**UNIT 1**

1. **Computer Networks**

A **computer network,** often simply referred to as a network, is a **collection of computers** and devices interconnected **by communications channels** that facilitate communications and allows **sharing of resources** and information among **interconnected devices.**

1. **Data Communication**

Data Communications is the transfer of data or information **between a source and a receiver.** The **source transmits** the data and the **receiver receives** it. The actual generation of the information is not part of Data Communications nor is the resulting action of the information at the receiver. Data Communication is interested in the transfer of data, the method of transfer and the preservation of the data during the transfer process.

The purpose of Data Communications is to **provide the rules and regulations** that allow computers with different **disk operating systems, languages, cabling** and **locations** to share resources. The rules and regulations are called **protocols and standards** in Data Communications.

For data communication to occur, the communicating devices must be part of a communication system made up of a combination of hardware and software. The effectiveness of a data communication system depends on the three 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 data accurately. Data that have been altered in transmission and left uncorrected are noise.
3. **Timeliness:** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video, audio, and voice data, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.
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. For example, let us assume that video packets are sent every **30 ms.** If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.
5. **Data communication Components**

data communications

system has

five components:

Rule I:

Rule 2:

Rule a:

Protocol

Protocol

Message

Rule 1:

Rule 2:

Rule ***n:***

Sender

Medium

Receiver



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. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
5. **Protocol:** A **protocol** is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.
6. Data Representation

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

1. **Text:** In data communications, text is represented as a bit pattern, a sequence of bits (0s or

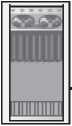
1s). Different sets of bit patterns have been designed to represent text symbols. Each set is called a **code,** and the process of representing symbols is called coding. Today, the prevalent coding system is called **Unicode**, which uses 32 bits to represent a symbol or character used in any language in the world. The **American Standard Code for Information Interchange (ASCII),** developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as **Basic Latin.**

1. **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.
2. **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.* For example, an image can be divided into 1000 pixels or 10,000 pixels. In the second case, there is a better representation of the image (better resolution), but more memory is needed to store the image.

Each pixel in image has been assigned a bit pattern. For black and white images, 1-bit pattern is used to represent a pixel. For gray scale images, 2-bit pattern is used i.e. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by For color images several methods are used for representation i.e. RGB (combination of red, green and blue), YCM (combination of yellow, cyan and magenta).

1. **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.
2. **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.
3. Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex:

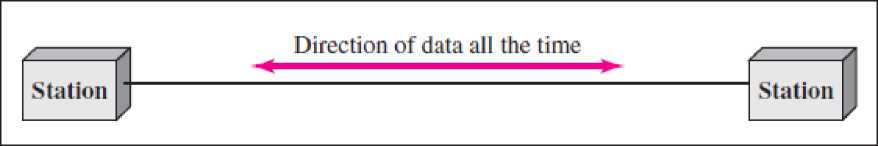


Direction of data

**Mai nframe**

Monitor

1. **Simplex**



/

**Station**

Direction of data at time 1

**/ J**

**Station**

Direction of data at time 2

**h. Half-duplex**

**c. Full-duplex**

**Simplex:** In **simplex mode,** the communication is unidirectional, as on a one-way street. 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 keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction. **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. The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are travelling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkie is 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. The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction.

This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals travelling in both directions. One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

1. NETWORKS

**Networking** is linking of two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software. 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.** The more throughputs and less delay are required which is contradictory. If we try to send more data to the network, throughput may increase but increase in delay due to traffic congestion in the network.

1. **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.
2. **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.

**Distributed computing** is a field of computer science that studies distributed systems. A **distributed system** consists of multiple autonomous computers that communicate through a computer network. The computers interact with each other in order to achieve a common goal. A computer program that runs in a distributed system is called a **distributed program,** and **distributed programming** is the process of writing such programs.

Distributed computing also refers to the use of distributed systems to solve computational problems. In distributed computing, a problem is divided into many tasks, each of which is solved by one or more computers.

Distributed programming typically falls into one of several basic architectures or categories: client-server, 3-tier architecture, //-tier architecture, distributed objects, loose coupling, or tight coupling.

* **Client-server:** Smart client code contacts the server for data then formats and displays it to the user. Input at the client is committed back to the server when it represents a permanent change.
* **3-tier architecture:** Three tier systems move the client intelligence to a middle tier so that stateless clients can be used. This simplifies application deployment. Most web applications are 3-Tier.
* **«-tier architecture:** //-tier refers typically to web applications which further forward their requests to other enterprise services. This type of application is the one most responsible for the success of application servers.
* **Tightly coupled (clustered):** refers typically to a cluster of machines that closely work together, running a shared process in parallel. The task is subdivided in parts that are made individually by each one and then put back together to make the final result.
* **Peer-to-peer:** an architecture where there is no special machine or machines that provide a service or manage the network resources. Instead all responsibilities are uniformly divided among all machines, known as peers. Peers can serve both as clients and servers.
* **Space based:** refers to an infrastructure that creates the illusion (virtualization) of one single address-space. Data are transparently replicated according to application needs. Decoupling in time, space and reference is achieved.

1. Type of Connection

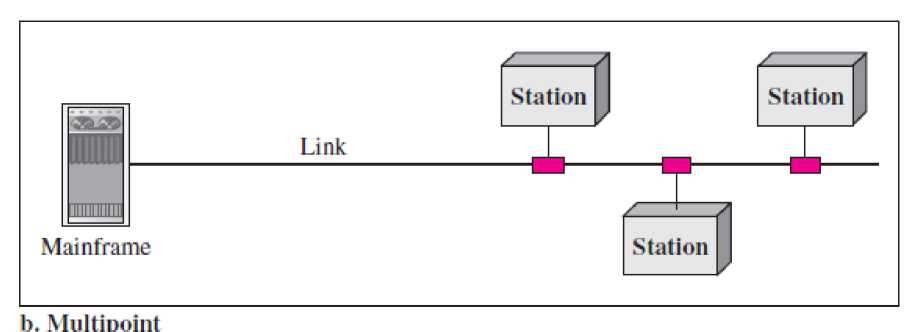
A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections: point-to-point and multipoint.

**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. Most point-to- point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television’s control system.

|  |  |  |  |
| --- | --- | --- | --- |
| Z f |  | Link | **z** |
| **Station** |  |  | **Station** |
| 1 | **/** |  |  |

1. **Point-to-point**

**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. If several devices can use the link simultaneously, it is a *spatially shared* connection. If users must take turns, it is a *timeshared* connection.



1. Topologies

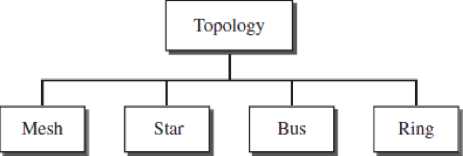
The term “**Topology**” refers to the way in which the end points or stations/computer systems, attached to the networks, are interconnected. Topology is essentially a stable geometric arrangement of computers in a network. Following points need to remember to select a topology:

* Application S/W and protocols.
* Types of data communicating devices.
* Geographic scope of the network.
* Cost.
* Reliability.

Depending on the requirement there are different Topologies to construct a network.

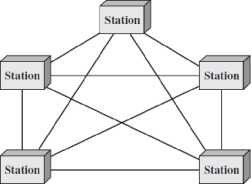
1. Mesh topology.
2. Star topology.
3. Tree (Hierarchical) topology.
4. Bus topology.
5. Ring topology.
6. Cellular topology.

* Ring and mesh topologies are felt convenient for peer to peer transmission.
* Star and tree are more convenient for client server.
* Bus topology is equally convenient for either of them.



**Mesh Topology:** In a **mesh topology,** every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with *n* nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to *n* - 1 nodes, node 2 must be connected to *n* - 1 nodes, and finally node *n* must be connected to *n* -1 nodes. So total number of physical links are n(n-l). If communication is done in both directions (duplex mode), then number of links are divided by 2.

n=n (n-l)/2



Advantages:

1. Due to dedicated links, it eliminates the network traffic problems.
2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
3. Because every message travels along a dedicated line to the recipient. That helps to manage the security or privacy.
4. The precise location of fault identification is easy.

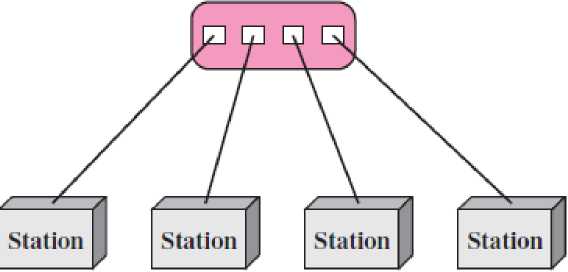
Disadvantages:

1. The amount of cabling and number of I/O ports required.
2. Installation and reconnection is difficult.

One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

i. **Star Topology** In a **star topology,** each device has a dedicated point-to-point link only to a central controller, usually called a **hub.** In star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub. Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. One big **disadvantage** of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

Hub

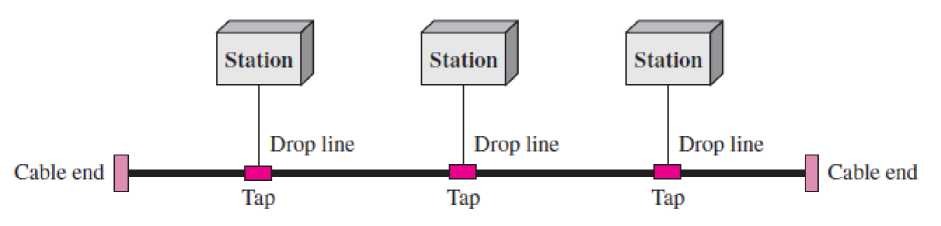


ii. **Bus Topology:** The preceding examples all describe point-to-point connections. A **bus topology** is multipoint topology. One long cable acts as a **backbone** to link all the devices in a network.

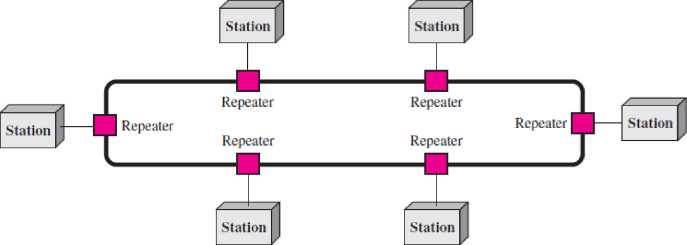
Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

**Advantages** of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies.

**Disadvantages** include difficult reconnection and fault isolation. It is difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.



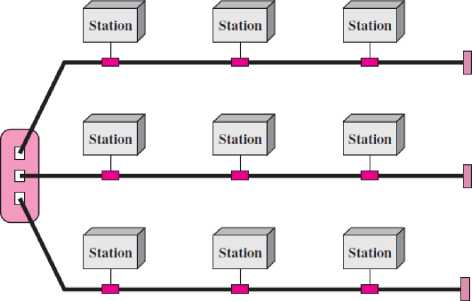
iii. **Ring Topology:** In a **ring topology,** each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

iii. **Hybrid Topology:** A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology.



**9. Protocols**

In computer networks, communication occurs between entities in different systems. An **entity** is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

1. **Syntax.** The term ***syntax*** refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.
2. **Semantics.** The word ***semantics*** refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?
3. **Timing.** The term ***timing*** refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

Standards

Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications. Data communication standards fall into two categories: *de facto* (meaning “by fact” or “by convention”) and *de jure* (meaning *“*by law” or “by regulation”).

**De facto.** Standards that have not been approved by an organized body but have been adopted as standards through widespread use are **de facto standards.** De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology. **De jure.** Those standards that have been legislated by an officially recognized body are **de jure standards.**

Standards Organizations

Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

**Standards Creation Committees**

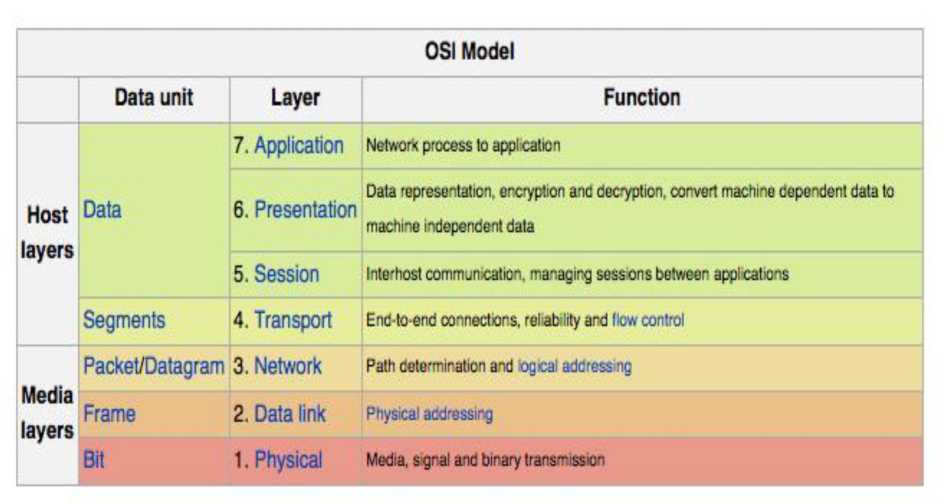
While many organizations are dedicated to the establishment of standards, data telecommunications in North America rely primarily on those published by the following:

1. **International Organization for Standardization (ISO).** The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.
2. **International Telecommunication Union—Telecommunication Standards Sector (ITU-T).** By the early 1970s, a number of countries were defining national standards for telecommunications, but there was still little international compatibility. The United Nations responded by forming, as part of its International Telecommunication Union (ITU), a committee, the **Consultative Committee for International Telegraphy and Telephony (CCITT).** This committee was devoted to the research and establishment of standards for telecommunications in general and for phone and data systems in particular. On March 1, 1993, the name of this committee was changed to the International Telecommunication Union— Telecommunication Standards Sector (ITU-T).
3. **American National Standards Institute (ANSI).** Despite its name, the American National Standards Institute is a completely private, nonprofit corporation not affiliated with the U.S. federal government. However, all ANSI activities are undertaken with the welfare of the United States and its citizens occupying primary importance.
4. **Institute of Electrical and Electronics Engineers (IEEE).** The Institute of Electrical and Electronics Engineers is the largest professional engineering society in the world. International in scope, it aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well as in all related branches of engineering. As one of its goals, the IEEE oversees the development and adoption of international standards for computing and communications.
5. **Electronic Industries Association (EIA).** Aligned with ANSI, the Electronic Industries Association is a nonprofit organization devoted to the promotion of electronics manufacturing concerns. Its activities include public awareness education and lobbying efforts in addition to standards development. In the field of information technology, the EIA has made significant contributions by defining physical connection interfaces and electronic signaling specifications for data communication.
6. THE OSI MODEL

An ISO standard that covers all aspects of network communications is the Open Systems Interconnection 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 purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

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.

Within a single machine, each layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between machines, layer *x* on one machine communicates with layer *x* on another machine. This communication is governed by an agreed-upon series of rules and conventions called protocols. The processes on each machine that communicate at a given layer are called **peer-to-peer processes.** Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.



Peer-to-Peer Processes

Physical layer of device A and device B is communicating directly by sending a stream of bits. In higher layers, at source computer communication is moving down through the layers

and receiver computer back up through layers. Sender device adds its own information and receiver computer unwrap the message layer by layer.

Communication is done with the help of interface among layers. Each interface defines the information and services a layer must provide for the layer above it.



Device

A

Application |-<-

7-6 interface [ Presentation

6-5 interface

Intermediate Intermediate

node node

Device

B

7

6

5

4

3

2

I

Session

5-4 interface |

Transport |-<-

4-3 interface

Network

3-2 interface [

Data link

| 2-1 interface |

^^^^^hysical^^^^-

Peer-to-peer protocol (7th layer)

Peer-to-peer protocol (6th layer)

Peer-to-peer protocol {5tli layer)

Peer-to-peer protocol (4tli layer)

**H**3id b 3rd

—Network I-\*-“

b-\*T

h 3rd Network I-\* ► 

1st

Application

7-6 interface |~ Presentation

6-5 interface |

Session

Network

| 3-2 interface [

5-4 interface [

Transport

4-3 interface |

2-1 interface [ ^Physical^^^j

7

6

5

4

3

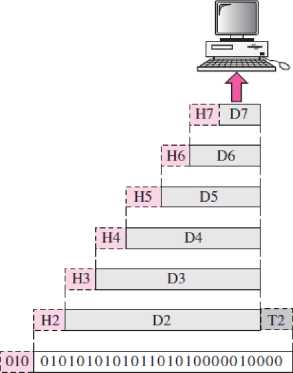
***2***

1

Physical communication

These seven layers are subdivided into three subgroups:

1. Network Support Layer: Physical, data link and network layers (layers 1, 2, 3) are network support layers. These layers concerns with physical connections, physical addressing, transport timing and reliability.
2. User Support Layer: Session, presentation and application (layers 5, 6, 7) are user support layers. These layers allow interoperability among unrelated software systems.
3. Transport layer (layer 4) links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use. The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.



r

|  | | | | |  | **H7| D7** |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | **H6** | **D6** |
|  | | | |  |  | |
|  | | | | **H5** | **D5** | |
|  | | |  |  | | |
|  | | | **H4** | **D4** | | |
|  | |  |  | | | |
|  | | **H3** | **D3** | | | |
|  |  |  | | | | |
|  | **H2** | **D2** | | | | | **T2** |
|  | | | | | | |
| **010** | **010101010101101010000010000** | | | | | | |

**Transmission medium**

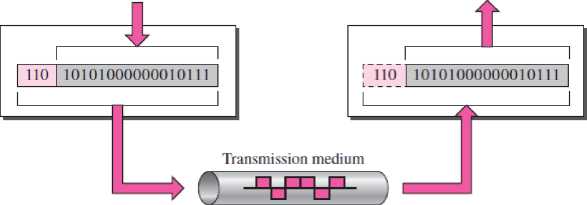
► 5 ~~TTir~~ j

The above figure shows that data transmission from source to receiver machine. At the source machine, data moves from upper layer to downwards, each layer add their header and possibly trailer to data unit. Physical layer change it into electromagnetic signal and transported along a physical link.

At the receivers system, data is transformed back from electromagnetic signal to digital form. As each block of data reaches the next higher layer, the headers and trailers attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken. By the time it reaches layer 7, the message is again in a form appropriate to the application and is made available to the recipient.

Physical Layer (Layer 1)

The **physical layer** coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.



From data link layer

To data link layer

Physical layer

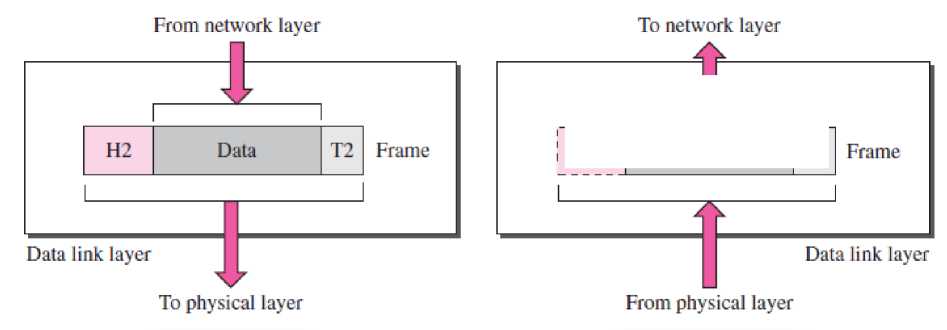
Physical layer

The physical layer is also concerned with the following:

1. The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
2. The physical layer data consists of a stream of **bits** (sequence of 0s or 1s) with no interpretation. For transmission, bits must be encoding to signals - electrical or optical.
3. The **transmission rate (Data Rate) —**the number of bits sent each second—is also defined by the physical layer.
4. **T**he sender and receiver not only must use the same bit rate but also must be synchronized at the bit level.
5. **T**he physical layer is concerned with the connection of devices to the media either through point-to-point or multipoint configuration.
6. **T**he physical topology defines how devices are connected to make a network.
7. **T**he physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

Data Link Layer(Layer 2)

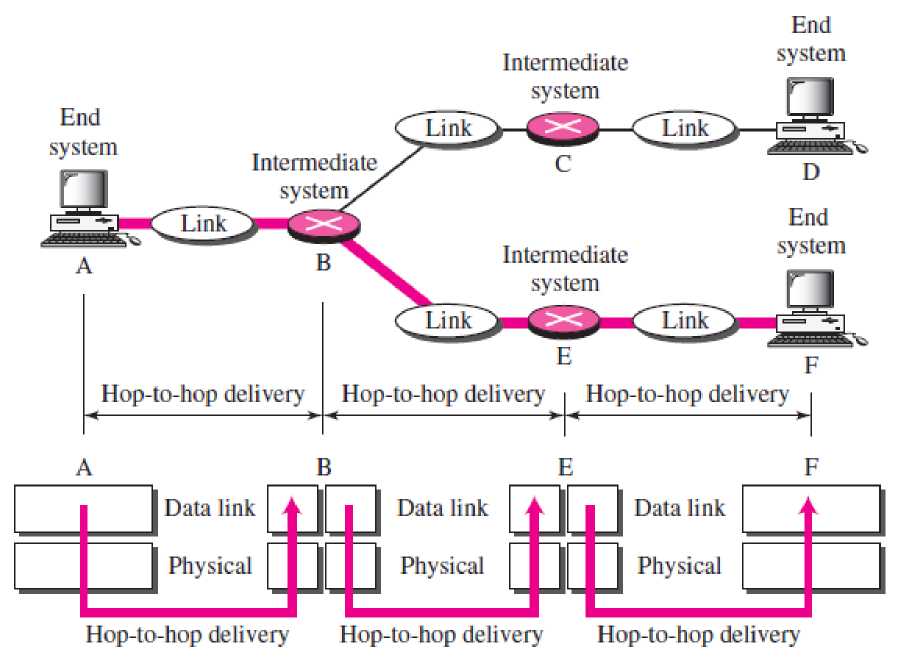
The main task of the **data link layer** is to transform a raw transmission facility into a line that appears free of undetected transmission errors. It does so by masking the real errors so the network layer does not see them. It accomplishes this task by having the sender break up the input data into **data frames** (typically a 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 sending back an **acknowledgement frame**.



|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
| H2  1 | Data | | T2 |

Other responsibilities of the data link layer include the following:

1. **Framing.** The data link layer divides the stream of bits received from the network layer into manageable data units called **frames*.***
2. **Physical addressing.** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.
3. **Flow control.** If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
4. **Error control.** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
5. **Access control.** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

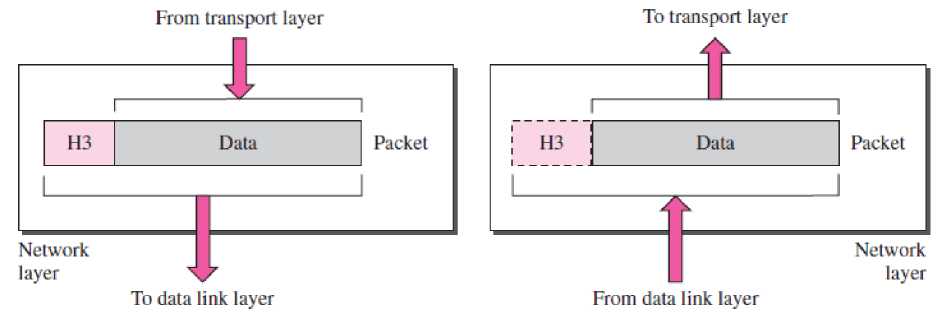


As the figure shows, communication at the data link layer occurs between two adjacent nodes. To send data from A to F, three partial deliveries are made. First, the data link layer at A sends a frame to the data link layer at B (a router). Second, the data link layer at B sends a new frame to the data link layer at E. Finally, the data link layer at E sends a new frame to the data link layer at F. Note that the frames that are exchanged between the three nodes have different values in the headers. The frame from A to B has B as the destination address and A as the source address. The frame from B to E has E as the destination address and B as the source address. The frame from E to F has F as the destination address and E as the source address. The values of the trailers can also be different if error checking includes the header of the frame.

Network Layer (Layer 3)

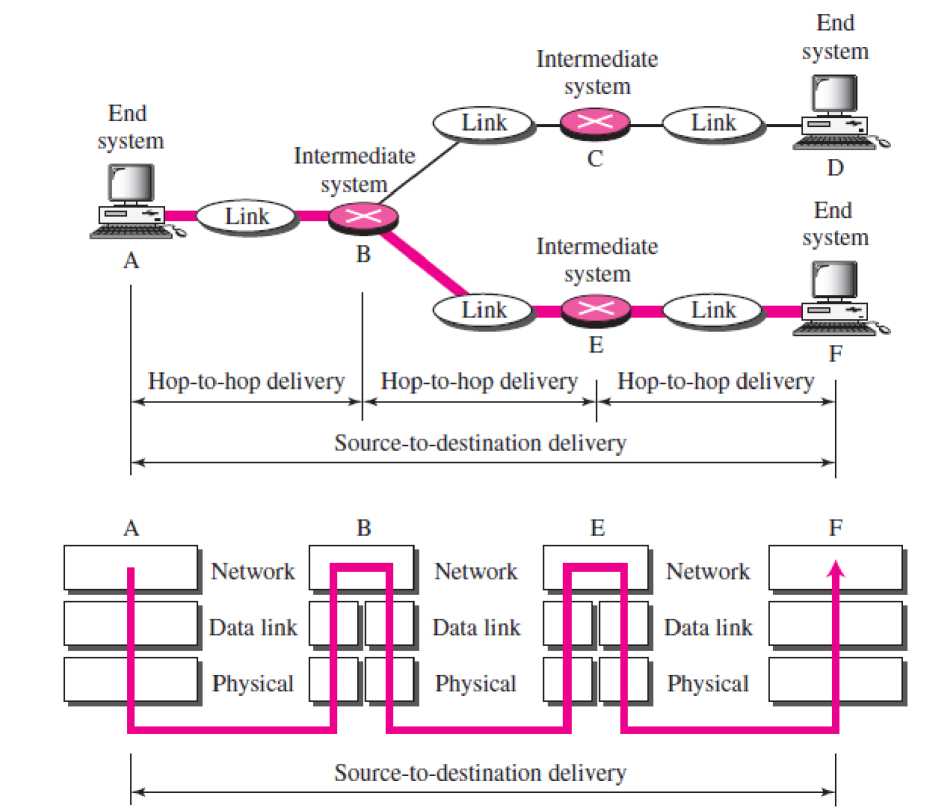
The **network layer** is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). The network layer ensures that each packet gets from its point of origin to its final destination.

If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery.



Other responsibilities of the network layer include the following:

1. **Logical addressing.** The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver. We discuss logical addresses later in this chapter.
2. **Routing.** When independent networks or links are connected to create *internetworks* (network of networks) or a large network, the connecting devices (called *routers* or *switches)* route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.



* As the figure shows, now we need a source-to-destination delivery.
* The network layer at A sends the packet to the network layer at B.
* When the packet arrives at router B, the router makes a decision based on the final destination (F) of the packet.
* Router B uses its routing table to find that the next hop is router E.
* The network layer at B, therefore, sends the packet to the network layer at E. The network layer at E, in turn, sends the packet to the network layer at F.

Transport Layer (Layer 4)

The **transport layer** is responsible for **process-to-process delivery** of the entire message. A process is an application program running on a host. Whereas the network layer oversees **source-to- destination delivery** of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

| *as/ tl* / \ Vt \ | | | | |
| --- | --- | --- | --- | --- |
| z LA/ / V'' / I t  *✓ / !* | | | |  |
| H4 Data | H4 | Data | H4 Data |  |
| 1 | 1 | | 1 |
| **A J** | | Segments | | |
| Transport \7 x | | > 4 | | |

From session layer

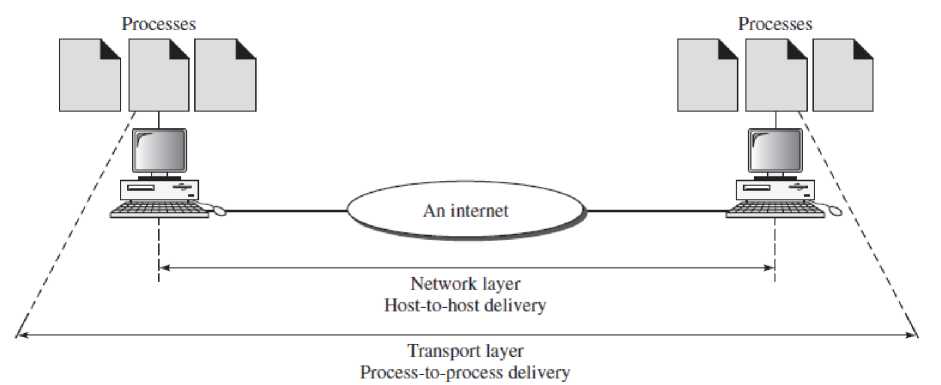
layer To network layer

|  | | A i  /\t\ | |
| --- | --- | --- | --- |
| / V  / | */ {* | 7 t LJ V  / 1 |  |
| H4 i Data 1 | ! H4 i Data 1 | H4i Data 1 |  |
| 1 | 1 | 1 |  |
|  |  | Segments | |
| A | **T** | Transport | |

To session layer

From network layer layer

1. **Service-point addressing.** Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a *service-point address* (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
2. **Segmentation and reassembly.** A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
3. **Connection control.** The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
4. **Flow control.** Like the data link layer, the transport layer is responsible for **flow control.** However, flow control at this layer is performed end to end rather than across a single link.
5. **Error control.** Like the data link layer, the transport layer is responsible for **error control.** However, error control at this layer is performed process-to process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without **error** (damage, loss, or duplication). Error correction is usually achieved through retransmission.

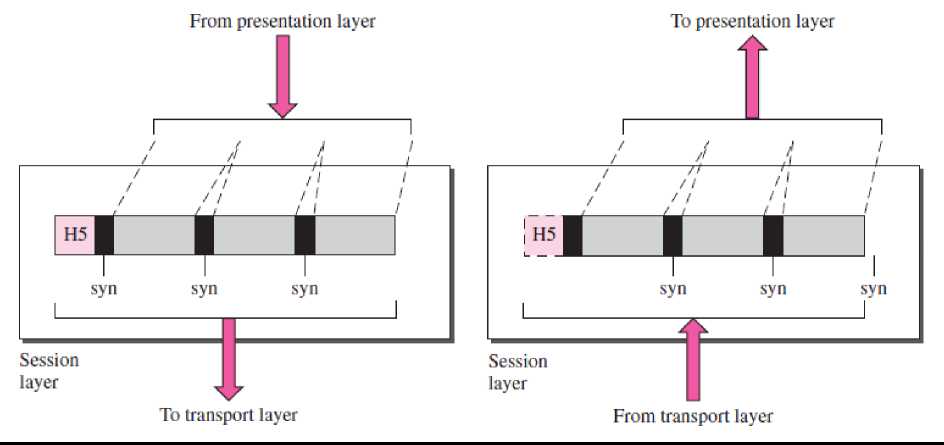


Session Layer (Layer 5)

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The **session layer** is the network *dialog controller.* It establishes, maintains, and synchronizes the interaction among communicating systems.

Specific responsibilities of the session layer include the following:

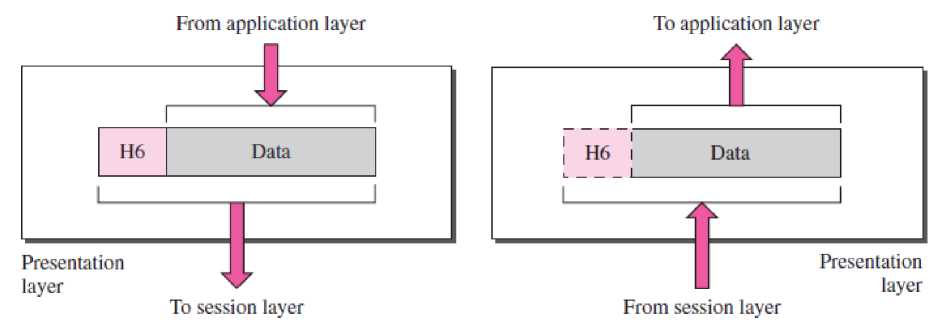
1. **Dialog control.** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
2. **Synchronization.** The session layer allows a process to add checkpoints, or **synchronization points,** to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent. Figure shows the relationship of the session layer to the transport and presentation layers.



Presentation Layer (Layer 6)

Sangeeta Arora

The **presentation layer** is concerned with the syntax and semantics of the information exchanged between two systems. Figure shows the relationship between the presentation layer and the application and session layers.

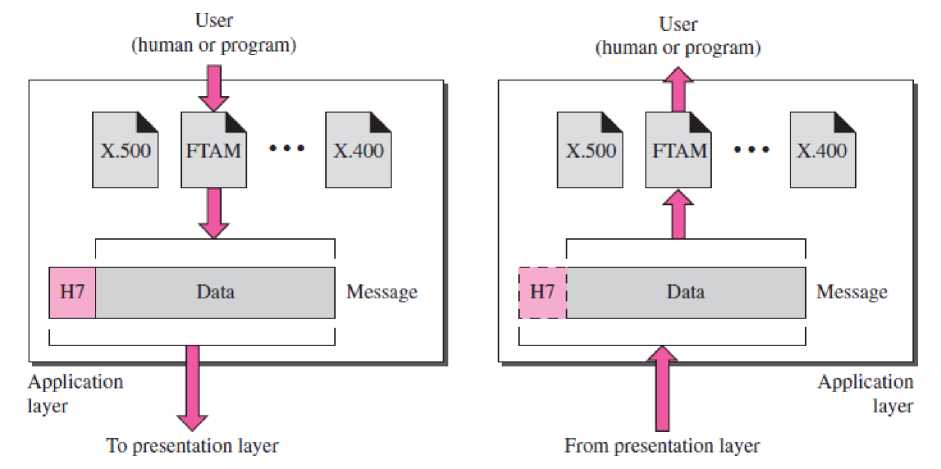


Specific responsibilities of the presentation layer include the following:

1. **Translation.** The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
2. **Encryption.** To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information toanother form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
3. **Compression.** Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

Application Layer (Layer 7)

The **application layer** enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

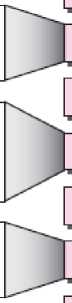


The above figure shows the relationship of the application layer to the user and the presentation layer. In this figure three services are shown i.e. X.400 (message-handling services), X.500 (directory services), and file transfer, access, and management (FTAM). The user in this example employs X.400 to send an e-mail message.

Specific services provided by the application layer include the following:

1. **Network virtual terminal.** A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.
2. **File transfer, access, and management.** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
3. **Mail services.** This application provides the basis for e-mail forwarding and storage.
4. **Directory services.** This application provides distributed database sources and access for global information about various objects and services.

Summary of Layers is shown in following figure:



To translate, encrypt, and compress data

To organize bits into frames; to provide hop-to-hop delivery

To provide reliable process-to- process message delivery and error recovery

Application

Presentation

Session

Transport

Network

Data link

Physical

To transmit bits over a medium; to provide mechanical and electrical specifications

To establish, manage, and terminate sessions

To move packets from source to destination; to provide internetworking

To allow access to network resources

1. Transmission Medium

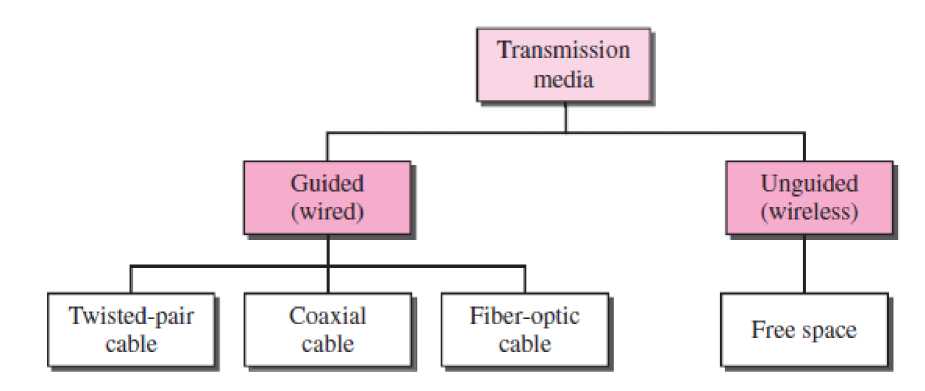
A **transmission medium** can be broadly defined as anything that can carry information from a source to a destination. For example, written message might use mail carrier as transmission medium.

In terms of data communication, the transmission medium is usually free space, metallic cable, or fiber-optic cable and information is usually a signal that is the result of a conversion of data from another form.

Transmission media can be divided into two broad categories: Guided and Unguided media.

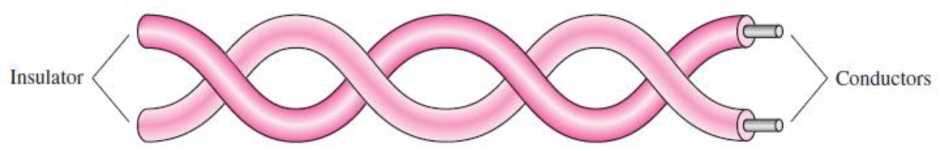
**Guided Media**

Guided Media includes Twisted-Pair, Co-axial and Fiber-Optic Cables. A signal travelling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. **Optical fiber** is a cable that accepts and transports signals in the form of light.



**a. Twisted-Pair Cable**

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



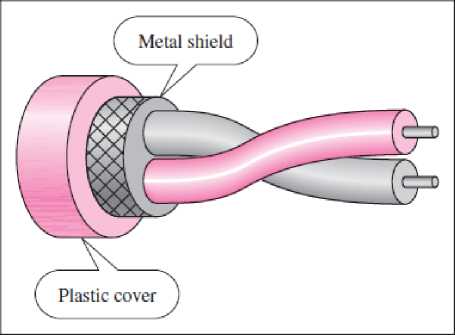
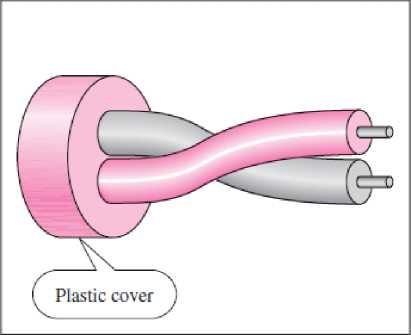
**One** of the wires is used to **carry signals to the receiver**, and the **other** is used only as a **ground reference**. The receiver uses the difference between the two.

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 these two wires are parallel, the unwanted signals effect on both wires is different due to noise found at different locations (e.g., one is closer and the other is farther). If wires are twisted, then noise balance can be maintained. For example, suppose in one twist, one wire is closer to the noise source and the other is farther; in the next twist, the reverse is true. Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk). This means that the receiver, which calculates the difference between the two, receives no unwanted signals. The unwanted signals are mostly cancelled out. From the above discussion, it is clear that the number of twists per unit of length (e.g., inch) has some effect on the quality of the cable. Local-area networks, such as 10Base-T and 100Base-T, also use twisted-pair cables.

***Unshielded Versus Shielded Twisted-Pair Cable***

The most common twisted-pair cable used in communications is referred to as **unshielded twisted­pair (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.



**a. I TP**

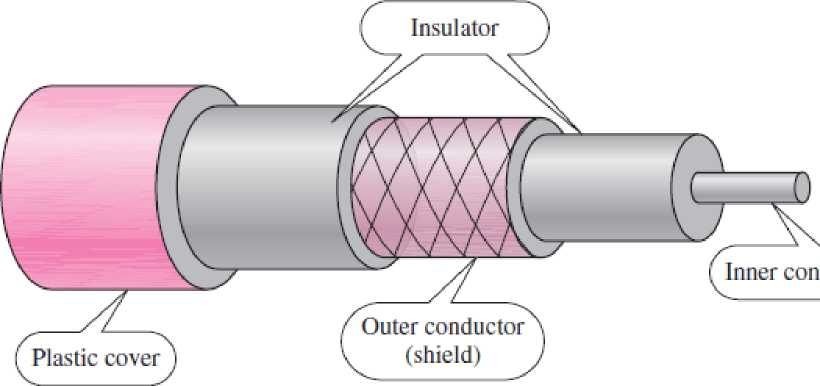
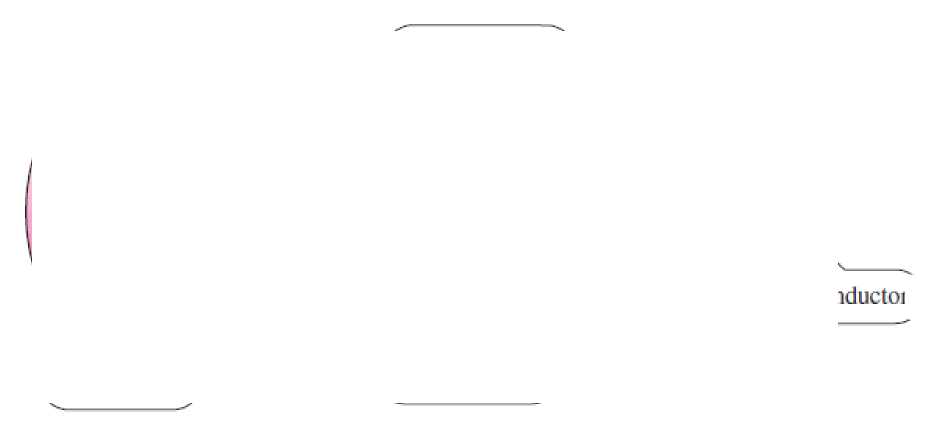
**b. STP**

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 Digital Subscriber Lines (DSL) that are used by the telephone companies to provide high-data- rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.

1. **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 conductor of 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.



The attenuation in co-axial cable is much higher than twisted-pair cable. Although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

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.

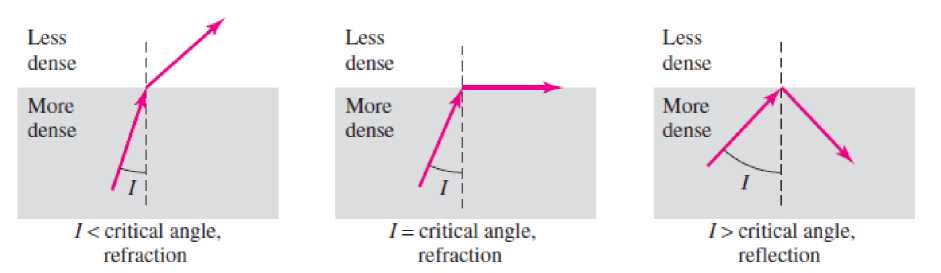
Cable TV networks also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable. Later, however, cable TV providers replaced most of the media with fiber-optic cable; hybrid networks use coaxial cable only at the network boundaries, near the consumer premises. Cable TV uses RG-59 coaxial cable.

Another common application of coaxial cable is in traditional Ethernet LANs. Because of its high bandwidth, and consequently high data rate, coaxial cable was chosen for digital transmission in early Ethernet LANs.

1. **Fiber-Optic Cable**

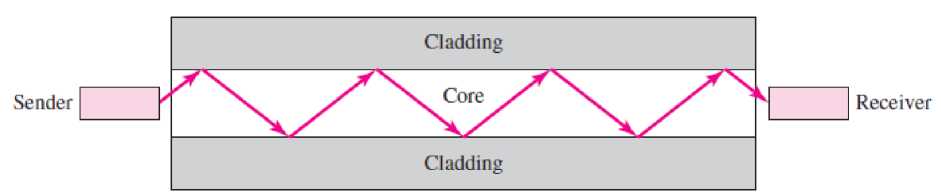
A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. To understand optical fiber, we first need to explore several aspects of the nature of light.

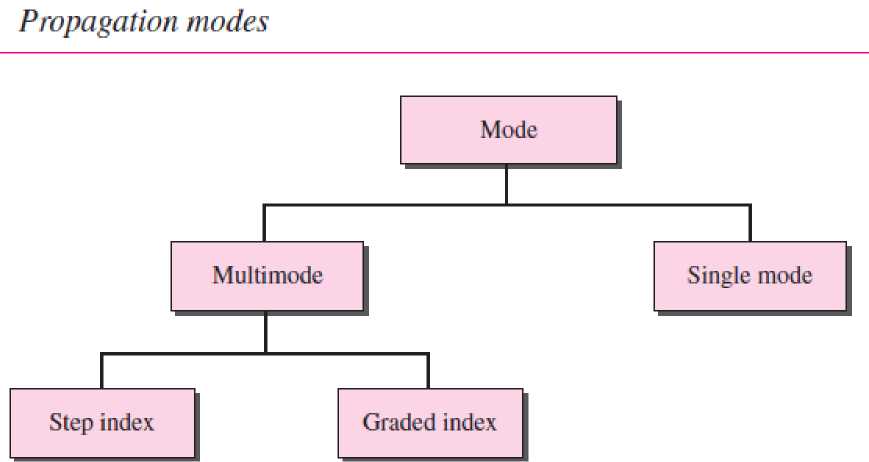
Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction. Following figure shows how a ray of light changes direction when going from a more dense to a less dense substance.



As the figure shows, if the **angle of incidence** *I* (the angle the ray makes with the line perpendicular to the interface between the two substances) is less than the **critical angle,** the ray **refracts** and moves closer to the surface. If the angle of incidence is equal to the critical angle, the light bends along the interface. If the angle is greater than the critical angle, the ray **reflects** (makes a turn) and travels again in the denser substance. The critical angle is a property of the substance, and its value differs from one substance to another.

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.





**Multimode** Multimode is so named because multiple beams from a light source move through the core in different paths.

In **multimode step-index fiber,** the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface, there is an abrupt change due to a lower density; this alters the angle of the beam's motion. The term *step index* refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.

A second type of fiber, called **multimode graded-index fiber,** decreases this distortion of the signal through the cable. The word *index* here refers to the index of refraction. As we saw above, the index of refraction is related to density. A graded-index fiber, therefore, is one with varying densities. Density is highest at the center of the core and decreases gradually to its lowest at the edge.

**Single-Mode** Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The **singlemode fiber** itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density (index of refraction). The decrease in density results in a critical angle that is close enough to 90° to make the propagation of beams almost horizontal. In this case, propagation of different beams is almost identical, and delays are negligible. All the beams arrive at the destination “together” and can be recombined with little distortion to the signal.

**Advantages** Fiber-optic cable has several advantages over metallic cable (twistedpair or coaxial).

* **Higher bandwidth.** Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.
* **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.
* **Immunity to electromagnetic interference.** Electromagnetic noise cannot affect fiber-optic cables.
* **Resistance to corrosive materials.** Glass is more resistant to corrosive materials than copper.
* **Light weight. Fiber-optic cables are much lighter than copper cables.**
* **Greater immunity to tapping. Fiber-optic cables are more immune to tapping than copper cables.**

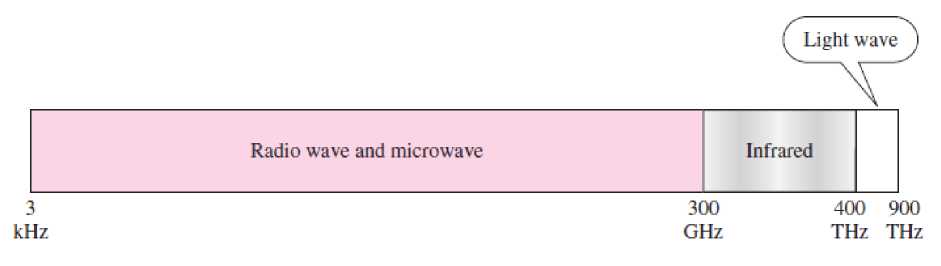
**Disadvantages** There are some disadvantages in the use of optical fiber.

* **Installation and maintenance.** Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
* **Unidirectional light propagation.** Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
* **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.

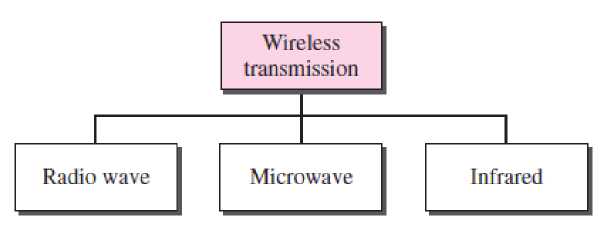
**UNGUIDED MEDIA: WIRELESS**

**Unguided media** 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.

Electromagnetic spectrum for wireless communication



In **ground propagation,** radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals flow out in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal: The greater the power, the greater the distance. In **sky propagation,** higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth. This type of transmission allows for greater distances with lower output power. In **line- of-sight propagation,** very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other and either tall enough or close enough together not to be affected by the curvature of the earth. Line-of-sight propagation is tricky because radio transmissions cannot be completely focused.



Radio Waves

Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called **radio waves.**

Radio waves, for the most part, are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. A sending antenna sends waves that can be received by any receiving antenna. The omnidirectional property has a **disadvantage**, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.

Radio waves, particularly those waves that propagate in the sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as **AM radio**.

Radio waves, particularly those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an **advantage** because, for example, an AM radio can receive signals inside a building. It is a **disadvantage** because we cannot isolate a communication to just inside or outside a building. The radio wave band is relatively narrow, just under 1 GHz, compared to the microwave band. When this band is divided into subbands, the subbands are also narrow, leading to a low data rate for digital communications.

Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Microwaves are unidirectional. When an antenna transmits microwave waves, 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:

* Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall. The curvature of the earth as well as other blocking obstacles do not allow two short towers to communicate by using microwaves. Repeaters are often needed for long distance communication.
* Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.
* The microwave band is relatively wide, almost 299 GHz. Therefore wider subbands can be assigned, and a high data rate is possible
* Use of certain portions of the band requires permission from authorities.

Infrared

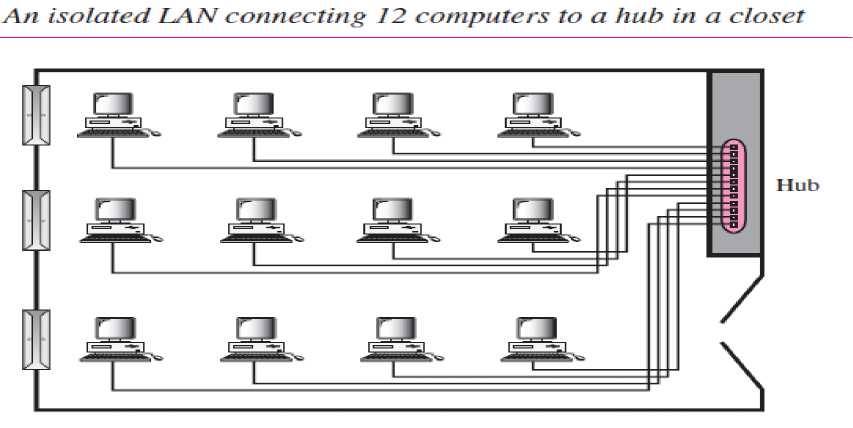
**Infrared waves,** with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This **advantageous** characteristic prevents **interference** between one system and another; a short-range communication system in one room cannot be affected by another system in the next room. Infrared remote control does not interfere with the use of the remote by our neighbours. However, this same characteristic makes infrared signals **useless for long-range communication**. In addition, Infrared waves cannot be used outside a building because the sun's rays contain infrared waves that can interfere with the communication.

1. Categories of Networks

The category into which a network falls is determined by its size. A LAN normally covers an area less than 2 miles; a WAN can be worldwide. Networks of a size in between are normally referred to as metropolitan area networks and span tens of miles.

1. ***Local Area Network***

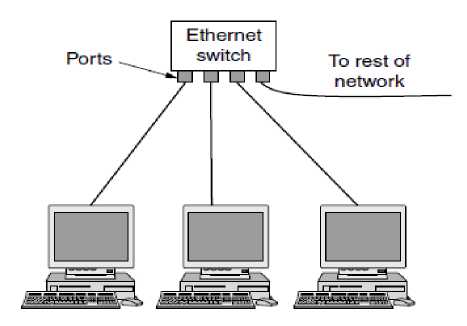
A **local area network (LAN)** is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers.



LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data. When LANs are used by companies, they are called **enterprise networks**.

**a. 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. Knowing these bounds helps with the task of designing network protocols. Typically, wired LANs run at speeds of 100 Mbps to 1 Gbps, have low delay (microseconds or nanoseconds), and make very few errors. Newer LANs can operate at up to 10 Gbps. Compared to wireless networks; wired LANs exceed them in all dimensions of performance. It is just easier to send signals over a wire or through a fiber than through the air.

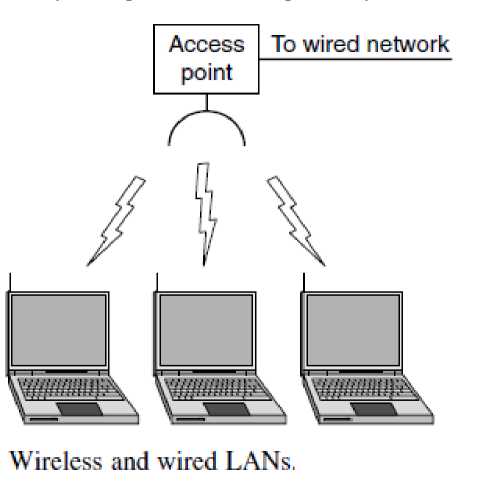
The topology of many wired LANs is built from point-to-point links. IEEE 802.3, popularly called **Ethernet**, is, by far, the most common type of wired LAN. In Figure shows a sample topology of **switched Ethernet**. Each computer speaks the Ethernet protocol and connects to a box called a **switch** with a point-to-point link. A switch has multiple **ports**, each of which can connect to one computer. The job of the switch is to relay packets between computers that are attached to it, using the address in each packet to determine which computer to send it to. To build larger LANs, switches can be plugged into each other using their ports.



Switched Ethernet

There are other wired LAN topologies too. In fact, switched Ethernet is a modern version of the original Ethernet design that broadcast all the packets over a single linear cable. At most one machine could successfully transmit at a time, and a distributed arbitration mechanism was used to resolve conflicts. It used a simple algorithm: computers could transmit whenever the cable was idle. If two or more packets collided, each computer just waited a random time and tried later.

1. **Wireless LANs** are used at places where cable installation is too much difficult. In these systems, every computer has a **radio modem** and **an antenna** that it uses to communicate with other computers. In most cases, each computer talks to a device in the ceiling as shown in Figure. This device, called an **AP** (**Access Point**), **wireless router**, or **base station**, relays packets between the wireless computers and also between them and the Internet. However, if other computers are close enough, they can communicate directly with one another in a peer-to-peer configuration. There is a standard for wireless LANs called **IEEE 802.11**, popularly known as **WiFi**, which has become very widespread. It runs at speeds anywhere from 11 to hundreds of Mbps.



**Bluetooth**

**Bluetooth** is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop) and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a **picone**t. A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability. A Bluetooth LAN, by nature, cannot be large. If there are many gadgets that try to connect, there is chaos.

Bluetooth technology has several applications. Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology. Monitoring devices can communicate with sensor devices in a small health care center. Home security devices can use this technology to connect different sensors to the main security controller. Conference attendees can synchronize their laptop computers at a conference.

Bluetooth was originally started as a project by the Ericsson Company. It is named for Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway. *Blaatand* translates to *Bluetooth* in English.

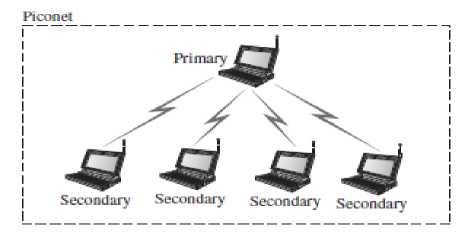
Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard. The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or a hall.

Architecture of Bluetooth

Bluetooth defines two types of networks: piconet and scatternet.

***Piconets***

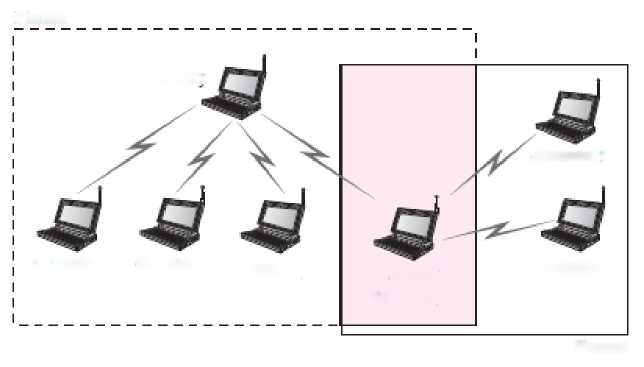
A Bluetooth network is called a **piconet,** or a small net. A piconet can have up to eight stations, one of which is called the **primary;**! the rest are called **secondaries.** All the secondary stations synchronize their clocks and hopping sequence with the primary. The communication between the primary and the secondary can be one-to-one or one-to-many.



Although a piconet can have a maximum of seven secondaries, an additional eight secondaries can be in the *parked state.* A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state. Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

***Scatternet***

Piconets can be combined to form what is called a **scatternet.** A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets.



Primarv

Piconet

Piconet

Secondary

Primary/

Secondary

Secondary

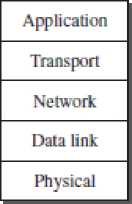
Secondary Secondary secondary

1. **Connecting LANs**

**CONNECTING DEVICES**

The five categories contain devices which can be defined as

1. Those which operate below the physical layer such as a passive hub.
2. Those which operate at the physical layer (a repeater or an active hub).
3. Those which operate at the physical and data link layers (a bridge or a two-layer switch).
4. Those which operate at the physical, data link, and network layers (a router or a three-layer switch).
5. Those which can operate at all five layers (a gateway).

**15.1 *Five categories of connecting devices***

Gale-wav

Router or three-layer switch **Bridge**

**w** two-layer switch

Repealer  
**or hub**

**Passive hub**

Passive Hubs

A passive hub is just a connector. It connects the wires coming from different branches. In a star­topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point.

Repeaters

A **repeater** is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern. The repeater then sends the refreshed signal. A repeater does not actually connect two LANs; it connects two segments of the same LAN.

Active Hubs

An active **hub** is actually a multiport repeater. It is normally used to create connections between stations in a physical star topology. s

Bridges

A **bridge** operates in both the physical and the data link layer. As a physical layer device, it regenerates the signal it receives. As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame.

Two-Layer Switches

The **two-layer switch** performs at the physical and data link layers. A two-layer switch is a bridge, a bridge with many ports and a design that allows better (faster) performance. A bridge with a few ports can connect a few LANs together. A bridge with many ports may be able to allocate a unique port to each station, with each station on its own independent entity. This means no competing traffic.

Routers

A **router** is a three-layer device that routes packets based on their logical addresses (host-to-host addressing). A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route. The routing tables are normally dynamic and are updated using routing protocols.

Three-Layer Switches

A three-layer switch is a router, but a faster and more sophisticated. The switching fabric in a three- layer switch allows faster table lookup and forwarding.

Gateway

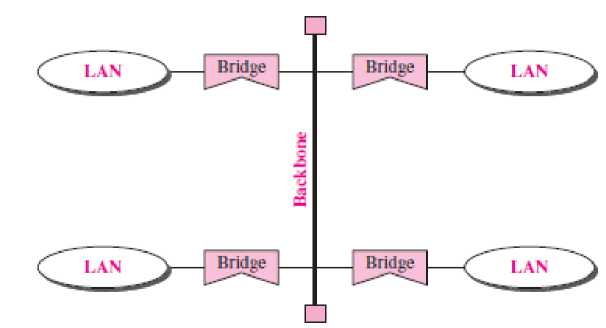
A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model. A gateway takes an application message, reads it, and interprets it. This means that it can be used as a connecting device between two internetworks that use different models. For example, a network designed to use the OSI model can be connected to another network using the Internet model. The gateway connecting the two systems can take a frame as it arrives from the first system, move it up to the OSI application layer, and remove the message.

**BACKBONE NETWORKS**

A backbone network allows several LANs to be connected. In a backbone network, no station is directly connected to the backbone; the stations are part of a LAN, and the backbone connects the LANs. The backbone is itself a LAN that uses a LAN protocol such as Ethernet; each connection to the backbone is itself another LAN.

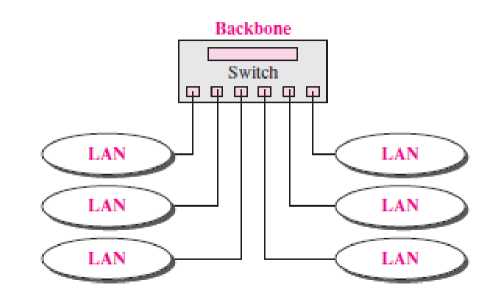
Bus Backbone

In a **bus backbone,** the topology of the backbone is a bus. Bus backbones are normally used as a distribution backbone to connect different buildings in an organization. Each building can comprise either a single LAN or another backbone (normally a star backbone). A good example of a bus backbone is one that connects single- or multiple-floor buildings on a campus. Each single-floor building usually has a single LAN. Each multiple-floor building has a backbone (usually a star) that connects each LAN on a floor. A bus backbone can interconnect these LANs and backbones.



Star Backbone

In a **star backbone,** sometimes called a collapsed or switched backbone, the topology of the backbone is a star. In this configuration, the backbone is just one switch that connects the LANs.



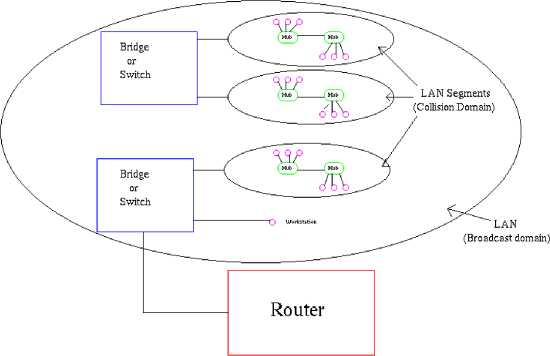
Star backbones are mostly used as a distribution backbone inside a building. In a multifloor building, we usually find one LAN that serves each particular floor. A star backbone connects these LANs. The backbone network, which is just a switch, can be installed in the basement or the first floor, and separate cables can run from the switch to each LAN. If the individual LANs have a physical star topology, either the hubs (or switches) can be installed in a closet on the corresponding floor, or all can be installed close to the switch. We often find a rack or chassis in the basement where the backbone switch and all hubs or switches are installed.

1. **VIRTUAL LANs**

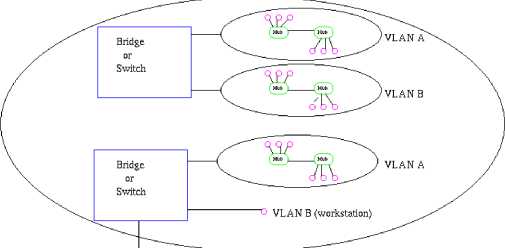
A local area network, or LAN, provides the nodes connected to it with direct (Layer 2) access to one another. It is usually comprised of one or more Ethernet switches. Computers on different LANs talk to each other using Layer 3 (IP), via a router.

In a traditional LAN, workstations are connected to each other by means of a hub or a repeater. These devices propagate any incoming data throughout the network. However, if two people attempt to send information at the same time, a collision will occur and all the transmitted data will be lost. Once the collision has occurred, it will continue to be propagated throughout the network by hubs and repeaters. The original information will therefore need to be resent after waiting for the collision to be resolved, thereby incurring a significant wastage of time and resources. To prevent collisions from traveling through all the workstations in the network, a bridge or a switch can be used. These devices will not forward collisions, but will allow broadcasts (to every user in the network) and multicasts (to a pre-specified group of users) to pass through. A router may be used to prevent broadcasts and multicasts from traveling through the network.

The workstations, hubs, and repeaters together form a LAN segment. A LAN segment is also known as a collision domain since collisions remain within the segment. The area within which broadcasts and multicasts are confined is called a broadcast domain or LAN. Thus a LAN can consist of one or more LAN segments. Defining broadcast and collision domains in a LAN depends on how the workstations, hubs, switches, and routers are physically connected together. This means that everyone on a LAN must be located in the same area.

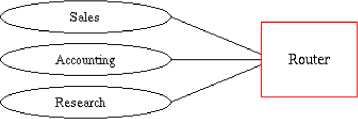


VLAN's allow a network manager to logically segment a LAN into different broadcast domains (see *Figure).* Since this is a logical segmentation and not a physical one, workstations do not have to be physically located together. Users on different floors of the same building, or even in different buildings can now belong to the same LAN.



Router

Physical View



Logical **View**

VLAN's offer a number of advantages over traditional LAN's. They are:

1. **Performance**

In networks where traffic consists of a high percentage of broadcasts and multicasts, VLAN's can reduce the need to send such traffic to unnecessary destinations.

1. **Formation of Virtual Workgroups**

Nowadays, it is common to find cross-functional product development teams with members from different departments such as marketing, sales, accounting, and research. These workgroups are usually formed for a short period of time. During this period, communication between members of the workgroup will be high. To contain broadcasts and multicasts within the workgroup, a VLAN can be set up for them. With VLAN's it is easier to place members of a workgroup together. Without VLAN's, the only way this would be possible is to physically move all the members of the workgroup closer together. However, virtual workgroups do not come without problems.

1. Simplified Administration

Seventy percent of network costs are a result of adds, moves, and changes of users in the network. Every time a user is moved in a LAN, recabling, new station addressing, and reconfiguration of hubs and routers becomes necessary. Some of these tasks can be simplified with the use of VLAN's. If a user is moved within a VLAN, reconfiguration of routers is unnecessary.

1. Reduced Cost

VLAN's can be used to create broadcast domains which eliminate the need for expensive routers.

1. Security

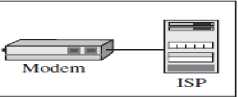
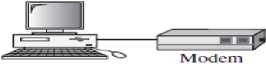
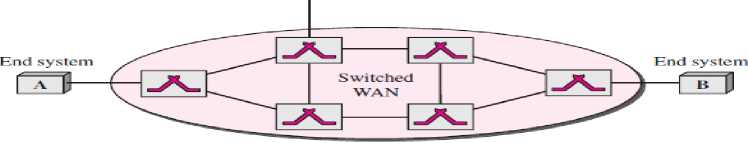
Periodically, sensitive data may be broadcast on a network. In such cases, placing only those users who can have access to that data on a VLAN can reduce the chances of an outsider gaining access to the data. VLAN's can also be used to control broadcast domains, set up firewalls, restrict access, and inform the network manager of an intrusion.

1. ***Wide Area Network***

A **wide area network (WAN)** provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. Normally two types of WAN is referred to the first as a switched WAN and to the second as a point-to-point WAN.

The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN.

The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP). This type of WAN is often used to provide Internet access. An early example of a switched WAN is X.25, a network designed to provide connectivity between end users. A good example of a switched WAN is the asynchronous transfer mode (ATM) network, which is a network with fixed-size data unit packets called cells.



**C? I Find system**

**a. Switched WAIS**

**Computer**

**Point-to-point  
WAN**

**l>. Point-to-point WAN**

1. ***Metropolitan Area Networks***

A **metropolitan area network (MAN)** is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city. A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL **Sangeeta Arora**

line to the customer. Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet.

(iv) Interconnection of Networks: Internetwork

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

