a specific host or router in a network(LAN or WAN).

Multiplexing and Demultiplexing

- Since the TCP/IP protocol suite uses several protocols at some layers, we can say that we have multiplexing at the source and demultiplexing at the destination.
- Multiplexing in this case means that a protocol at a layer can encapsulate a packet from several next-higher layer protocols (one at a time).
- Demultiplexing means that a protocol can decapsulate and deliver a packet to several next-higher layer protocols (one at a time).



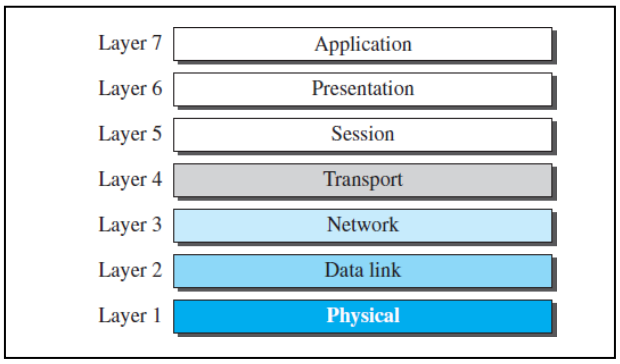
- To be able to multiplex and demultiplex, a protocol needs to have a field in its header to identify to which protocol the encapsulated packets belong.
- At the transport layer, either UDP or TCP can accept a message from several application-layer protocols.
- At the network layer, IP can accept a segment from TCP or a user datagramfrom UDP. IP can also accept a packet from other protocols such as ICMP, IGMP, and so on.
- At the data-link layer, a frame may carry the payload coming from IP or other protocolssuch as ARP

THE OSI MODEL

- Established in 1947, the**International Organization for Standardization (ISO)** is a multinational bodydedicated to worldwide agreement on international standards.
- An ISO standard that covers allaspects of network communications is the **Open Systems Interconnection (OSI)model.**
- It was first introduced in the late 1970s.An *open system* is a set of protocols that allows

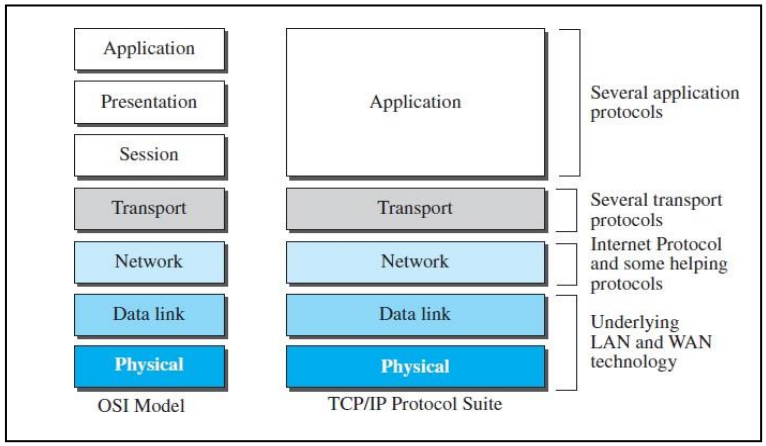
any two different systems to communicate regardless of their underlying architecture.

- The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.
- It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.



OSI versus TCP/IP

- When we compare the two models, we find that two layers, session and presentation, are missing from the TCP/IP protocol suite.
- These two layers were not added to the TCP/IP protocol suite after the publication of theOSI model.
- The application layer in the suite is usually considered to be the combination of three layers in the OSI model, as shown in Figure.



- Two reasons were mentioned for this decision.
    1. TCP/IP has more than one transport-layer protocol. Some of the functionalities of the session layer are available in some of the transport-layer protocols.
    2. The application layer is not only one piece of software. Many applications can be developed at this layer.

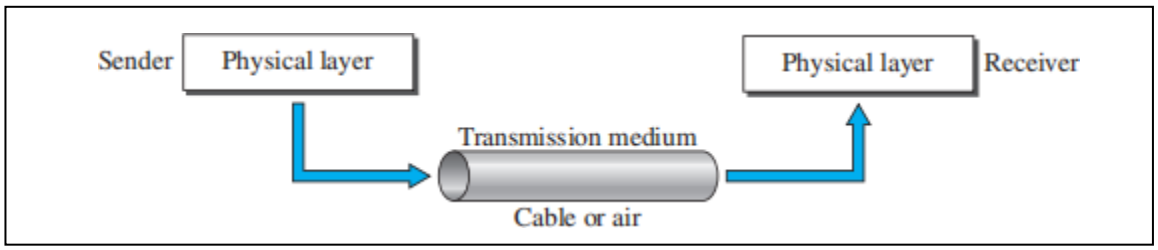
Lack of OSI Model's Success

1. OSI was completed when TCP/IP was fully in place and a lot of time and money had been spent on the suite; changing it would cost a lot.
2. Some layers in the OSI model were never fully defined.
3. When OSI was implemented by an organization in a different application, it did not showa high enough level of performance to entice the Internet authority to switch from the TCP/IP protocol suite to the OSI model.

Introduction to Physical Layer

1.6 Transmission Medium

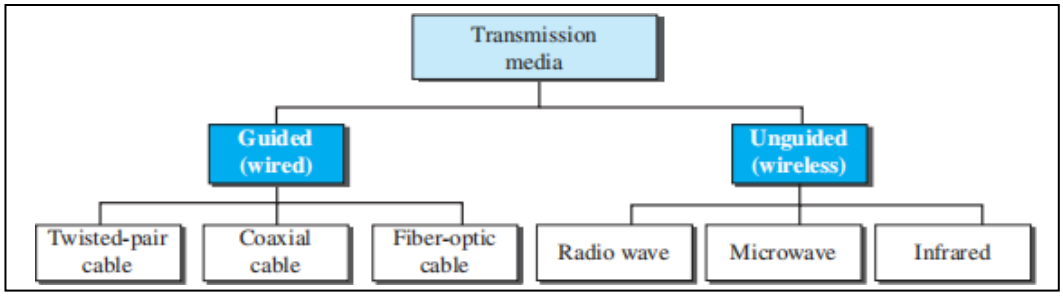
Transmission media are actually located below the physical layer and are directly con- trolled by the physical layer. We could say that transmission media belong to layer zero. Figure shows the position of transmission media in relation to the physical layer.



A **transmission medium** can be broadly defined as anything that can carry Information from a source to a destination. For example, the transmission medium for two people having a dinner conversation is the air.

Computers and other telecommunication devices use signals to represent data. These signals are transmitted from one device to another in the form of electromagnetic energy, which is propagated through transmission media.

In telecommunications, transmission media can be divided into two broad categories: guided and unguided. Guided media include twisted-pair cable, coaxial cable, and fiber-optic cable. Unguided medium is free space.

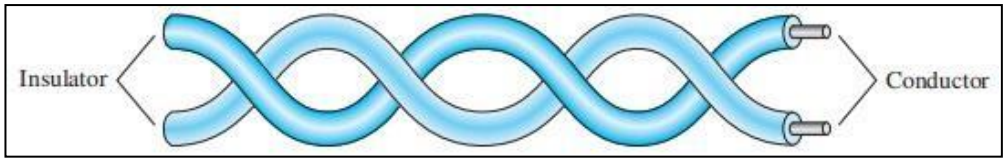


1.6.1 Guided Media

Guided media- provide a conduit from one device to another, include **twisted-pair cable, coaxial cable,** and **fiber-optic cable.**

a. Twisted-Pair Cable

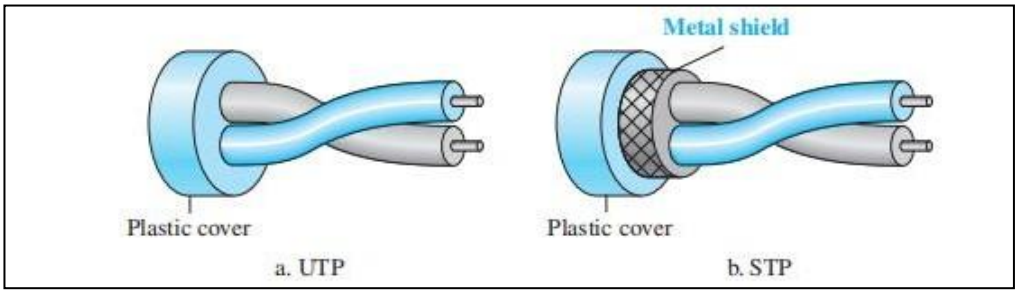
A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in Figure .



- One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.
- In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.
- If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e.g., one is closer and the other is farther). This results in a difference at the receiver.

Unshielded Versus Shielded Twisted-Pair Cable

The most common twisted-pair cable used in communications is referred to as **unshielded twisted-pair (UTP)**. IBM has also produced a version of twisted-pair cable for its use, called **shielded twisted-pair (STP).** STP cable has a metal foil or braided- mesh covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.



Categories

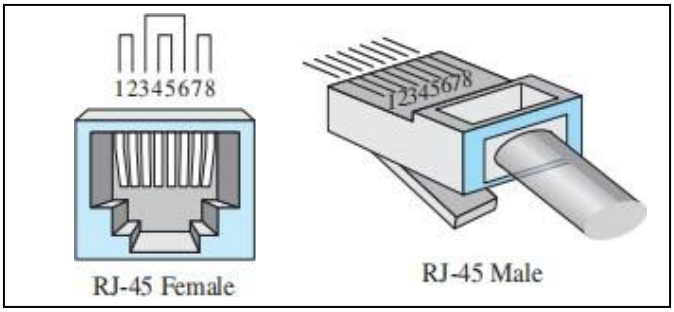
The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into seven categories. Categories are determined by cable quality, with 1 as the lowest and 7 as the highest. Each EIA category is suitable for specific uses. Table shows these categories.

Category	Specification	Data Rate (Mbps)	Use
1	Unshielded twisted-pair used in telephone	0.1	Telephone
2	Unshielded twisted-pair originally used in T lines	2	T-1 lines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
5E	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs

7	Sometimes called *SSTP (shielded screen twisted-pair)*. Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk and increases the data rate.	600	LANs

Connectors

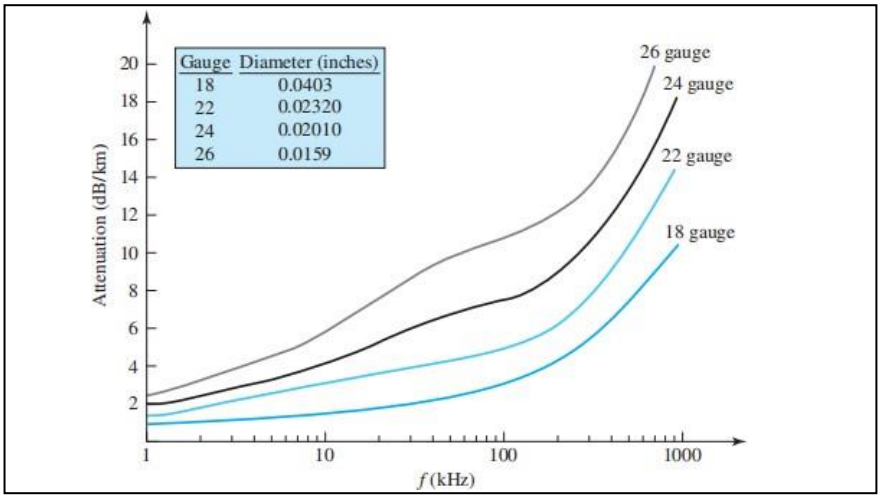
The most common UTP connector is **RJ45** (RJ stands for registered jack), as shown in Figure



The RJ45 is a keyed connector, meaning the connector can be inserted in only one way.

Performance

One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance. A twisted-pair cable can pass a wide range of frequencies. However, Figure shows that with increasing frequency, the attenuation, measured in decibels per kilometer (dB/km), sharply increases with frequencies above 100 kHz. Note that ***gauge*** is a measure of the thickness of the wire.



Applications

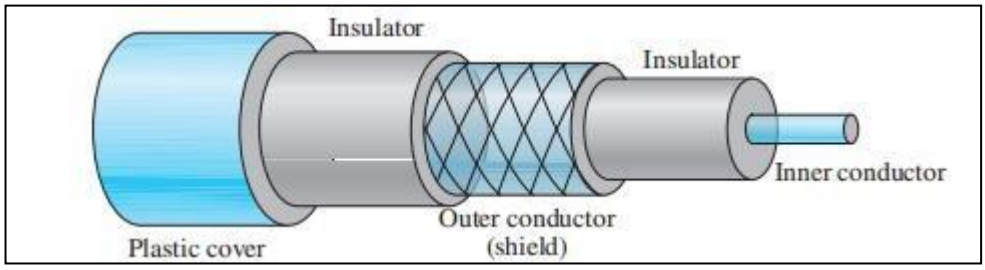
Twisted-pair cables are used in telephone lines to provide voice and data channels. The local loop—the line that connects subscribers to the central telephone office— commonly consists of unshielded twisted-pair cables.

The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.

Local-area networks, such as 10Base-T and 100Base-T, also use twisted-pair cables.

b. Coaxial Cable

Coaxial cable (or *coax*) carries signals of higher frequency ranges than those in twisted- pair cable. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductorof metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.



Coaxial Cable Standards

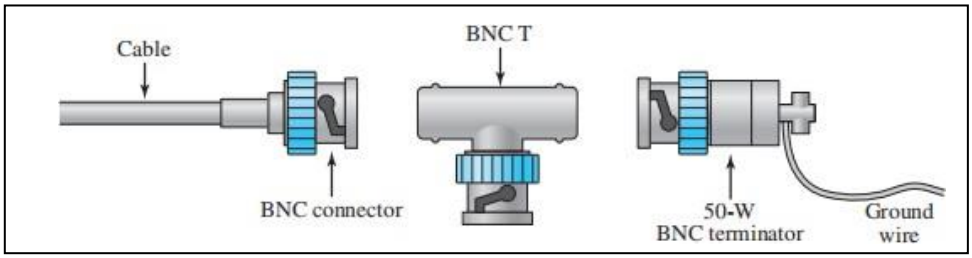
Coaxial cables are categorized by their **Radio Government (RG)** ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the

inner conductor, the thickness and type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function, as shown in Table.

Category	*Impedance*	*Use*
RG-59	75 □	Cable TV
RG-58	50 □	Thin Ethernet
RG-11	50 □	Thick Ethernet

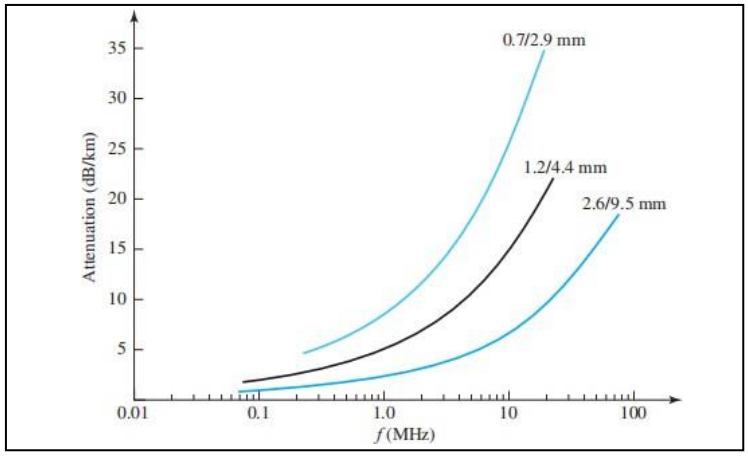
Coaxial Cable Connectors

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the **Bayonet Neill-Concelman (BNC)** connector. Figure shows three popular types of these connectors: the BNC connector, the BNC T connector, and the BNC terminator.



Performance

We notice in Figure that the attenuation is much higher in coaxial cable than in twisted-pair cable. In other words, although coaxial cable has a much higher bandwidth, the signal weakens



rapidly and requires the frequent use of repeaters.

Applications

1. Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals. Later it was used in digital telephone networks

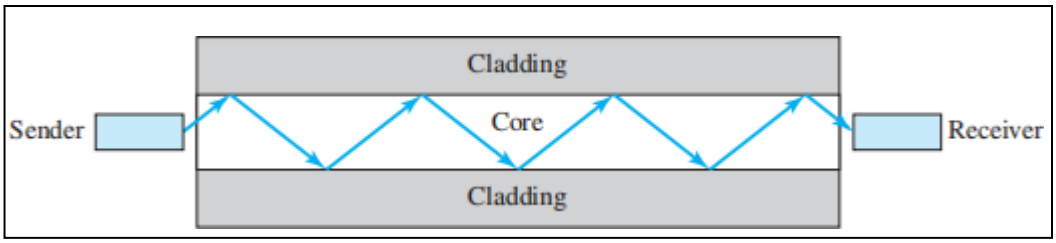
where a single coaxial cable could carry digital data up to 600 Mbps.

2. Cable TV networks also use coaxial cables.
3. Another common application of coaxial cable is in traditional Ethernet LANs.

c. FIBER-OPTIC CABLE

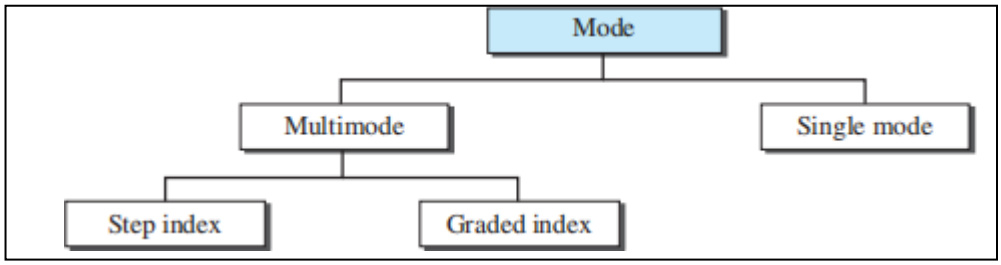
A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.

Optical fibers use reflection to guide light through a channel. A glass or plastic **core** is surrounded by a **cladding** of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.



Propagation Modes

Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics. Multi- mode can be implemented in two forms: step-index or graded-index.



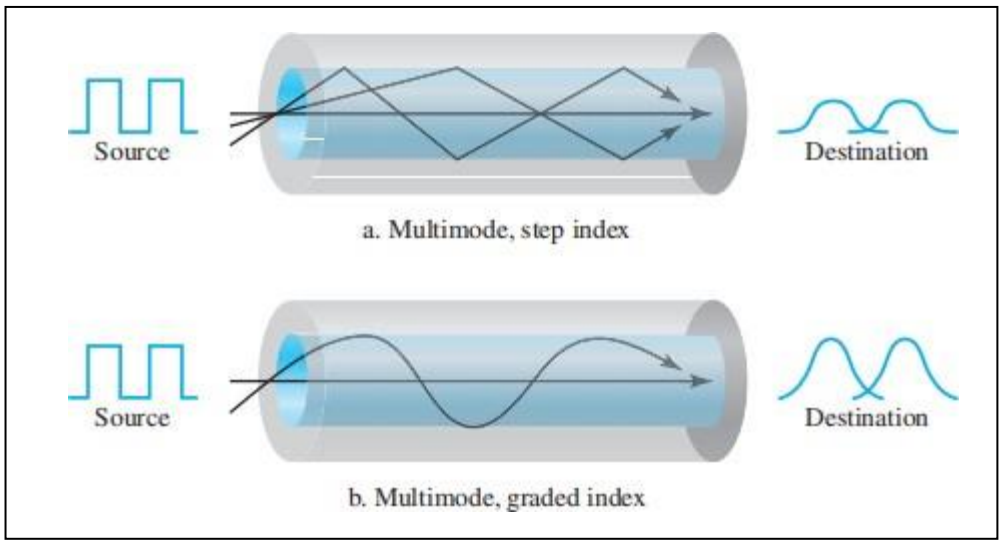
Multimode

Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core, as shown in Figure.

In **multimode step-index fiber**, the core's density is constant, causing light to travel in straight

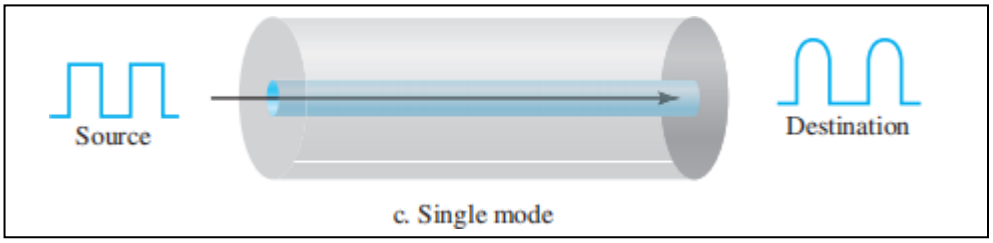
lines until it hits the lower-density cladding, which changes the light's angle abruptly. This sudden change, called the step-index, can distort the signal.

In contrast, **multimode graded-index** fiber reduces this distortion by gradually decreasing the core's density from the center to the edge, allowing light to bend smoothly and reducing signal distortion.



Single-Mode

Single-mode fiber uses step-index fiber with a very narrow core and a focused light source. This setup limits light beams to nearly horizontal paths. The fiber's smaller diameter and lower density create a critical angle close to 90°, ensuring that the beams travel almost parallel. As a result, the beams reach the destination together, with minimal delays and distortion.



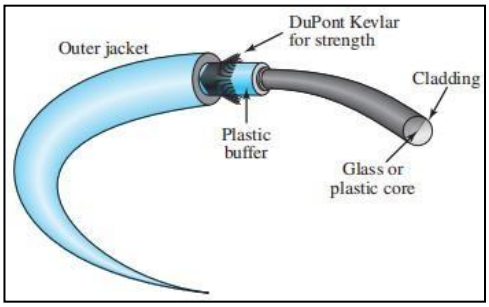
Fiber Sizes

Optical fibers are defined by the ratio of the diameter of their core to the diameter of their cladding, both expressed in micrometers. The common sizes are shown in Table. Note that the last size listed is for single-mode only.

Type	*Core (□m)*	*Cladding (□m)*	*Mode*
50□125	50.0	125	Multimode, graded index
62.5□125	62.5	125	Multimode, graded index
100□125	100.0	125	Multimode, graded index
7□125	7.0	125	Single mode

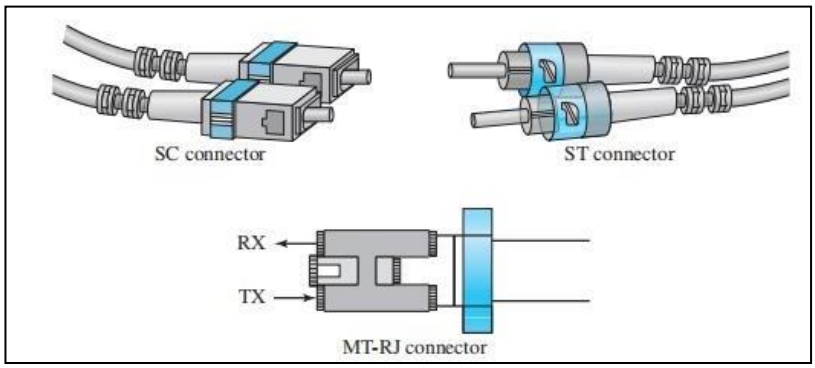
Cable Composition

Figure shows the composition of a typical fiber-optic cable. The outer jacket is made of either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable. Kevlar is a strong material used in the fabrication of bulletproof vests. Below the Kevlar is another plastic coatingto cushion the fiber. The fiber is at the center of the cable, and it consists of cladding and core.



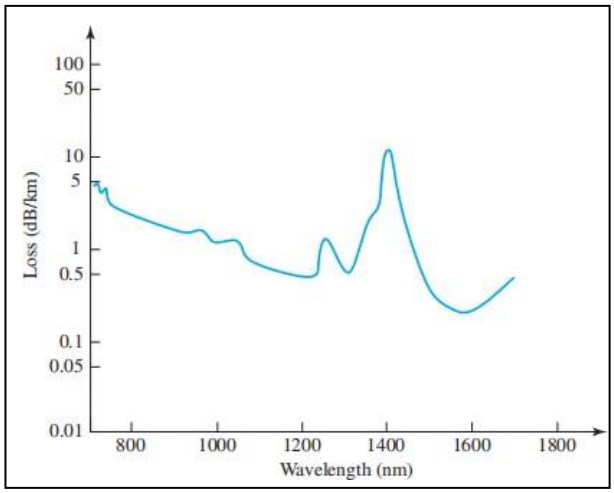
Fiber-Optic Cable Connectors

There are three types of connectors for fiber-optic cables, as shown in Figure. The **subscriber channel (SC) connector** is used for cable TV. It uses a push/pull locking system. The **straight-tip (ST) connector** is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC. **MT-RJ** is a connector that is the same size as RJ45.



Performance

The plot of attenuation versus wavelength in Figure shows a very interesting phenomenon in fiber-optic cable. Attenuation is flatter than in the case of twisted-pair cable and coaxial cable. The performance is such that we need fewer (actually one- tenth as many) repeaters when we usefiber-optic cable.



Applications

1. Fiber-optic cable is often found in backbone networks because its wide bandwidth iscost-effective.
2. Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network.
3. Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable.

Advantages and Disadvantages of Optical Fiber

Advantages

Fiber-optic cable has several advantages over metallic cable (twisted-pair or coaxial).

Higher bandwidth. Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable.

1. **Less signal attenuation**. Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.

2. **Immunity to electromagnetic interference**. Electromagnetic noise cannot affect fiber-optic cables.
3. **Resistance to corrosive materials**. Glass is more resistant to corrosive materials than copper.
4. **Light weight**. Fiber-optic cables are much lighter than copper cables.
5. **Greater immunity to tapping**. Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

Disadvantages

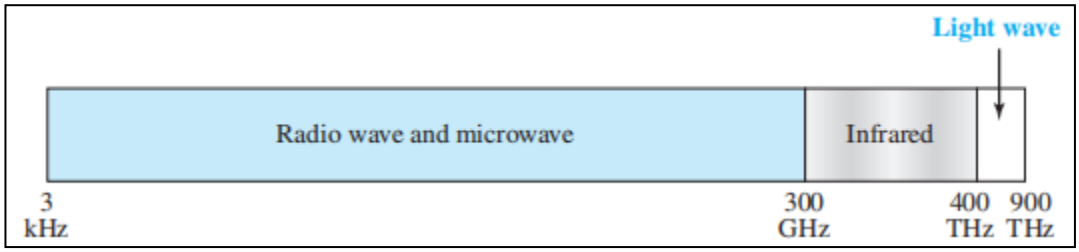
There are some disadvantages in the use of optical fiber.

1. **Installation and maintenance.** Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
2. **Unidirectional light propagation**. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
3. **Cost.** The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

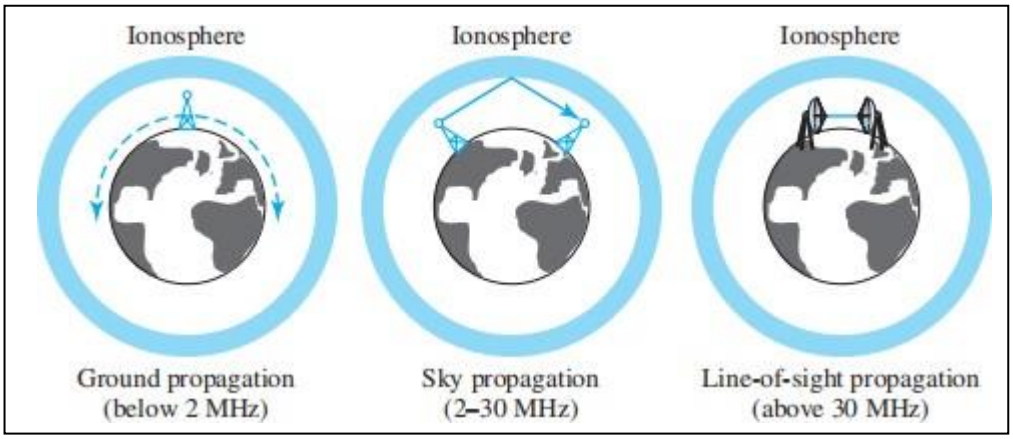
1.6.2 Unguided Media: Wireless

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

Figure shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.



Unguided signals can travel from the source to the destination in several ways: ground propagation, sky propagation, and line-of-sight propagation, as shown in Figure.



In **ground propagation**, radio waves travel close to the Earth, following its curve. These low-frequency signals spread out from the antenna, and their range depends on the signal's power.

In **sky propagation**, higher-frequency waves bounce off the ionosphere and return to Earth, allowing longer distances with less power.

In **line-of-sight propagation**, very high-frequency signals travel straight from one antenna to another. The antennas must face each other and be positioned to avoid Earth's curvature. Line-of-sight can be challenging because the signals can't be perfectly focused.

The section of the electromagnetic spectrum defined as radio waves and microwaves is divided into eight ranges, called *bands*, each regulated by government authorities. These bands are rated from *very low frequency* (VLF) to *extremely high frequency* (EHF). Table lists these bands, their ranges, propagation methods, and some applications.

Band	*Range*	*Propagation*	*Application*
very low frequency (VLF)	3–30 kHz	Ground	Long-range radio navigation
low frequency (LF)	30–300 kHz	Ground	Radio beacons and navigational locators
middle frequency (MF)	300 kHz–3 MHz	Sky	AM radio

high frequency (HF)	3–30 MHz	Sky	Citizens band (CB), ship□aircraft
very high frequency (VHF)	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
ultrahigh frequency (UHF)	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
superhigh frequency (SF)	3–30 GHz	Line-of-sight	Satellite
extremely high frequency (EHF)	30–300 GHz	Line-of-sight	Radar, satellite

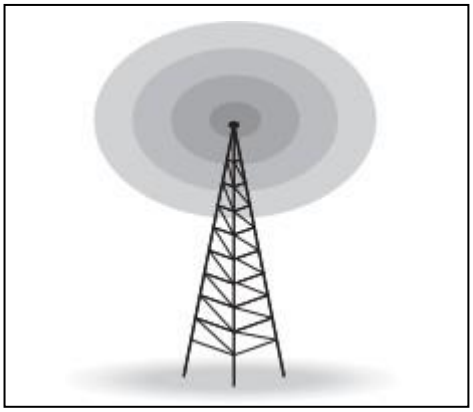
We can divide wireless transmission into three broad groups: radio waves, micro- waves, and infrared waves.

I. Radio Waves

- Although there is no clear-cut demarcation between radio waves and microwaves, electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called **radio waves;** waves ranging in frequencies between 1 and 300 GHz are called **micro- waves.** However, the behavior of the waves, rather than the frequencies, is a better criterion for classification.
- Radio waves are mostly omnidirectional, meaning they spread out in all directions from the antenna, so the sending and receiving antennas don't need to be aligned. However,this also means signals can interfere with each other if they use the same frequency.
- Sky-mode radio waves can travel long distances, making them suitable for broadcasting like AM radio.
- Low and medium-frequency radio waves can penetrate walls, which is helpful for indoor reception but makes it hard to contain signals.
- The radio wave band is narrow, limiting data rates for digital communication, and is heavily regulated by authorities like the FCC.

Omnidirectional Antenna

Radio waves use **omnidirectional antennas** that send out signals in all directions. Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas. Figure shows an omnidirectional antenna.



Applications

The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, mari- time radio, cordless phones, and paging are examples of multicasting.

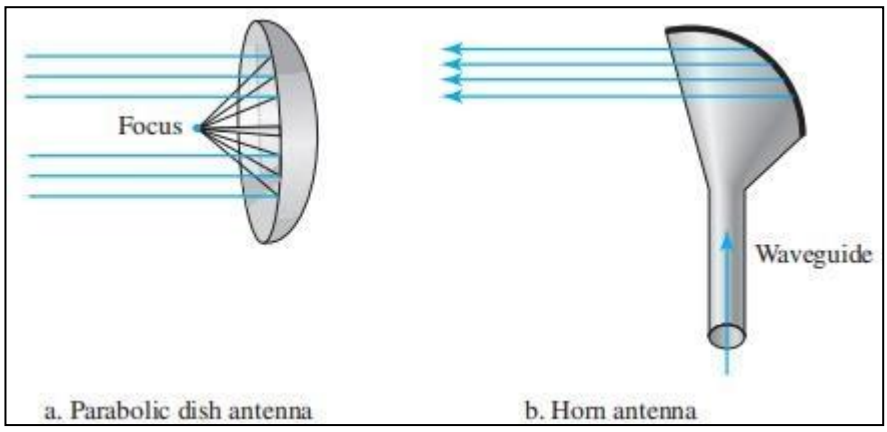
II. Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called micro- waves. Microwaves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas. The following describes some characteristics of microwave propagation:

a. **Microwave propagation is line-of-sight** Microwave propagation requires a clear line-of-sight between antennas. This means that distant towers must be very tall to avoid obstacles and Earth's curvature. For long distances, repeaters are often needed to maintainthe signal.
b. **Very high-frequency microwaves cannot penetrate walls.** This characteristic can be a disadvantage if receivers are inside buildings.
c. **The microwave band is relatively wide**, almost 299 GHz. Therefore wider subbands can be assigned, and a high data rate is possible.
d. Use of certain portions of the band requires permission from authorities.

Unidirectional Antenna

Microwaves need **unidirectional antennas** that send out signals in one direction. Two types of antennas are used for microwave communications: the parabolic dish and the horn.



A **parabolic dish antenna** uses a parabolic shape to focus incoming signals to a single point, capturing more of the signal than a single-point receiver. Outgoing signals are sent through a horn aimed at the dish, which reflects the waves outward.

A **horn antenna**, shaped like a large scoop, directs outgoing signals in narrow beams and collects incoming signals by funneling them down into the stem, similar to how the parabolic dish works.

Applications

Microwaves, due to their unidirectional properties, are very useful when unicast (one- to-one) communication is needed between the sender and the receiver. They are used in cellular phones , satellite networks , and wireless LANs.

III. Infrared

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication.

Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interfer- ence between one system and another; a short-range communication system in one room cannot be affected by another system in the next room. When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors. However, this

same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications

The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate.

The *Infrared Data Association* (IrDA), an association for sponsoring the use of infrared waves, has established standards for using these signals for communication between devices such as keyboards, mice, PCs, and printers.

For example, some manufacturers provide a special port called the **IrDA port** that allows a wireless keyboard to commnicate with a PC. The standard originally defined a data rate of 75 kbps for a distance up to 8 m. The recent standard defines a data rate of 4 Mbps.

Infrared signals defined by IrDA transmit through line of sight; the IrDA port on the keyboard needs to point to the PC for transmission to occur.