MODULE 1

1.1 DATA COMMUNICATIONS

- Data communication is defined as exchange of data between 2 devices over a transmission-medium.
- A communication-system is made up of

  → hardware (physical equipment) and

  → software (programs)
- For data-communication, the communicating-devices must be part of a communication-system.
- Four attributes of a communication-system:

  1) Delivery

  ➢ The system must deliver data to the correct destination.

  2) Accuracy

  ➢ The system must deliver the data accurately.

  ➢ Normally, the corrupted-data are unusable.

  3) Timeliness

  ➢ The system must deliver audio/video data in a timely manner.

  ➢ This kind of delivery is called real-time transmission.

  ➢ Data delivered late are useless.

  4) Jitter

  ➢ Jitter refers to the variation in the packet arrival-time.

  ➢ In other words, jitter is the uneven delay in the delivery of audio/video packets.

1.1.1 Components of Communication System

- Five components of a communication-system (Figure 1.1):

  1) Message

  2) Sender

  3) Receiver

  4) Transmission-Medium

  5) Protocol

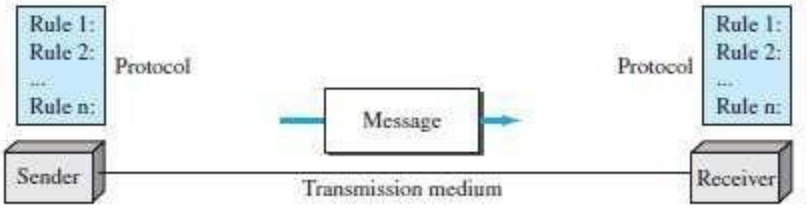


Figure 1.1 *Five components of data communication*

1) Message

- Message is the information (or data) to be communicated.
- Message may consist of
  - → number/text
  - → picture or
  - → audio/video

2) Sender

- Sender is the device that sends the data-message.
- Sender can be
  - → computer and
  - → mobile phone

3) Receiver

- Receiver is the device that receives the message.
- Receiver can be
  - → computer and
  - → mobile phone

4) Transmission Medium

- Transmission-medium is physical-path by which a message travels from sender to receiver.
- Transmission-medium can be wired or wireless.
- Examples of wired medium:
  - → twisted-pair wire (used in landline telephone)
  - → coaxial cable (used in cable TV network)
  - → fiber-optic cable
- Examples of wireless medium:
  - → radio waves
  - → microwaves
  - → infrared waves (ex: operating TV using remote control)

5) Protocol

- A protocol is a set of rules that govern data-communications.
- In other words, a protocol represents an agreement between the communicating-devices.
- Without a protocol, 2 devices may be connected but not communicating.

1.1.2 Data Representation

- Five different forms of information:

1) Text

➢ Text is represented as a bit-pattern. (Bit-pattern □ sequence of bits: 0s or 1s).

➢ Different sets of bit-patterns are used to represent symbols (or characters).

➢ Each set is called a code.

➢ The process of representing symbols is called encoding.

➢ Popular encoding system: ASCII, Unicode.

2) Number

➢ Number is also represented as a bit-pattern.

➢ ASCII is not used to represent number. Instead, number is directly converted to binary-form.

3) Image

➢ Image is also represented as a bit-pattern.

➢ An image is divided into a matrix of pixels (picture-elements).

➢ A pixel is the smallest element of an image. (Pixel □ Small dot)

➢ The size of an image depends upon number of pixels (also called resolution).For example: An image can be divided into 1000 pixels or 10,000 pixels.

➢ Two types of images:

i) Black & White Image

¤ If an image is black & white, each pixel can be represented by a value either 0 or 1.

¤ For example: Chessboard

ii) Color Image

¤ There are many methods to represent color images.

¤ RGB is one of the methods to represent color images.

¤ RGB is called so called '.' each color is combination of 3 colors: red, green & blue.

4) Audio

➢ Audio is a representation of sound.

➢ By nature, audio is different from text, numbers, or images. Audio is continuous, not discrete.

5) Video

➢ Video is a representation of movie.

➢ Video can either

→ be produced as a continuous entity (e.g., by a TV camera), or

→ be a combination of images arranged to convey the idea of motion.

1.1.3 Direction of Data Flow

- Three ways of data-flow between 2 devices (Figure 1.2):

    1) Simplex
    2) Half-duplex
    3) Full-duplex

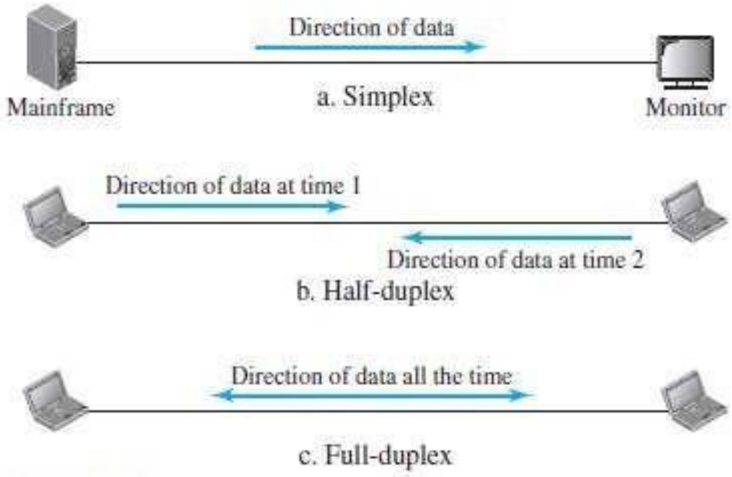

Direction of data
Mainframe
a. Simplex
Monitor
Direction of data at time 1
Direction of data at time 2
b. Half-duplex
Direction of data all the time
c. Full-duplex

Figure 1.2 *Data flow (simplex, half-duplex, and full-duplex)*

1) Simplex

➢ The communication is unidirectional

(For ex: The simplex mode is like a one-way street).

➢ On a link, out of 2 devices:

i) Only one device can transmit.

ii) Another device can only receive.

➢ For example (Figure 1.2a):

The monitor can only accept output.

➢ Entire-capacity of channel is used to send the data in one direction.

2) Half Duplex

➢ Both the stations can transmit as well as receive but not at the same time.

(For ex: The half-duplex mode is like a one-lane road with 2 directional traffic).

➢ When one station is sending, the other can only receive and vice-versa.

➢ For example (Figure 1.2b): Walkie-talkies

➢ Entire-capacity of a channel is used by one of the 2 stations that are transmitting the data.

3) Full Duplex

➢ Both stations can transmit and receive at the same time.

(For ex: The full-duplex is like a 2-way street with traffic flowing in both directions at thesame time).

- For example (Figure 1.2c):

  Mobile phones (When 2 people are communicating by a telephone line, both can listenand talk at the same time)

- Entire-capacity of a channel is shared by both the stations that are transmitting the data.

1.2 NETWORKS

- A network is defined as a set of devices interconnected by communication-links.
- This interconnection among computers facilitates information sharing among them.
- Computers may connect to each other by either wired or wireless media.
- Often, devices are referred to as nodes.
- A node can be any device capable of sending/receiving data in the network.
- For example: Computer & Printer
- The best-known computer network is the Internet.

1.2.1 Network Criteria

- A network must meet following 3 criteria's:

1) Performance

- Performance can be measured using i) Transit-time or ii) Response-time.

  i) Transit Time is defined as time taken to travel a message from one device to another.

  ii) Response Time is defined as the time elapsed between enquiry and response.

- The network-performance depends on following factors:

  i) Number of users

  ii) Type of transmission-medium

  iii) Efficiency of software

- Often, performance is evaluated by 2 networking-metrics: i) throughput and ii) delay.
- Good performance can be obtained by achieving higher throughput and smaller delay times

2) Reliability

- Reliability is measured by

  → frequency of network-failure

  → time taken to recover from a network-failure

  → network's robustness in a disaster

- More the failures are, less is the network's reliability.

3) Security

- Security refers to the protection of data from the unauthorized access or damage.
- It also involves implementing policies for recovery from data-losses.

1.2.2 Physical Structures

1.2.2.1 Type of Connection

- Two types of connections (Figure 1.3):

1) Point-to-Point

- Only two devices are connected by a dedicated-link (Figure 1.3a).
- Entire-capacity of the link is reserved for transmission between those two devices.
- For example: Point-to-Point connection b/w remote-control & TV for changing the channels.

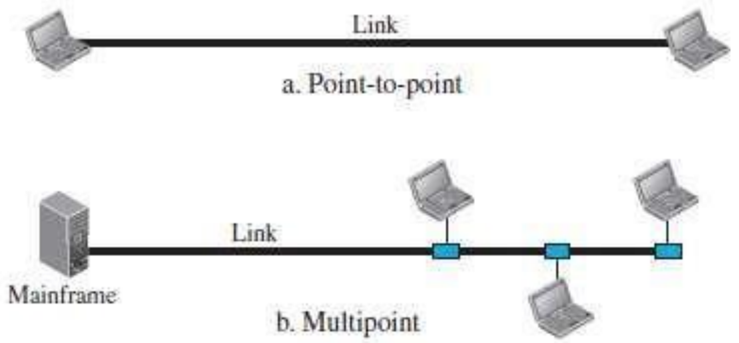
2) Multipoint (Multi-Drop)

- Three or more devices share a single link.
- The capacity of the channel is shared, either spatially or temporally (Figure 1.3b).

i) If link is used simultaneously by many devices, then it is spatially shared connection.

ii) If user takes turns while using the link, then it is time shared (temporal) connection.

(spatially□space or temporally □time)



a. Point-to-point

b. Multipoint

Figure 1.3 *Types of connections: point-to-point and multipoint*

1.2.2.2 Physical Topology

- The physical-topology defines how devices are connected to make a network.
- Four basic topologies are:

1) Mesh

2) Star

3) Bus and

4) Ring

1.2.2.2.1 Bus Topology

- All the devices are connected to the single cable called bus (Figure 1.4).
- Every device communicates with the other device through this bus.
- A data from the source is broadcasted to all devices connected to the bus.
- Only the intended-receiver, whose physical-address matches, accepts the data.

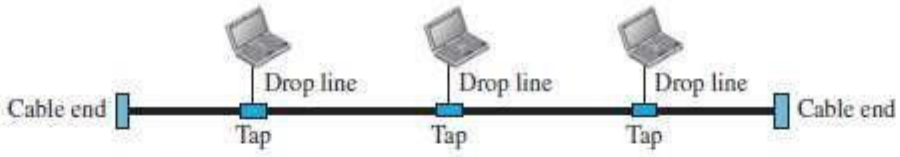


Figure 1.4 *A bus topology connecting three stations*

- Devices are connected to the bus by drop-lines and taps.
- A drop-line is a connection running between the device and the bus.
- A tap is a connector that links to the bus or
- Advantages:
  1) Easy installation.
  2) Cable required is the least compared to mesh/star topologies.
  3) Redundancy is eliminated.
  4) Costs less (Compared to mesh/star topologies).
  5) Mostly used in small networks. Good for LAN.
- Disadvantages:
  1) Difficult to detect and troubleshoot fault.
  2) Signal reflection at the taps can cause degradation in quality.
  3) A fault/break in the cable stops all transmission.
  4) There is a limit on
     i) Cable length
     ii) Number of nodes that can be connected.
  5) Security is very low because all the devices receive the data sent from the source.

1.2.2.2.2 Star Topology

- All the devices are connected to a central controller called a hub (Figure 1.5).
- There exists a dedicated point-to-point link between a device & a hub.
- The devices are not directly linked to one another. Thus, there is no direct traffic between devices.
- The hub acts as a junction:

  If device-1 wants to send data to device-2, the

  device-1 sends the data to the hub,

  then the hub relays the data to the device-2.

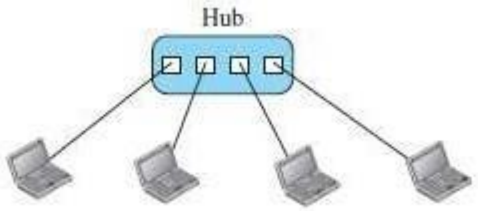


Figure 1.5 *A star topology connecting four stations*

- Advantages:
  1) Less expensive: Each device needs only one link & one I/O port to connect it to any devices.
  2) Easy installation & reconfiguration: Nodes can be added/removed w/o affecting the network.
  3) Robustness: If one link fails, it does not affect the entire system.
  4) Easy to detect and troubleshoot fault.
  5) Centralized management: The hub manages and controls the whole network.
- Disadvantages:
  1) Single point of failure: If the hub goes down, the whole network is dead.
  2) Cable length required is the more compared to bus/ring topologies.
  3) Number of nodes in network depends on capacity of hub.

1.2.2.2.3 Ring Topology

- Each device is connected to the next, forming a ring (Figure 1.6).
- There are only two neighbors for each device.
- Data travels around the network in one direction till the destination is reached.
- Sending and receiving of data takes place by the help of token.
- Each device has a repeater.
- A repeater

  → receives a signal on transmission-medium &

  → regenerates & passes the signal to next device.

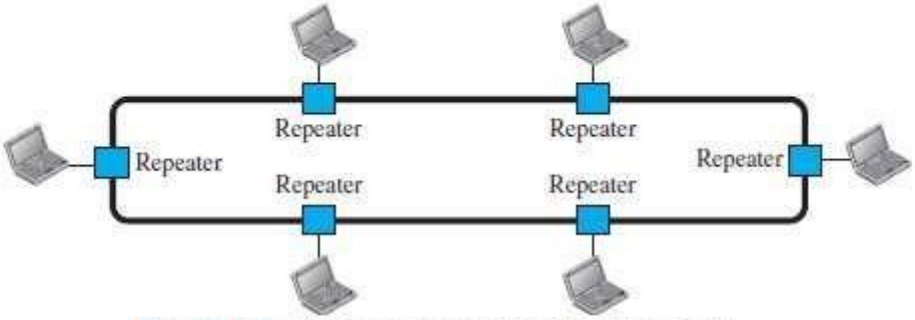


Figure 1.6 *A ring topology connecting six stations*

- Advantages:

  1) Easy installation and reconfiguration.

     To add/delete a device, requires changing only 2 connections.

  3) Fault isolation is simplified.

     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.

  3) Congestion reduced: Because all the traffic flows in only one direction.

- Disadvantages:

  1) Unidirectional traffic.

  2) A fault in the ring/device stops all transmission.

     The above 2 drawbacks can be overcome by using dual ring.

  3) There is a limit on

     i) Cable length &

     ii) Number of nodes that can be connected.

  4) Slower: Each data must pass through all the devices between source and destination.

1.2.2.2.4 Mesh Topology

- All the devices are connected to each other (Figure 1.7).
- There exists a dedicated point-to-point link between all devices.
- There are n(n-1) physical channels to link n devices.
- Every device not only sends its own data but also relays data from other nodes.
- For ‘n’ nodes,
  → there are n(n-1) physical-links
  → there are n(n-1)/2 duplex-mode links
- Every device must have (n–1) I/O ports to be connected to the other (n-1) devices.

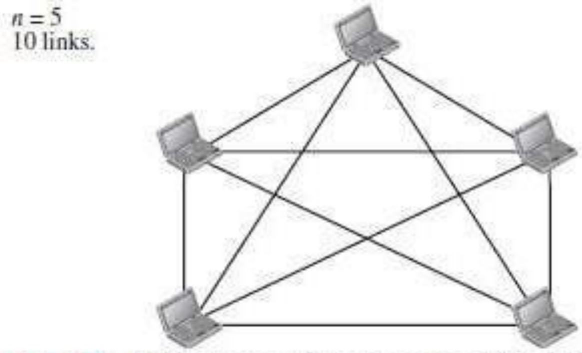


Figure 1.7 *A fully connected mesh topology (five devices)*

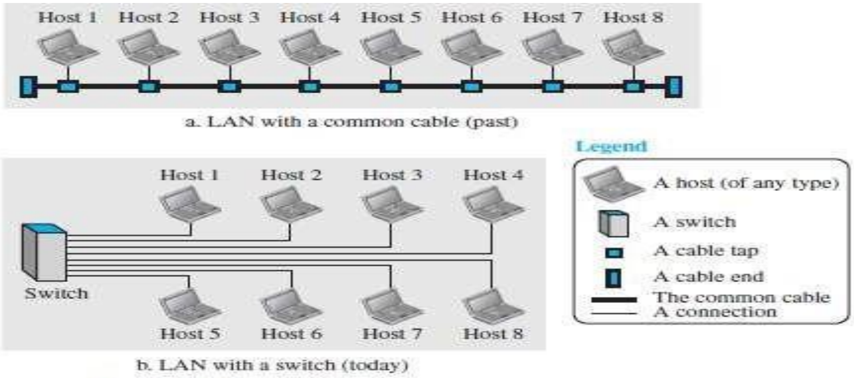
- Advantages:
  1) Congestion reduced: Each connection can carry its own data load.
  2) Robustness: If one link fails, it does not affect the entire system.
  3) Security: When a data travels on a dedicated-line, only intended-receiver can see the data.
  4) Easy fault identification & fault isolation: Traffic can be re-routed to avoid problematic links.
- Disadvantages:
  1) Difficult installation and reconfiguration.
  2) Bulk of wiring occupies more space than available space.
  3) Very expensive: as there are many redundant connections.
  4) Not mostly used in computer networks. It is commonly used in wireless networks.
  5) High redundancy of the network-connections.

1.3 Network Types

- Two popular types of networks:
  1) LAN (Local Area Network) &
  2) WAN (Wide Area Network)

1.3.1 LAN

- LAN is used to connect computers in a single office, building or campus (Figure 1.8).
- LAN is usually privately owned network.
- A LAN can be simple or complex.
  1) Simple: LAN may contain 2 PCs and a printer.
  2) Complex: LAN can extend throughout a company.
- Each host in a LAN has an address that uniquely defines the host in the LAN.
- A packet sent by a host to another host carries both source host's and destination host's addresses.
- LANs use a smart connecting switch.
- The switch is able to
  → recognize the destination address of the packet &
  → guide the packet to its destination.
- The switch
  → reduces the traffic in the LAN &
  → allows more than one pair to communicate with each other at the same time.
- Advantages:
  1) Resource Sharing
  ➢ Computer resources like printers and hard disks can be shared by all devices on the network.
  2) Expansion
  ➢ Nowadays, LANs are connected to WANs to create communication at a wider level.



a. LAN with a common cable (past)

b. LAN with a switch (today)

Figure 1.8 *An isolated LAN in the past and today*

1.3.2 WAN

- WAN is used to connect computers anywhere in the world.
- WAN can cover larger geographical area. It can cover cities, countries and even continents.
- WAN interconnects connecting devices such as switches, routers, or modems.
- Normally, WAN is
  → created & run by communication companies (Ex: BSNL, Airtel)
  → leased by an organization that uses it.
- A WAN can be of 2 types:

1) Point-to-Point WAN

➢ A point-to-point WAN is a network that connects 2 communicating devices through a transmission media (Figure 1.9).

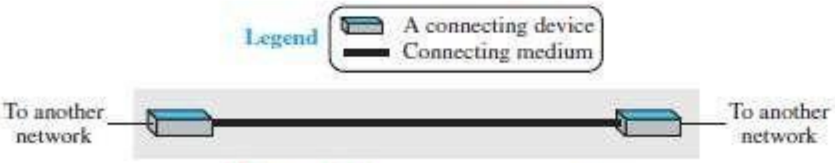


Figure 1.9 *A point-to-point WAN*

2) Switched WAN

➢ A switched WAN is a network with more than two ends.

➢ The switched WAN can be the backbones that connect the Internet.

➢ A switched WAN is a combination of several point-to-point WANs that are connected by switches (Figure 1.10).

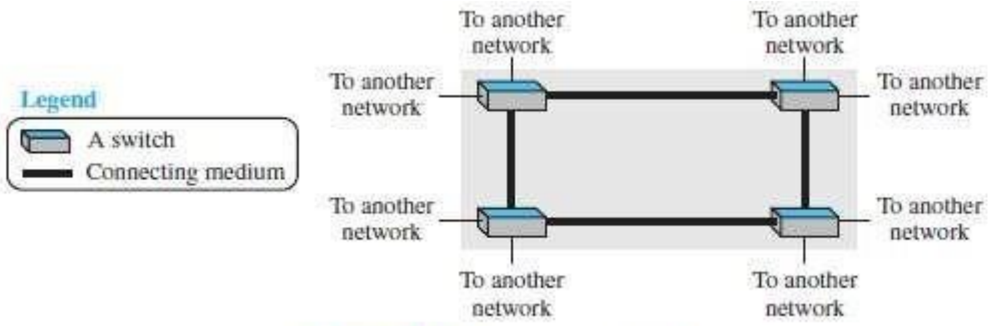


Figure 1.10 *A switched WAN*

1.3.2.1 Internetwork

- A network of networks is called an internet. (Internet inter-network) (Figure 1.12).
- For example (Figure 1.11):

➢ Assume that an organization has two offices,

i) First office is on the east coast &

ii) Second office is on the west coast.

➢ Each office has a LAN that allows all employees in the office to communicate with each other.

➢ To allow communication between employees at different offices, the management leases a point-to-point dedicated WAN from a ISP and connects the two LANs.

(ISP Internet service provider such as a telephone company ex: BSNL).

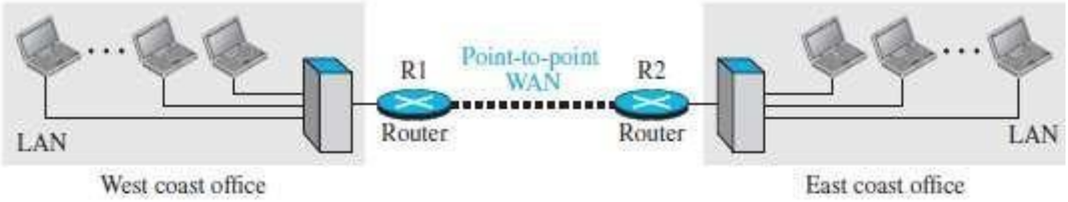


Figure 1.11 *An internetwork made of two LANs and one point-to-point WAN*

➢ When a host in the west coast office sends a message to another host in the same office, therouter 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 eastcoast, router R1 routes the packet to router R2, and the packet reaches the destination.

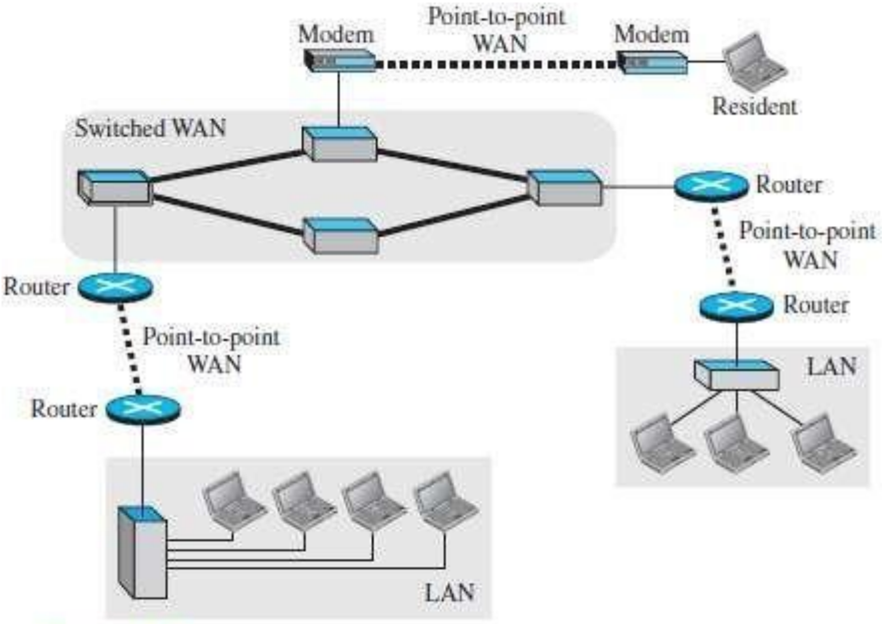


Figure 1.12 *A heterogeneous network made of four WANs and three LANs*

1.3.3 LAN vs. WAN

Parameters	LAN	WAN
Expands to	Local Area Network	Wide Area Network
Meaning	LAN is used to connect computers in a single office, building or campus	WAN is used to connect computers in a large geographical area suchas countries
Ownership of network	Private	Private or public
Range	Small: up to 10 km	Large: Beyond 100 km
Speed	High: Typically 10, 100 and 1000 Mbps	Low: Typically 1.5 Mbps
Propagation Delay	Short	Long
Cost	Low	High
Congestion	Less	More
Design & maintenance	Easy	Difficult
Fault Tolerance	More Tolerant	Less Tolerant
Media used	Twisted pair	Optical fiber or radio waves
Used for	College, Hospital	Internet
Interconnects	LAN interconnects hosts	WAN interconnects connecting devices such as switches, routers,or modems

1.3.4 Switching

- An internet is a switched network in which a switch connects at least two links together.
- A switch needs to forward data from a network to another network when required.
- Two types of switched networks are 1) circuit-switched and 2) packet-switched networks.

1.3.4.1 Circuit Switched Network

- ➢ A dedicated connection, called a circuit, is always available between the two end systems.
- ➢ The switch can only make it active or inactive.

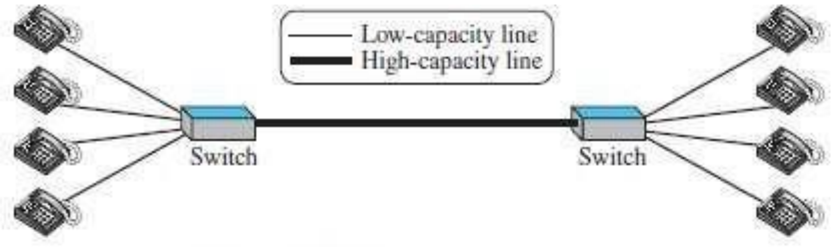


Figure 1.13 *A circuit-switched network*

- ¤ As shown in Figure 1.13, the 4 telephones at each side are connected to a switch.
- ¤ The switch connects a telephone at one side to a telephone at the other side.
- ¤ A high-capacity line can handle 4 voice communications at the same time.

¤ The capacity of high line can be shared between all pairs of telephones.

¤ The switch is used for only forwarding.

➢ Advantage:

A circuit-switched network is efficient only when it is working at its full capacity.

➢ Disadvantage:

Most of the time, the network is inefficient because it is working at partial capacity.

1.3.4.2 Packet Switched Network

➢ In a computer network, the communication between the 2 ends is done in blocks of data called packets.

➢ The switch is used for both storing and forwarding because a packet is an independent entitythat can be stored and sent later.

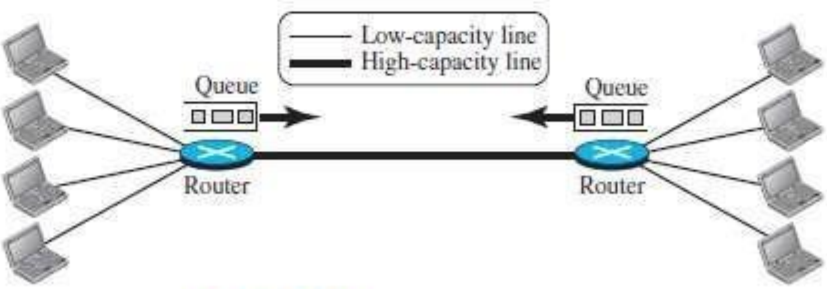


Figure 1.14 *A packet-switched network*

¤ As shown in Figure 1.14, the 4 computers at each side are connected to a router.

¤ A router has a queue that can store and forward the packet.

¤ The high-capacity line has twice the capacity of the low-capacity line.

¤ If only 2 computers (one at each site) need to communicate with each other, there isno waiting for the packets.

¤ However, if packets arrive at one router when high-capacity line is at its full capacity,the packets should be stored and forwarded.

➢ Advantages:

A packet-switched network is more efficient than a circuit switched network.

➢ Disadvantage:

The packets may encounter some delays.

[Note: Packet Switching is explained in detail at the end of the chapter]

1.3.5 The Internet Today

- A network of networks is called an internet. (Internet □ inter-network)
- Internet is made up of (Figure 1.15)
  1) Backbones
  2) Provider networks &
  3) Customer networks

1) Backbones

- ➢ Backbones are large networks owned by communication companies such as BSNL and Airtel.
- ➢ The backbone networks are connected through switching systems, called peering points.

2) Provider Networks

- ➢ Provider networks use the services of the backbones for a fee.
- ➢ Provider networks are connected to backbones and sometimes to other provider networks.

3) Customer Networks

- ➢ Customer networks actually use the services provided by the Internet.
- ➢ Customer networks 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.

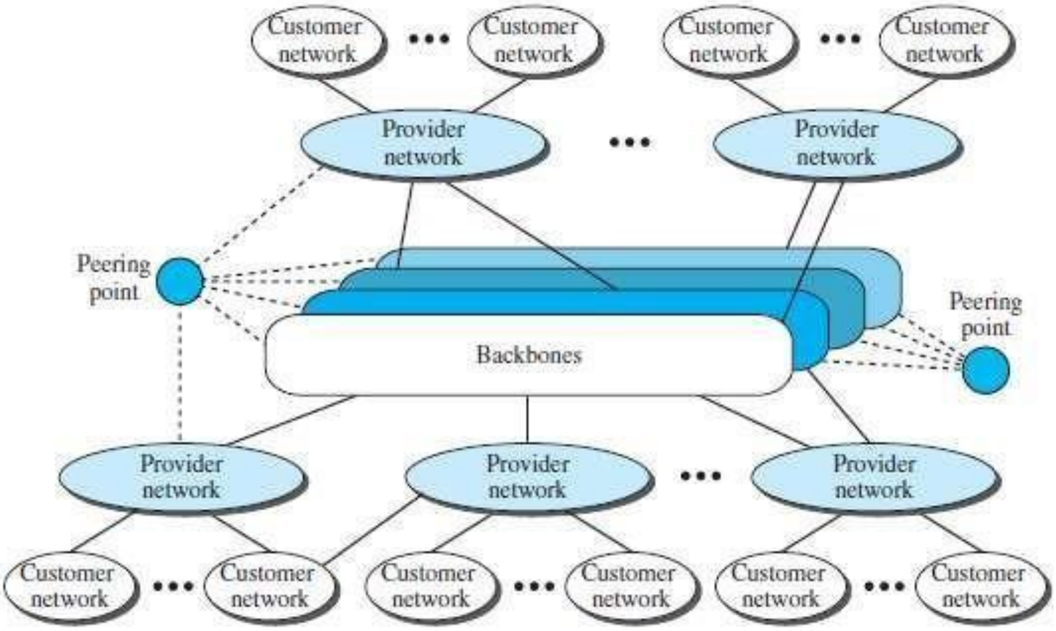


Figure 1.15 *The Internet today*

1.3.6 Accessing the Internet

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

1) Using Telephone Networks

➢ Most residences have telephone service, which means they are connected to a telephone network.

➢ Most telephone networks have already connected themselves to the Internet.

➢ Thus, residences can connect to the Internet using a point-to-point WAN.

➢ This can be done in two ways:

A) Dial-up service

¤ A modem can be added to the telephone line.

¤ A modem converts data to voice.

¤ The software installed on the computer

→ dials the ISP &

→ imitates making a telephone connection.

¤ Disadvantages:

i) The dial-up service is very slow.

ii) When line is used for Internet connection, it cannot be used for voiceconnection.

iii) It is only useful for small residences.

B) DSL Service

¤ DSL service also allows the line to be used simultaneously for voice & data communication.

¤ Some telephone companies have upgraded their telephone lines to provide higherspeed Internet services to residences.

2) Using Cable Networks

➢ A residence can be connected to the Internet by using cable service.

➢ Cable service provides a higher speed connection.

➢ The speed varies depending on the number of neighbors that use the same cable.

3) Using Wireless Networks

➢ A residence can use a combination of wireless and wired connections to access the Internet.

➢ A residence can be connected to the Internet through a wireless WAN.

4) Direct Connection to the Internet

➢ A large organization can itself become a local ISP and be connected to the Internet.

- The organization
  - → leases a high-speed WAN from a carrier provider and
  - → connects itself to a regional ISP.

1.4 PROTOCOL LAYERING

- A protocol defines the rules that both the sender and receiver and all intermediate devices need tofollow to be able to communicate effectively.
- When communication is simple, we may need only one simple protocol.

  When communication is complex, we need to divide the task b/w different layers. We need a protocol at each layer, or protocol layering.

1.4.1 Scenarios

First Scenario

- In the first scenario, communication is so simple that it can occur in only one layer (Figure 2.1).
- 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

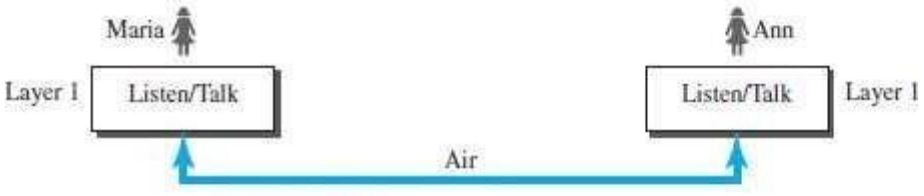


Figure 2.1 *A single-layer protocol*

Second Scenario

- Maria and Ann communicate using regular mail through the post office (Figure 2.2).
- However, they do not want their ideas to be revealed by other people if the letters are intercepted.
- They agree on an encryption/decryption technique.
- 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.

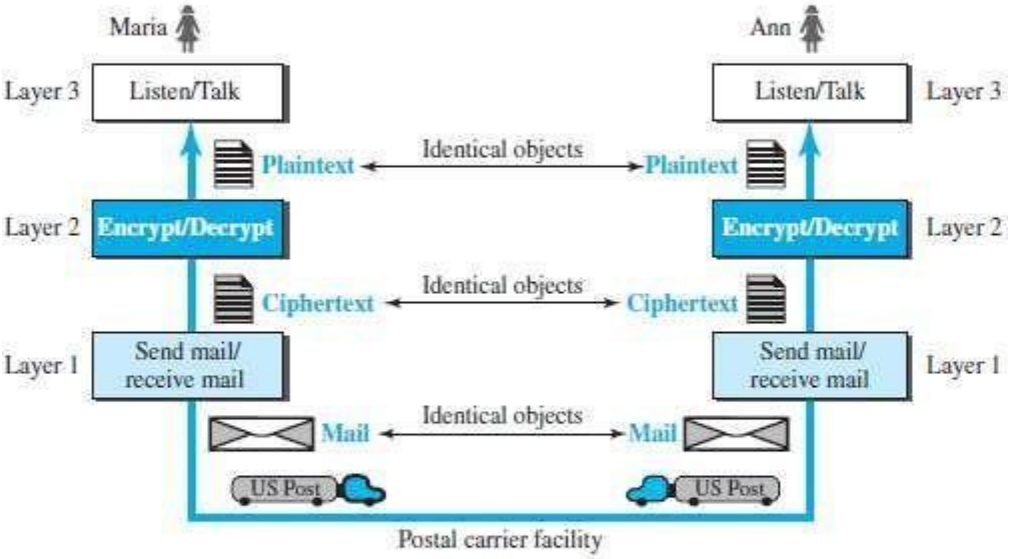


Figure 2.2 *A three-layer protocol*

1.4.1.1 Protocol Layering

- Protocol layering enables us to divide a complex task into several smaller and simpler tasks.
- Modularity means independent layers.
- A layer (module) can be defined as a black box with inputs and outputs, without concern about how inputs are changed to outputs.
- If two machines provide the same outputs when given the same inputs, they can replace each other.
- Advantages:

  1) It allows us to separate the services from the implementation.

  2) There are intermediate systems that need only some layers, but not all layers.
- Disadvantage:

  1) Having a single layer makes the job easier. There is no need for each layer to provide a service to the upper layer and give service to the lower layer.

1.4.2 Principles of Protocol Layering

1) First Principle

- If we want bidirectional communication, we need to make each layer able to perform 2 opposite tasks, one in each direction.
- For example, the third layer task is to listen (in one direction) and talk (in the other direction).

2) Second Principle

- The two objects under each layer at both sites should be identical.

- For example, the object under layer 3 at both sites should be a plaintext letter.

1.4.3 Logical Connections

- We have layer-to-layer communication (Figure 2.3).
- There is a logical connection at each layer through which 2 end systems can send the object createdfrom that layer.

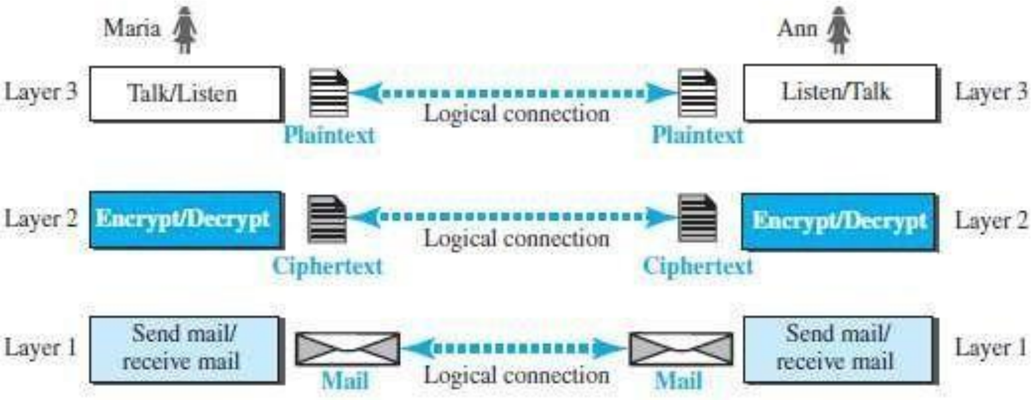
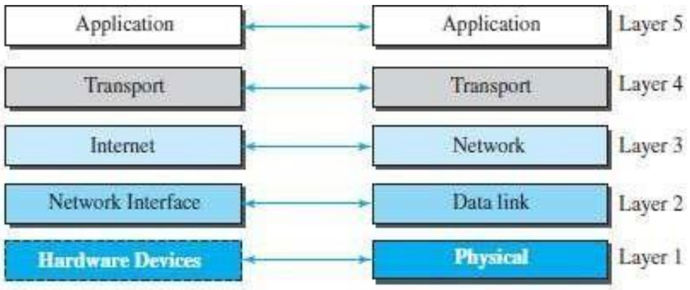


Figure 2.3 *Logical connection between peer layers*

1.5 TCP/IP PROTOCOL SUITE

- TCP/IP is a protocol-suite used in the Internet today.
- Protocol-suite refers a set of protocols organized in different layers.
- 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 byone or more lower level protocols.

1.5.1 Layered Architecture



a. Original layers

b. Layers used in this book

Figure 2.4 *Layers in the TCP/IP protocol suite*

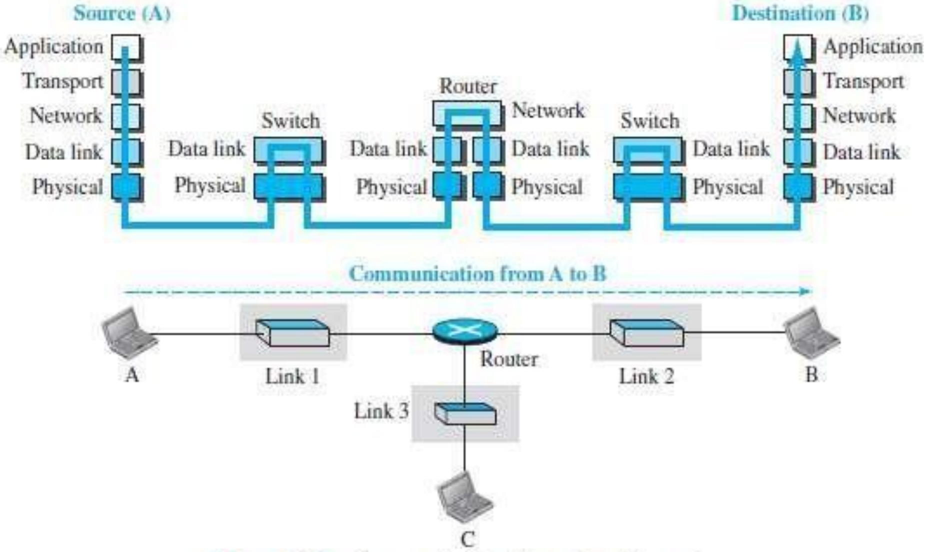


Figure 2.5 *Communication through an internet*

- Let us assume that computer A communicates with computer B (Figure 2.4).
- As the Figure 2.5 shows, we have five communicating devices:

  1) Source host(computer A) 2) Link-layer switch in link 1

  3) Router 4) Link-layer switch in link 2

  5) Destination host (computer B).

- Each device is involved with a set of layers depending on the role of the device in the internet.
- The two hosts are involved in all five layers.
- The source host

  → creates a message in the application layer and

  → sends the message down the layers so that it is physically sent to the destination host.

- The destination host

  → receives the message at the physical layer and

  → then deliver the message through the other layers to the application layer.

- The router is involved in only three layers; there is no transport or application layer.
- A router is involved in n combinations of link and physical layers.where n = 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 is involved only in two layers: i) data-link and ii) physical.

1.5.2 Layers in the TCP/IP Protocol Suite

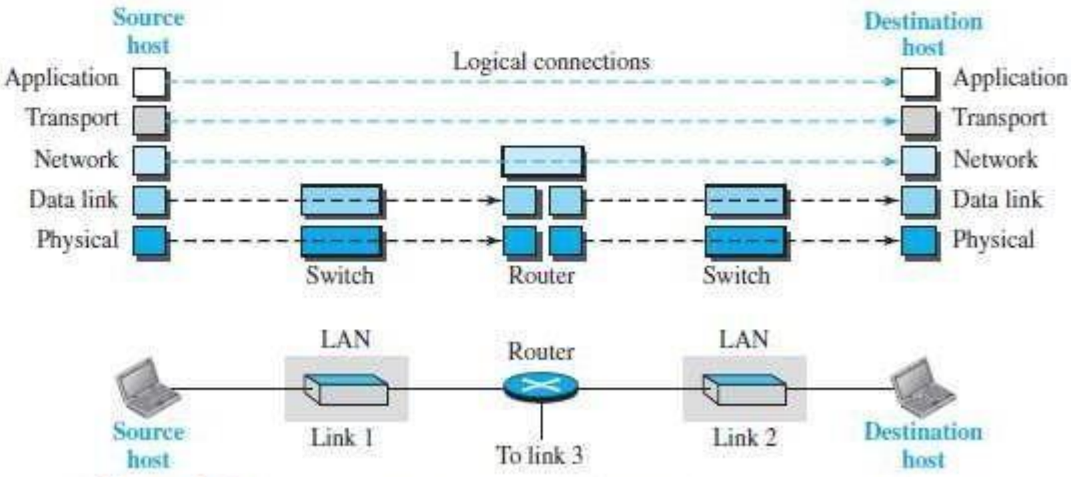


Figure 2.6 *Logical connections between layers of the TCP/IP protocol suite*

- As shown in the figure 2.6, 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. A hop is a host or router.
- The domain of duty of the top three layers is the internet. The domain of duty of the two lower layers is the link.
- In top 3 layers, the data unit should not be changed by any router or link-layer switch.

In bottom 2 layers, the data unit is changed only by the routers, not by the link-layer switches.

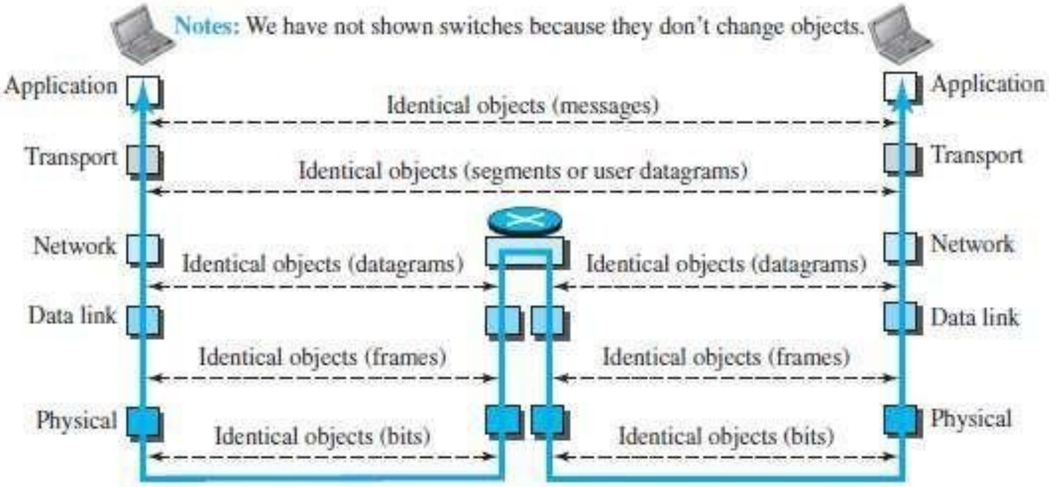

Notes: We have not shown switches because they don't change objects.
Application
Transport
Network
Data link
Physical
Application
Transport
Network
Data link
Physical
Identical objects (messages)
Identical objects (segments or user datagrams)
Identical objects (datagrams)
Identical objects (datagrams)
Identical objects (frames)
Identical objects (frames)
Identical objects (bits)
Identical objects (bits)

Figure 2.7 *Identical objects in the TCP/IP protocol suite*

- Identical objects exist between two hops. Because router may fragment the packet at the networklayer and send more packets than received (Figure 2.7).
- The link between two hops does not change the object.

1.5.3 Description of Each Layer

Physical Layer

- The physical layer is responsible for movements of individual bits from one node to another node.
- Transmission media is another hidden layer 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.
- The physical layer
  - → receives bits from the data-link layer &
  - → sends through the transmission media.

Data Link Layer

- Data-link-layer (DLL) is responsible for moving frames from one node to another node over a link.
- The link can be wired LAN/WAN or wireless LAN/WAN.
- The data-link layer
  - → gets the datagram from network layer
  - → encapsulates the datagram in a packet called a frame.
  - → sends the frame to physical layer.
- TCP/IP model does not define any specific protocol.
- DLL supports all the standard and proprietary protocols.
- Each protocol may provide a different service.
- Some protocols provide complete error detection and correction; some protocols provide only error correction.

Network Layer

- The network layer is responsible for source-to-destination transmission of data.
- The network layer is also responsible for routing the packet.
- The routers choose the best route for each packet.
- Why we need the separate network layer?
  1) The separation of different tasks between different layers.
  2) The routers do not need the application and transport layers.

- TCP/IP model defines 5 protocols:

1) IP (Internetworking Protocol)
2) ARP (Address Resolution Protocol)
3) ICMP (Internet Control Message Protocol)
4) IGMP (Internet Group Message Protocol)

1) IP

- ➢ IP is the main protocol of the network layer.
- ➢ IP defines the format and the structure of addresses.
- ➢ IP is also responsible for routing a packet from its source to its destination.
- ➢ It is a connection-less & unreliable protocol.
  - i) Connection-less means there is no connection setup b/w the sender and the receiver.
  - ii) Unreliable protocol means
    - → IP does not make any guarantee about delivery of the data.
    - → Packets may get dropped during transmission.
- ➢ It provides a best-effort delivery service.
- ➢ Best effort means IP does its best to get the packet to its destination, but with no guarantees.
- ➢ IP does not provide following services
  - → flow control
  - → error control
  - → congestion control services.
- ➢ If an application requires above services, the application should rely only on the transport-layer protocol.

2) ARP

- ➢ ARP is used to find the physical-address of the node when its Internet-address is known.
- ➢ Physical address is the 48-bit address that is imprinted on the NIC or LAN card.
- ➢ Internet address (IP address) is used to uniquely & universally identify a device in the internet.

3) ICMP

- ➢ ICMP is used to inform the sender about datagram-problems that occur during transit.

4) IGMP

- ➢ IGMP is used to send the same message to a group of recipients.

Transport Layer

- TL protocols are responsible for delivery of a message from a process to another process.
- The transport layer
  - → gets the message from the application layer
  - → encapsulates the message in a packet called a segment and
  - → sends the segment to network layer.
- TCP/IP model defines 3 protocols:1) TCP (Transmission Control Protocol)
  2) UDP (User Datagram Protocol) &
  3) SCTP (Stream Control Transmission Protocol)

1) TCP

- ➢ TCP is a reliable connection-oriented protocol.
- ➢ A connection is established b/w the sender and receiver before the data can be transmitted.
- ➢ TCP provides
  - → flow control
  - → error control and
  - → congestion control

2) UDP

- ➢ UDP is the simplest of the 3 transport protocols.
- ➢ It is an unreliable, connectionless protocol.
- ➢ It does not provide flow, error, or congestion control.
- ➢ Each datagram is transported separately & independently.
- ➢ It is suitable for application program that
  - → needs to send short messages &
  - → cannot afford the retransmission.

3) SCTP

- ➢ SCTP provides support for newer applications such as voice over the Internet.
- ➢ It combines the best features of UDP and TCP.

Application Layer

- The two application layers exchange messages between each other.
- Communication at the application layer is between two processes (two programs running at this layer).
- 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.

- TCP/IP model defines following protocols:
  1) SMTP is used to transport email between a source and destination.
  2) TELNET is used for accessing a site remotely.
  3) FTP is used for transferring files from one host to another.
  4) DNS is used to find the IP address of a computer.
  5) SNMP is used to manage the Internet at global and local levels.
  6) HTTP is used for accessing the World Wide Web (WWW).

(FTP □ File Transfer Protocol SMTP □ Simple Mail Transfer Protocol)
(DNS □ Domain Name System HTTP □ Hyper Text Transfer
Protocol)(SNMP □ Simple Network Management Protocol TELNET □ Terminal Network)

1.5.4 Encapsulation and Decapsulation

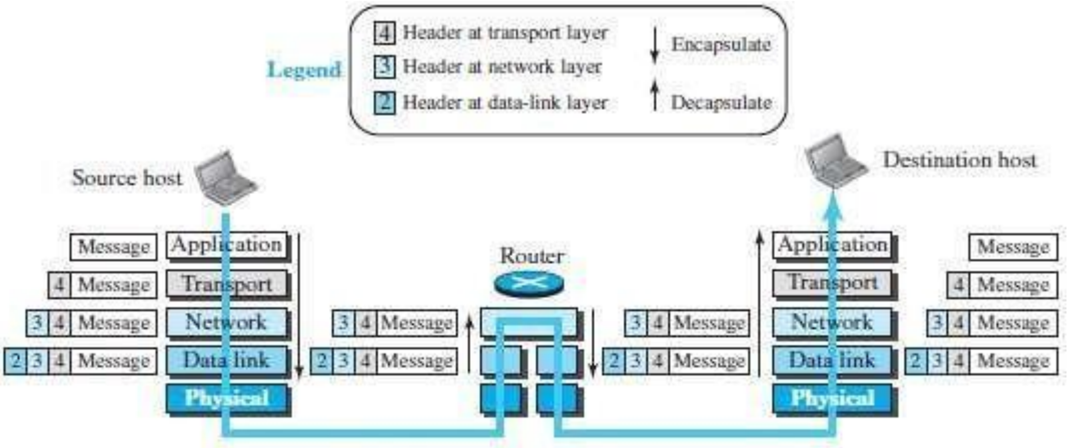


Figure 2.8 *Encapsulation/Decapsulation*

A) Encapsulation at the Source Host

- At the source, we have only encapsulation (Figure 2.8).

1) At the application layer, the data to be exchanged is referred to as a message.

- ➢ A message normally does not contain any header or trailer.
- ➢ The message is passed to the transport layer.

2) The transport layer takes the message as the payload.

- ➢ TL adds its own header to the payload.
- ➢ The header contains
  - → identifiers of the source and destination application programs
  - → information needed for flow, error control, or congestion control.
- ➢ The transport-layer packet is called the segment (in TCP) and the user datagram (in UDP).

- ➢ The segment is passed to the network layer.

3) The network layer takes the transport-layer packet as payload.

- ➢ NL adds its own header to the payload.
- ➢ The header contains
  - → addresses of the source and destination hosts
  - → some information used for error checking of the header &
  - → fragmentation information.
- ➢ The network-layer packet is called a datagram.
- ➢ The datagram is passed to the data-link layer.

4) The data-link layer takes the network-layer packet as payload.

- ➢ DLL adds its own header to the payload.
- ➢ The header contains the physical addresses of the host or the next hop (the router).
- ➢ The link-layer packet is called a frame.
- ➢ The frame is passed to the physical layer for transmission

B) Decapsulation and Encapsulation at the Router

- At the router, we have both encapsulation & encapsulation and because the router is connected totwo or more links.

1) Data-link layer

- → receives frame from physical layer
- → decapsulates the datagram from the frame and
- → passes the datagram to the network layer.

2) The network layer

- → inspects the source and destination addresses in the datagram header and
- → consults forwarding table to find next hop to which the datagram is to be delivered.

- ➢ The datagram is then passed to the data-link layer of the next link.

3) The data-link layer of the next link

- → encapsulates the datagram in a frame and
- → passes the frame to the physical layer for transmission.

C) Decapsulation at the Destination Host

- At the destination host, each layer
  - → decapsulates the packet received from lower layer
  - → removes the payload and
  - → delivers the payload to the next-higher layer

1.5.5 Addressing

- We have logical communication between pairs of layers.
- Any communication that involves 2 parties needs 2 addresses: source address and destination address.
- We need 4 pairs of addresses (Figure 2.9):

1) At the application layer, we normally use names to define
   - → site that provides services, such as vtunotesbysri.com, or
   - → e-mail address, such as vtunotesbysree@gmail.com.

2) At the transport layer, addresses are called port numbers.
   - ➢ Port numbers define the application-layer programs at the source and destination.
   - ➢ Port numbers are local addresses that distinguish between several programs running at thesame time.

3) At the network-layer, addresses are called IP addresses.
   - ➢ IP address uniquely defines the connection of a device to the Internet.
   - ➢ The IP addresses are global, with the whole Internet as the scope.

4) At the data link-layer, addresses are called MAC addresses
   - ➢ The MAC addresses defines a specific host or router in a network (LAN or WAN).
   - ➢ The MAC addresses are locally defined addresses.

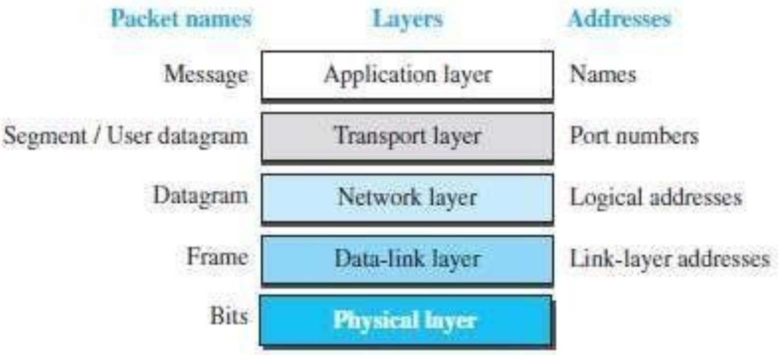


Figure 2.9 *Addressing in the TCP/IP protocol suite*

1.5.6 Multiplexing and Demultiplexing

- Multiplexing means a protocol at a layer can encapsulate a packet from several next-higher layer protocols (one at a time) (Figure 2.10).
- Demultiplexing means a protocol can decapsulate and deliver a packet to several next-higher layer protocols (one at a time).

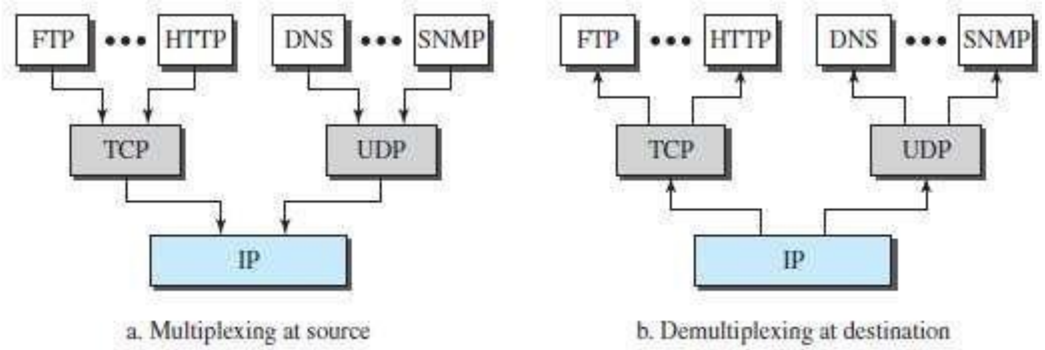
1) At transport layer, either UDP or TCP can accept a message from several application-layer protocols.

2) At network layer, IP can accept

→ a segment from TCP or a user datagram from UDP.

→ a packet from ICMP or IGMP.

3) At data-link layer, a frame may carry the payload coming from IP or ARP.



a. Multiplexing at source

b. Demultiplexing at destination

Figure 2.10 *Multiplexing and demultiplexing*

1.6 OSI MODEL

- OSI model was developed by ISO.
- ISO is the organization, OSI is the model.
- Purpose: OSI was developed to allow systems with diff. platforms to communicate with each other.
- Platform means hardware, software or operating system.
- OSI is a network-model that defines the protocols for network communications.
- OSI has 7 layers as follows (Figure 2.11):

1) Application Layer
2) Presentation Layer
3) Session Layer
4) Transport Layer
5) Network Layer
6) Data Link Layer
7) Physical Layer

- Each layer has specific duties to perform and has to co-operate with the layers above & below it.

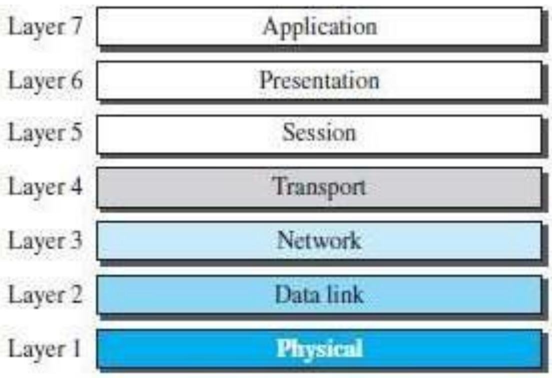


Figure 2.11 *The OSI model*

1.6.1 OSI vs. TCP/IP

1) The four bottommost layers in the OSI model & the TCP/IP model are same (Figure 2.12).

However, the Application-layer of TCP/IP model corresponds to the Session, Presentation& Application Layer of OSI model.

Two reasons for this are:

1) TCP/IP has more than one transport-layer protocol.

2) Many applications can be developed at Application layer

2) The OSI model specifies which functions belong to each of its layers.

In TCP/IP model, the layers contain relatively independent protocols that can be mixedand matched depending on the needs of the system.

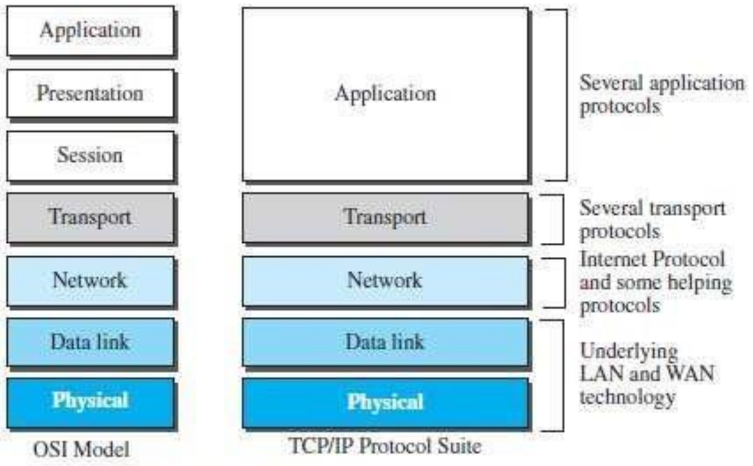


Figure 2.12 *TCP/IP and OSI model*

1.6.2 Lack of OSI Model's Success

- OSI was completed when TCP/IP was fully in place and a lot of time and money had been spent onthe suite; changing it would cost a lot.
- Some layers in the OSI model were never fully defined.
- When OSI was implemented by an organization in a different application, it did not show a high enough level of performance

CHAPTER3: TRANSMISSION MEDIA

1.1 Introduction

In a data transmission system, the **transmission medium** is the physical path between transmitter and receiver.

Transmission media carries the information from sender to receiver. We use different types of cables or waves to transmit data. Data is transmitted normally through electrical or electromagnetic signals.

An electrical signal is in the form of current. An electromagnetic signal is series of electromagnetic energy pulses at various frequencies. These signals can be transmitted through copper wires, optical fibers, atmosphere, water and vacuum. Transmission media is also called **Communication channel.**

Criteria for selection of Transmission Media.

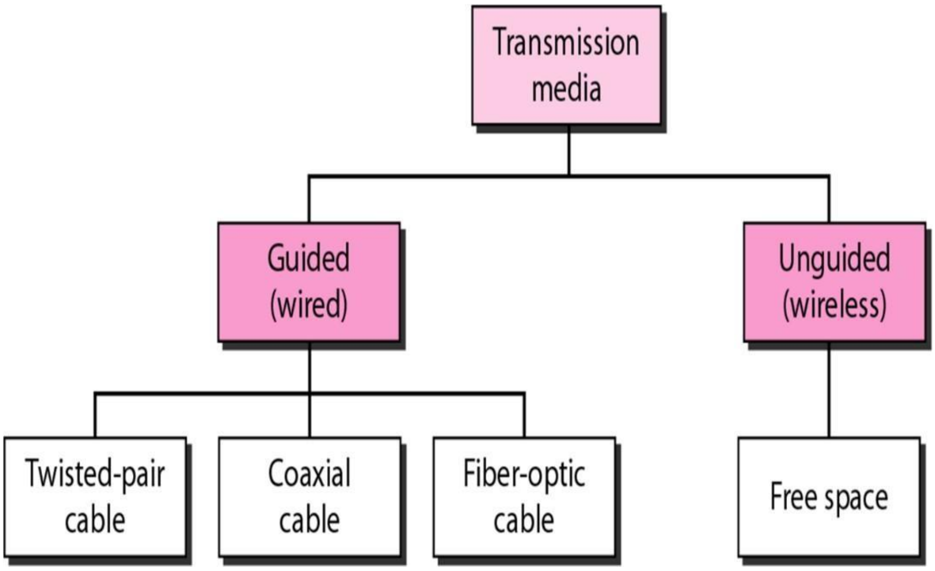
Different Medias have different properties like **bandwidth, delay, cost and ease of installation and maintenance**. The data transmission capabilities of various Media vary depending upon the various factors. These factors are:

1. **Type of Media (Wired or Wireless).**
2. **Flexibility.** In order to expand network.
3. **Bandwidth**. It refers to the data carrying capacity of a channel or medium. Higher bandwidth communication channels support higher data rates.
4. **Reliability**. The consistency of transmission media (effect of weather conditions).
5. **Radiation**. It refers to the leakage of signal from the medium due to undesirable electrical characteristics of the medium.
6. **Noise Absorption**. It refers to the susceptibility of the media to external electricalnoise that can cause distortion of data signal.
7. **Attenuation**. It refers to loss of energy as signal propagates outwards. The amountof energy lost depends on frequency.
8. **Number of receivers**. The number of users to be connected.
9. **Transmission Rate**.
10. **Cost and Ease of Installation**.
11. **Distances**, etc.

1.2 Types of Transmission Medias

There are two categories of transmission media used in computer communications.

1. **Guided Media (Wired)**
2. **Unguided Media (Wireless Media)**



1. **Guided Media (Wired)**

In a Guided transmission media the signals are sent through to a specific (solid) pathusing wire or cable. Guided media are made up of **copper conductor** bounded by **jacket (insulation)** material. Guided media is used high speed, good security and low cast requirements. Guided media is used in point to point communication.

Guided media are further divided in three Types.

1. **Twisted Pairs Cable**
2. **Coaxial Cable**
3. **Fiber Optics Cable**

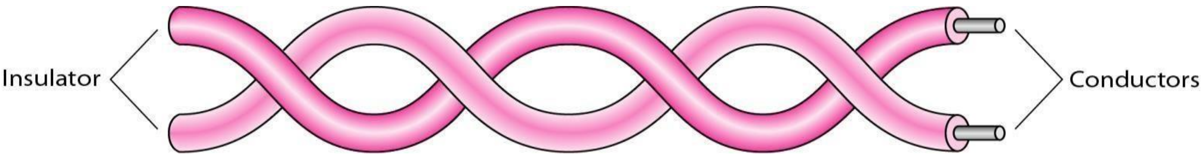
1. Twisted Pair cable

- The **least expensive** and **most widely used guided transmission medium.**
- It **is lightweight, cheap, can be installed easily**, and they support many different types of network.
- A twisted pair consists of **two insulated copper wires** arranged in a regular **spiral pattern**.
- Typically, a number of these pairs are bundled together into a cable by wrappingthem in a tough protective sheath.

- Over longer distances, cables may contain hundreds of pairs.
- Twisted pair (TP) maybe used to **transmit both analog and digital signal**.
- For analog signals amplifiers are required about every 5 to 6 kms. For digital signals repeaters are required every 2 to 3kms.

Why twist a cable?

- The twisting tends to **decrease the crosstalk (EMI) interference** between adjacent pairs in a cable.
- Neighboring pairs in a bundle typically have somewhat different twist lengths to reduce the crosstalk interference.
- On long-distance links, the twist length typically varies from 5 to 15



Application:-

1. It is the most commonly used medium of telephone n/w.
2. In the telephone system individual residential telephone sets are connected to thelocal telephone exchange or to end office by twisted pair wire.
3. Twisted pair also the most common medium used for the digital signaling for connections to a digital data switch.
4. It is also commonly used within a building for LAN.

There are two types of twisted pair:-

- **A. Unshielded twisted pair (UTP).**
- **B. Shielded twisted pair (STP).**

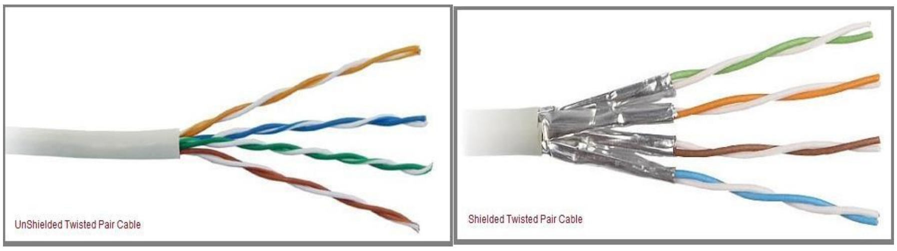


Fig. UTP and STP cables

A. Unshielded Twisted Pair (UTP):-

- Usually consists of two copper wires wrapped in individual plastic insulation.
- UTP cables are the most common telecommunications medium.
- The frequency range of the twisted pair cables enable both voice and data transmission.
- UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ-11** connector and 4 pair cable use**RJ-45** connector.

(a)

There are five categories of UTPs:

- **Category 1:-** These originally used only for voice communication and can supportonly low data rates.
- **Category 2:-** Suitable for Voice and Data gives speed upto 4 mbps. This can't be used for high speed data communication. Older n/w's use this category.
- **Category 3:-** It is suitable for most PC n/w's support data rate of up to 16mbps currently most telephone n/w uses this.
- **Category 4:-** It offers data rate up to 20mbps.
- **Category 5:-**It offers data rate of 100mbps. Can be used for fast **Ethernet**. It requires more insulation and more twist per foot. It requires compatible equipment's.

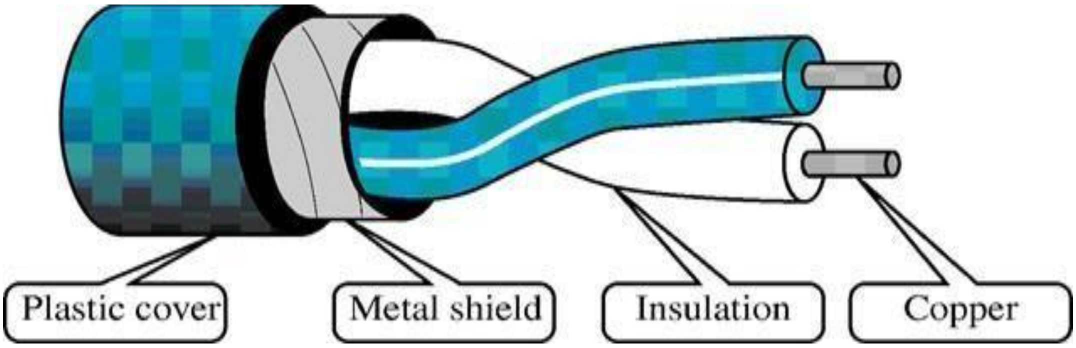
Advantages:

□ Installation is easy
□ Flexible
□ Cheap
□ It has high speed capacity,
□ 100-meter limit
□ Higher grades of UTP are used in LAN technologies like Ethernet.

Disadvantages:

□ Bandwidth is low when compared with Coaxial Cable
□ Provides less protection from interference (EMI).

2. Shielded twisted pair (STP).



- The only difference between STP and UTP is that STP cables have a shielding in usually of aluminum or polyester material between the outer jacket and wire.
- The shield makes STP less vulnerable to EMI, because the shield is electrically grounded.
- The metal mesh around the insulated wires eliminates **crosstalk**.
- **Crosstalk** occurs when one line picks up some of the other signals traveling down another line.

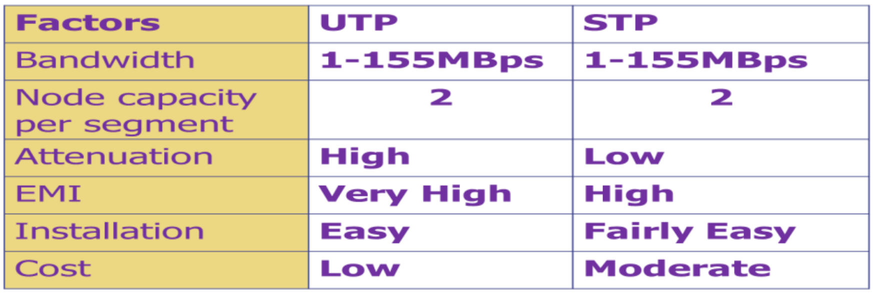
Advantages:

□ Easy to install
□ Performance is adequate
□ Can be used for Analog or Digital transmission
□ Increases the signaling rate
□ Higher capacity than unshielded twisted pair
□ Eliminates crosstalk

Disadvantages:

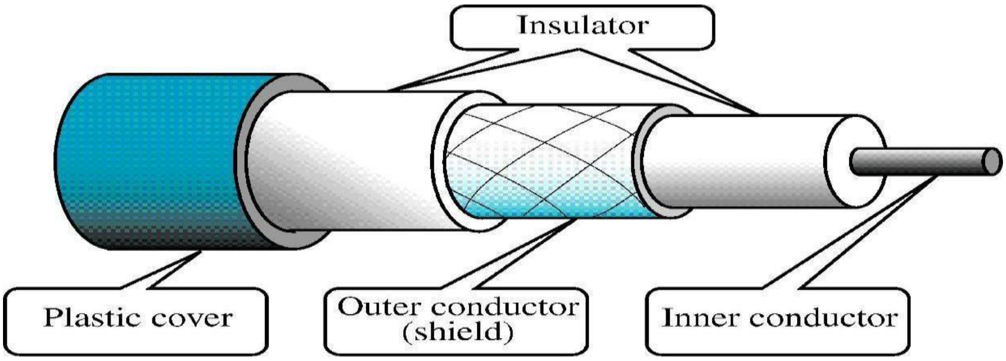
□ Difficult to manufacture
□ Heavy
□ Expensive than UTP

Difference UTP vs STP



Factors	UTP	STP
Bandwidth	1-155MBps	1-155MBps
Node capacity per segment	2	2
Attenuation	High	Low
EMI	Very High	High
Installation	Easy	Fairly Easy
Cost	Low	Moderate

2. Co-axial cable



- The name coaxial is because it contains two conductors that are parallel to eachother and share common axis.
- Inner conductor is made of copper which is surrounded by PVC insulation.
- The outer conductor is metal foil, mesh or both.
- Outer metallic conductor is used as a shield against noise.
- The outer conductor is also encased in an insulating sheath.
- The outermost part is the plastic cover which protects the whole cable.
- Co-axial cable is much less susceptible to interference and cross talk than the twisted pair.
- Co-axial cable is used to transmit both analog and digital signal.

Application –

Co-axial cable is widely used in the wide variety of applications. The most important of these are: -

1. TV distribution: -

Co-axial cable is spreading rapidly as a means of distributing TV signals to individual homes –cables TV. A cable TV system can carry dozens or even hundreds of TV channels at ranges up to a few tens of miles.

2. Long distance telephone transmission:-

Co-axial cable has traditionally been as important part of the long distance telephone n/w using FDM (frequency division multiplication) a co-axial cable can carry over 10,000 voice channels simultaneously.

3. Short distance communication links: -

Co-axial cable is also commonly used for short range connection between devices.

E.g. can be used to provide high speed I/O channels for an PC system.

4. LAN: -

Co-axial cable can be support a large number of devices with a variety of data and traffic types over distance that covers single building or a complex of building

.

Co-axial cables usually for data transmission are of two types.

- 10 base 2 thin net - Node capacity per segment for 10 base 2 is 30.
- 10 base 2 thick net- Node capacity for 10 base 5 is 100.

There are two types of Coaxial cables:

BaseBand

This is a 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LAN's. Baseband transmits a single signal at a time with very high speed. Themajor drawback is that it needs amplification after every 1000 feet.

BroadBand

This uses analog transmission on standard cable television cabling. It transmits several simultaneous signal using different frequencies. It covers large area when compared with Baseband Coaxial Cable.

Advantages:

□ Bandwidth is high

□ Used in long distance telephone lines.

□ Transmits digital signals at a very high rate of 10Mbps.

□ Much higher noise immunity

□ Data transmission without distortion.

□ The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable

Disadvantages :

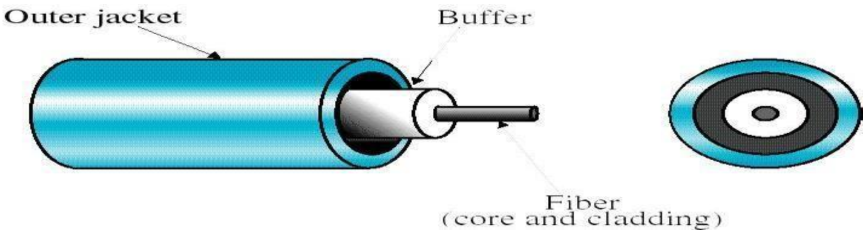
□ Single cable failure can fail the entire network.

□ Difficult to install and expensive when compared with twisted pair.

□ If the shield is imperfect, it can lead to grounded loop.

3. Optical Fiber or fiber optics

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- A light pulse can be used to signal a one (1) bit.
- The absence of a pulse signals a zero(0).
- The bandwidth of an optical transmission system is potentially enormous.



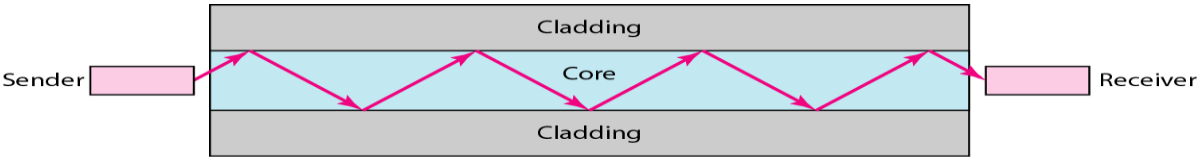
An optical fiber has an cylindrical shape and consists of 3 concentric section –

(i) Core
(ii) Cladding
(iii) Jacket

1. **Core:-** It's the inner most section is made of glass or plastic and is surrounded by its own cladding. The core diameter is in the range of **8 to 50 µm**.
2. **Cladding: -** A glass or plastic coating that has optical properties different from those of the core having a diameter **of 125 µm**. The cladding acts as **a reflectorto light** that would otherwise escape the core.
3. **Jacket: -** The outer most layers surrounding caddied fiber is the jacket. Jacket is composed of plastic or other material layer to protect against moisture, cut, crushing and other environmental dangers.

Optical Fiber Communication

- A transmitter (Light Source) at senders end sends a Light across the fiber.
- A receiver at the other end makes use of Light Sensitive transistor to detect the absence or presence of light to indicate 0 or 1.



- The transmission medium is an ultra-thin fiber of glass.
- Light enters the cylindrical glass or plastic core at small angles are reflected and propagates along the fiber.
- The detector generates an electrical pulse when light falls on it.

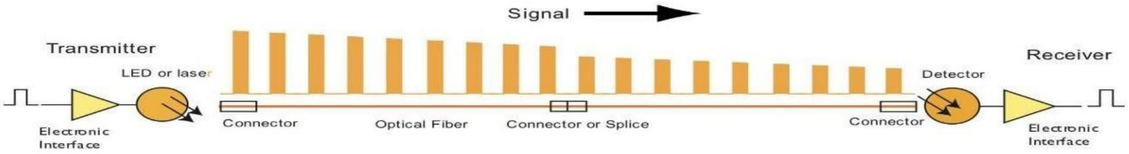


Fig. OFC Communication

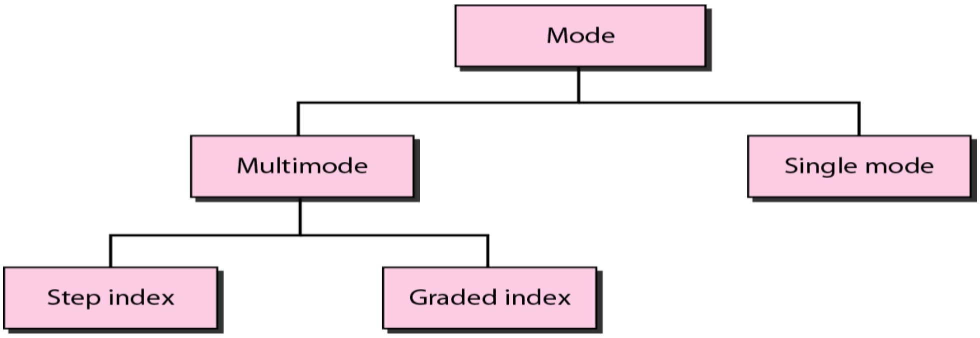
Two different types of **light sources** are used in fiber optic system.

- The Light Emitting Diode (LED)
- Injection Laser Diode (ILD)

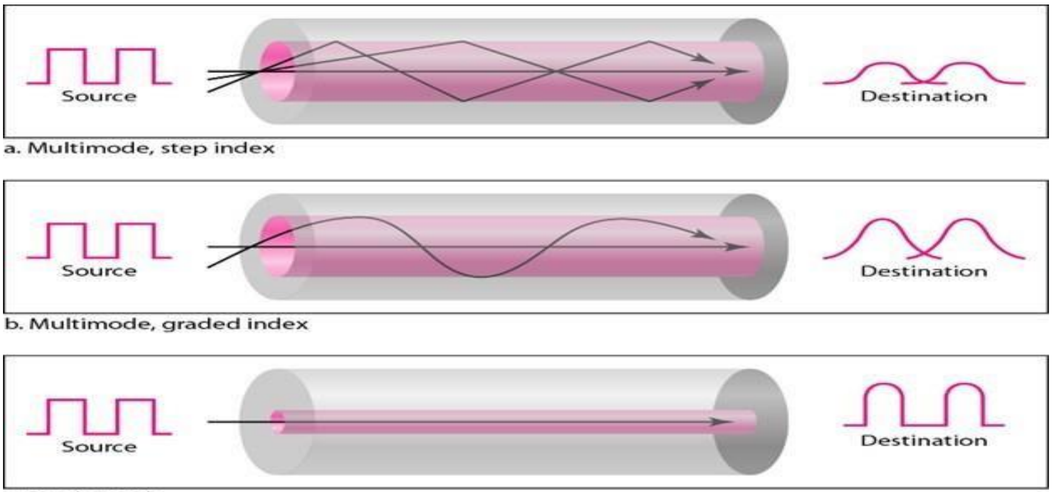
Both are semiconductor devices that emit a beam of light when voltage is applied. Led is less costly than ILD. ILD operates on laser principle, is more efficient, and can sustain greater data rate.

Types of Fiber Propagation Modes

- Optical fiber may be multi-mode or single mode.
- Single mode fibers allow a single light pass and are used with laser signaling. Single mode fibers can allow greater bandwidth and cable runs than multimode, but it is more expensive.
- Multimode fibers use multiple light pass the physical characteristics of the multiple mode fiber make all parts of the signal arrive at the same time appearingto the receiver as though they were one pulse.



1. Multimode **step-index fiber**
   - the reflective walls of the fiber move the light pulses to the receiver
2. Multimode **graded-index fiber**
   - acts to refract the light toward the center of the fiber by variations in the density
3. **Single mode fiber**
   - the light is guided down the center of an extremely narrow core



a. Multimode, step index

b. Multimode, graded index

c. Single mode

Advantages :

- Provides high quality transmission of signals at very high speed (bandwidth 2 Gbps)
- These are not affected by electromagnetic interference, so noise and distortion isvery less.
- **Highly secure** due to tap difficulty and lack of signal radiation.
- Used for both analog and digital signals.
- **Smaller size** and **light weight**
- **Lower attenuation**

Disadvantages :

- It is expensive
- Difficult to install. requires **highly skilled installers**
- Maintenance is expensive and difficult.
- Do not allow complete routing of light signals.

Applications

◈ Telephones, including cellular wireless ◈
Internet
◈ LANs - local area networks
◈ CATV - for video, voice and Internet connections ◈
Utilities - management of power grid
◈ Security - closed-circuit TV and intrusion sensors ◈
Transportation – smart lights and highways
◈ Military – everywhere!

Characteristics of cable media:-

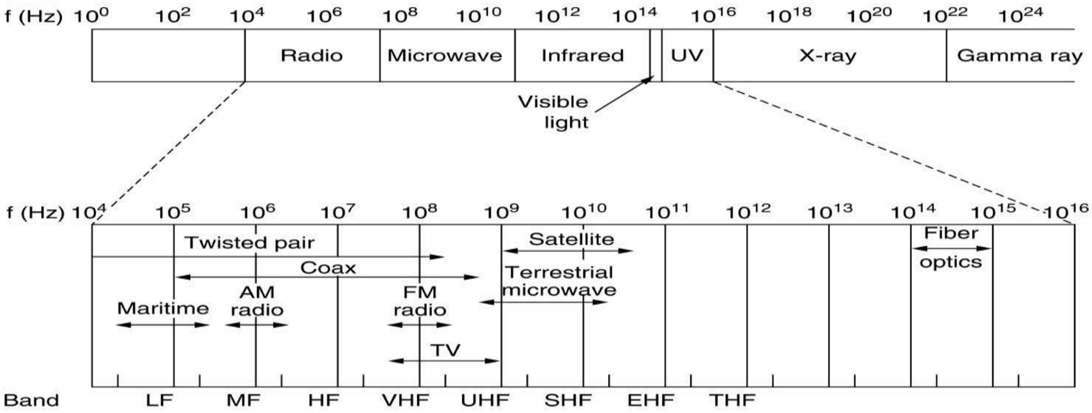
Factor	**UTP**	**STP**	**Co-axial**	**Fiber optics**
Cost	Low	Moderate	Moderate	Highest
Installation	Easy	Fairly easy	Fairly easy	Difficult
Data rate	1 to 155 mbps	1to 155 mbps	500 mbps	2 GBPS
Node capacity	2	2	30-100	2
Attenuation	High(100's of meter)	High(100's of meter)	Lower (range offew km's)	Lowest (10 Km's)
EMI	Most vulnerable	Less vulnerable than UTP	Less vulnerable than UTP	Not effected by EMI
Bandwidth	Low	Moderate	Moderatly high	Very high
Signals	Electrical	Electrical	Electrical	Light

2. Unguided Media

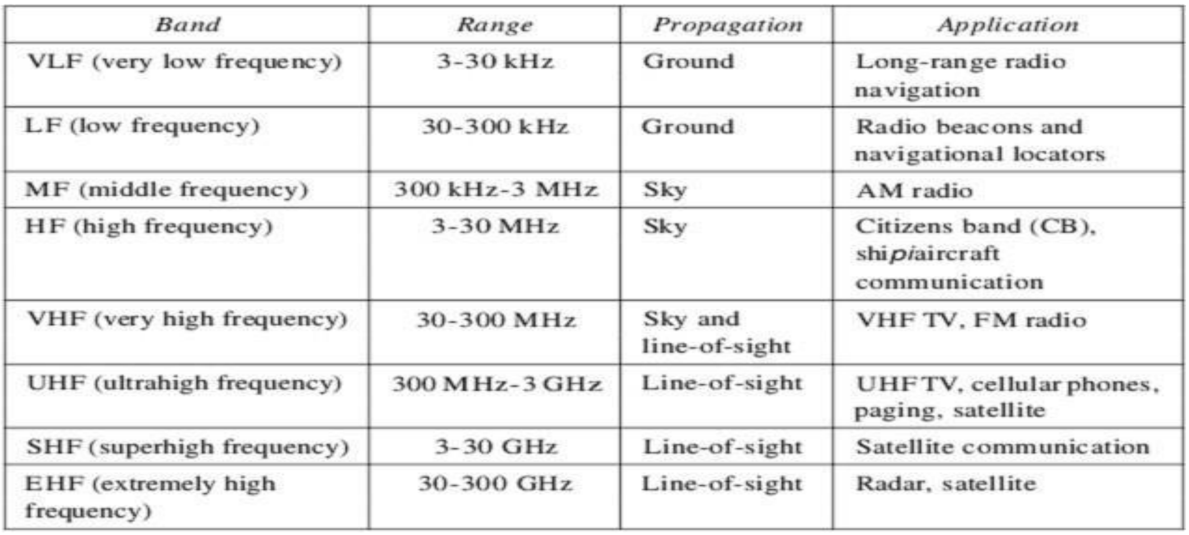
- Unguided media transmit electromagnetic waves without using a physical conductor.
- This is also called as wireless communication.
- Signals are normally broadcast through free space and thus are available toanyone who has **a device capable of receiving them.**

Electromagnetic Spectrum (Communication Band)

Electromagnetic spectrum is used for wireless communication. It is divided into various sub-bands.


f (Hz) 10⁰ 10² 10⁴ 10⁶ 10⁸ 10¹⁰ 10¹² 10¹⁴ 10¹⁶ 10¹⁸ 10²⁰ 10²² 10²⁴
Radio
Microwave
Infrared
UV
X-ray
Gamma ray
Visible light
f (Hz) 10⁴ 10⁵ 10⁶ 10⁷ 10⁸ 10⁹ 10¹⁰ 10¹¹ 10¹² 10¹³ 10¹⁴ 10¹⁵ 10¹⁶
Twisted pair
Coax
Satellite
Terrestrial microwave
Fiber optics
Maritime
AM radio
FM radio
TV
Band LF MF HF VHF UHF SHF EHF THF

The following table shows segmentation of electromagnetic spectrum.



Band	*Range*	*Propagation*	*Application*
VLF (very low frequency)	3-30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30-300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz-3 MHz	Sky	AM radio
HF (high frequency)	3-30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF (very high frequency)	30-300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF (ultrahigh frequency)	300 MHz-3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF (superhigh frequency)	3-30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30-300 GHz	Line-of-sight	Radar, satellite

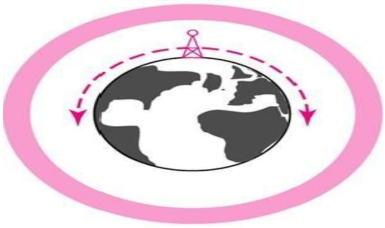
Propagation Methods

Unguided signals can travel from the source to destination in several ways:

- Ground propagation,
- Sky-Propagation, and
- Line-of-Sight Propagation

1. **Ground propagation mode:**

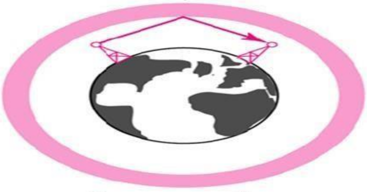
- Radio waves **travel close to the earth**.
- These **low-frequency signals** proceed in all directions from the transmitting antenna and follow the **curvature of the planet**.
- **Distance** depends on the amount of **power in the signal**: The greater the power,the greater the distance.



Ground propagation
(below 2 MHz)

2. **Sky propagation mode:**

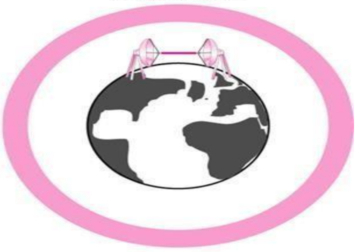
- In this **high-frequency radio waves** radiate upward into the ionosphere where **they are reflected back** to earth.
- Ionosphere is the layer of atmosphere where **particles exist as ions**.
- This type of transmission allows for **greater distances with lower outputpower**.



Sky propagation
(2–30 MHz)

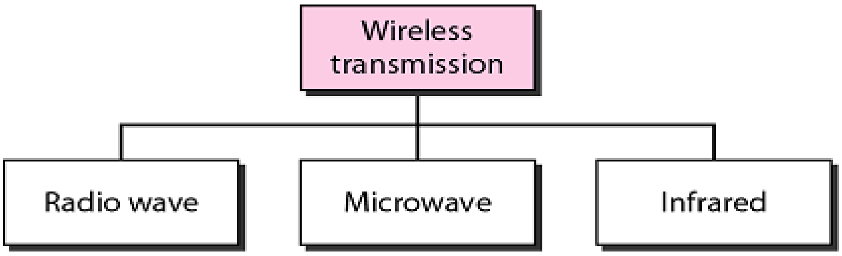
3. **Line-of-sight propagation mode:**

- In this, **very high-frequency** signals are transmitted **in straight lines** directlyfrom **antenna to antenna**.
- Antennas must be **directional**, facing each other and tall enough.
- Line-of-sight propagation **is tricky** because radio transmissions cannot be completely focused.



Line-of-sight propagation
(above 30 MHz)

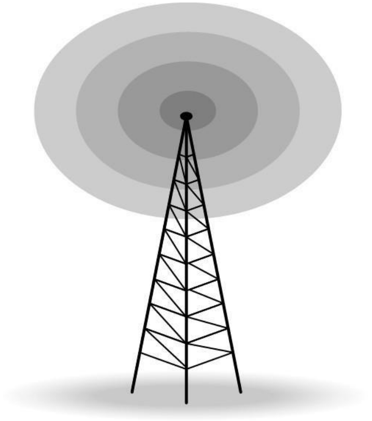
Classification of Wireless Media



- Wireless communication may be via:
  - **Radio frequency** communication
  - **Microwave** communication
  - **Infrared** short range communication

1. Radio Wave Transmission

- Electromagnetic waves ranging in frequency between **3 kHz and 1 GHz** arenormally called radio waves.
- Radio waves, are **omnidirectional**, i.e. they are **propagated in all directions**.
- A sending antenna sends waves that can be received by **any receiving antenna**.



- Radio waves, particularly of **low and medium frequencies**, **can penetrate walls**.
- It is an **advantage** because, an **AM radio** can receive signals **inside a building**.
- It is a **disadvantage** because we **cannot isolate** a communication to just **insideor outside a building**.

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**,
- **Maritime radio**,
- **Cordless phones** and **paging**.

2. Microwave Transmission

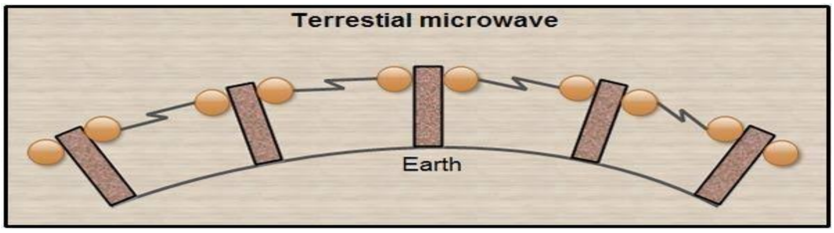
- Electromagnetic waves having frequencies between **1GHz and 300 GHz** are called microwaves.

- 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.
- **Microwaves use line-of-sight transmission**.
- This means that microwaves must be transmitted in straight line and no obstructions, such as buildings or mountains, between microwave stations.
- To avoid possible obstructions, microwave antennas often are positioned on the **tops of buildings**, **towers**, or **mountains.**

Microwave transmission is divided into two types

A. Terrestrial Microwave

- Used for **long-distance telephone service.**
- Uses radio frequency spectrum, from **2 to 40 GHz**.
- Parabolic dish transmitter, mounted high.
- Requires **unobstructed line of sight** between source and receiver
- Curvature of the earth requires stations (**repeaters**) 30 miles apart



Advantages:

- Effect of noise is reduced because of repeaters.
- Maintenance is less as compared to cable.
- No interference with other transmission channels.

Disadvantages:

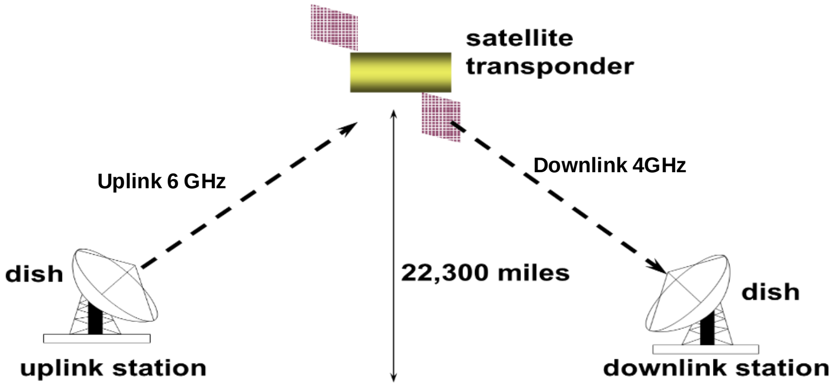
- Communication can be affected because of atmospheric phenomenon and passing airplanes and rain
- Line of sight requirement
- Expensive towers and repeaters.

Application:-

- Long-distance telecommunication service
  - requires fewer amplifiers or repeaters than coaxial cable
  - Example
    - telephone system
    - TV distribution
- Short point-to-point links
  - Data link between local area network
  - Closed-Circuit TV
- **By passing n/w:-** Microwave can also be used for bypass application. A business can establish a microwave link to long a distance telecommunication facility in the same city, by passing the local telephone company.

B. Satellite microwave:-

- A communication satellite acts like a microwave station.
- It is used to link two or more ground waves microwave transmitter or receiver known as earth stations.
- The satellite receives transmission on one frequency band (uplink), amplifies or repeats the signal and transmit it on another frequency (down link).
- A single orbiting satellite will operate on no. of frequency bands calledtransponder channels or simply transponder.



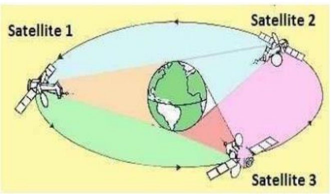
- In the fig the satellite is being used to provide a point to point link between two distant grounds based antenna.
- The signal, a beam of **modulated microwaves** is sent towards the satellite called **UPLINK (6 Ghz).**
- Then the satellite processes the signal and send it back to the receiver's antenna present on the earth's surface called as **DOWNLINK (4Ghz).**
- The satellite has to **receive, process** and **transmit** the signal.
- A unit called as Satellite Transponder performs all these functions.
- The communication satellite has two sets of transponders.
- Each set having **12 transponders**.
- Each transponder has a bandwidth of 36MHz.

Types of Satellite by there purpose

- Communication Satellite
- Weather satellite
- Remote- Sensing Satellite
- Scientific Satellite

Geostationary Earth Orbit (GEO)

- These satellites are in orbit 35,863 km above the earth's surface along the equator.
- Objects in Geostationary orbit revolve around the earth at the same speed as theearth rotates.
- This means GEO satellites remain in the same position relative to the surface of earth.



- **Principal Satellite Transmission Bands**
- **C band:**
  - 4(downlink) - 6(uplink) GHz
  - the first to be designated
- **Ku band:**
  - 12(downlink) -14(uplink) GHz
  - rain interference is the major problem
- **Ka band:**
  - 19(downlink) - 29(uplink) GHz
  - equipment needed to use the band is still very expensive

Application:-

- **Television** distribution
  - A network provides programming from a central location
  - Direct broadcast satellite (DBS)
  - Long-distance **telephone** transmission
    - High-usage international trunks
- Private business networks
- **Military** Applications
- Other applications
  - **digital** cinema
  - Satellite **radio**
  - Satellite **internet access**

3. Infrared

- Infrared waves, with frequencies from **300 GHz to 400 THz** (wavelengths from **1 mm to 770 nm**),
- Used for **short-range communication**.
- Infrared communication is achieved using transmitters/receivers (Transceivers) that modulate non-coherent infrared light.
- Transceiver must be in line of sight of each other either directly or via reflectionfrom light colored surface such as the sealing of the room.
- One important difference between infrared and microwave transmission is thatthey don't penetrate walls.
- The **remote controls** used for televisions, VCRs, and stereos all use infrared communication.
- They are relatively directional, cheap, and easy to build.

Applications

- TV Remote control
- Guidance in weapon system
- Wireless keyboards and mouse.

PACKET SWITCHING

1.1 PACKET SWITCHED NETWORK

- The message is divided into packets of fixed or variable size.
- The packet-size is determined by
  - → network and
  - → governing protocol.
- There is no resource reservation; resources are allocated on-demand.

1.1.1 Datagram Networks

- This is analogous to postal system.
- Each packet is routed independently through the network.
- Each packet has a header that contains source and destination addresses.
- Each switch examines the header to determine the next hop in the path to the destination.
- If the transmission line is busy
  then the packet is placed in the queue until the line becomes free.
- Packets are referred to as datagrams.
- Datagram switching is normally done at the network layer.
- In Internet, switching is done by using the datagram switching.
- Advantage:
  1) High utilization of transmission-line can be achieved by sharing among multiple packets.
- Disadvantages:
  1) Packets may arrive out-of-order, and re-sequencing may be required at the destination
  2) Loss of packets may occur when a switch has insufficient buffer

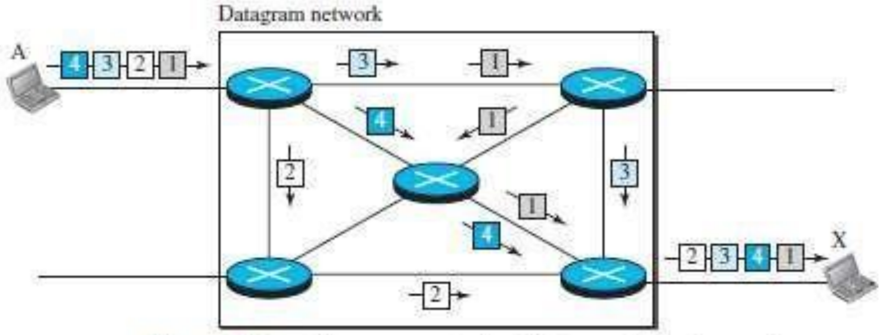


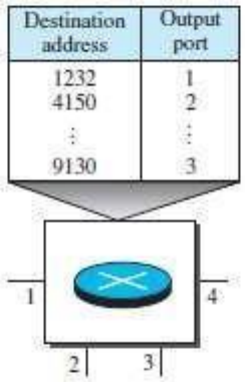
Figure 8.7 *A datagram network with four switches (routers)*

- ➢ The Figure 8.7 shows how the 4 packets are transferred from station-A to station-X.
- ➢ The switches are referred to as routers.
- ➢ All four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination.
- ➢ This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X.
- ➢ This approach can cause the datagrams of a transmission to arrive at their destination out-of- order with different delays between the packets.
- ➢ Packets may also be lost or dropped because of a lack-of-resources.

- ➢ It is the responsibility of an upper-layer protocol to
  - → reorder the datagrams or
  - → ask for lost datagrams.
- ➢ The datagram-networks are referred to as connectionless networks. This is because
  1) The switch does not keep information about the connection state.
  2) There are no setup or teardown phases.
  3) Each packet is treated the same by a switch regardless of its source or destination.

1.1.1.1 Routing Table

- Each switch has a routing-table which is based on the destination-address.
- The routing-tables are dynamic & updated periodically.
- The destination-addresses and the corresponding forwarding output-ports are recorded in the tables.



Destination address	Output port
1232	1
4150	2
⋮	⋮
9130	3

Figure 8.8 *Routing table in a datagram network*

1.1.1.1.1 Destination Address

Every packet carries a header that contains the destination-address of the packet.

When the switch receives the packet,

→ This destination-address is examined.

→ The routing-table is consulted to find the corresponding port through which the packet should be forwarded.

The destination address in the header of a packet in remains the same during the entire journey of the packet.

1.1.1.1.2 Efficiency

Datagram-networks are more efficient when compared to circuit-switched-network. This is becauseResources are allocated only when there are packets to be transferred.If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be re-allocated during these minutes for other packets from other sources.

1.1.1.1.3 Delay

Datagram-networks may have greater delay when compared to circuit-switched-network. This is because Each packet may experience a wait at a switch before it is forwarded. Since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message.

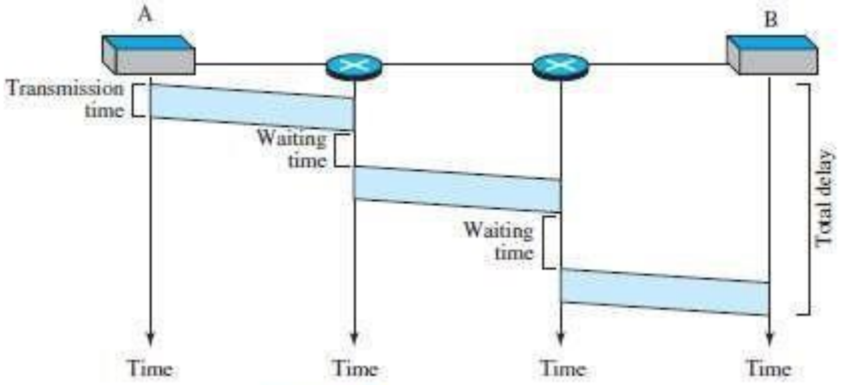


Figure 8.9 *Delay in a datagram network*

The Figure 8.9 gives an example of delay for one single packet.

The packet travels through two switches.

There are three transmission times (3T), three propagation delays (slopes 3t of the lines), and two waiting times (W1+ W2).

Total delay = $3T + 3\tau + w_1 + w_2$

1.1.2 Virtual Circuit Network (VCN)

- This is similar to telephone system.
- A virtual-circuit network is a combination of circuit-switched-network and datagram-network.
- Five characteristics of VCN:

1) As in a circuit-switched-network, there are setup & teardown phases in addition to the data transfer phase.

2) As in a circuit-switched-network, resources can be allocated during the setup phase. As in a datagram-network, resources can also be allocated on-demand.

3) As in a datagram-network, data is divided into packets.
Each packet carries an address in the header.
However, the address in the header has local jurisdiction, not end-to-end jurisdiction.

4) As in a circuit-switched-network, all packets follow the same path established during the connection.

5) A virtual-circuit network is implemented in the data link layer.
A circuit-switched-network is implemented in the physical layer. A datagram-network is implemented in the network layer.

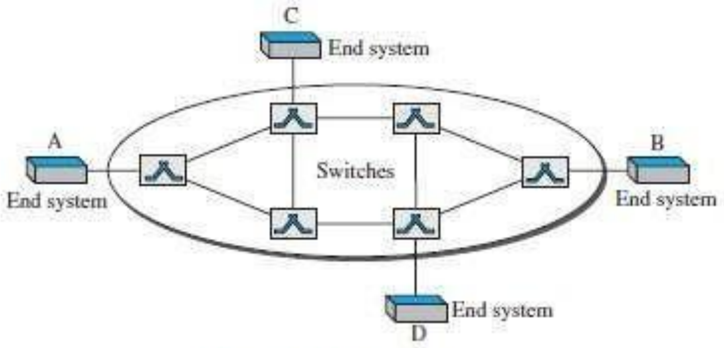


Figure 8.10 *Virtual-circuit network*

- The Figure 8.10 is an example of a virtual-circuit network.
- The network has switches that allow traffic from sources to destinations.
- A source or destination can be a computer, packet switch, bridge, or any other device that connects other networks.

1.1.2.1 Addressing

- Two types of addressing: 1) Global and 2) Local (virtual-circuit identifier).

1) Global Addressing

- A source or a destination needs to have a global address.
- Global address is an address that can be unique in the scope of the network or internationally if the network is part of an international network.

2) Virtual Circuit Identifier

- The identifier used for data-transfer is called the virtual-circuit identifier (VCI).
- A VCI, unlike a global address, is a small number that has only switch scope.
- VCI is used by a frame between two switches.
- When a frame arrives at a switch, it has a VCI. When the frame leaves, it has a different VCI.

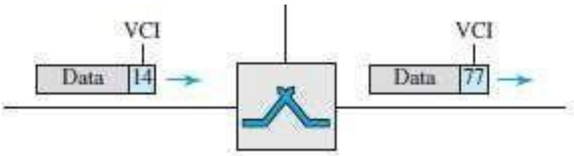


Figure 8.11 *Virtual-circuit identifier*

- Figure 8.11 show how the VCI in a data-frame changes from one switch to another.

1.1.2.2 Three Phases

- A source and destination need to go through 3 phases: setup, data-transfer, and teardown.

1) In setup phase, the source and destination use their global addresses to help switches make table entries for the connection.
2) In the teardown phase, the source and destination inform the switches to delete the corresponding entry.
3) Data-transfer occurs between these 2 phases.

1.1.2.2.1 Data Transfer Phase

To transfer a frame from a source to its destination, all switches need to have a table-entry for this virtual-circuit.

The table has four columns.

The switch holds 4 pieces of information for each virtual-circuit that is already set up.

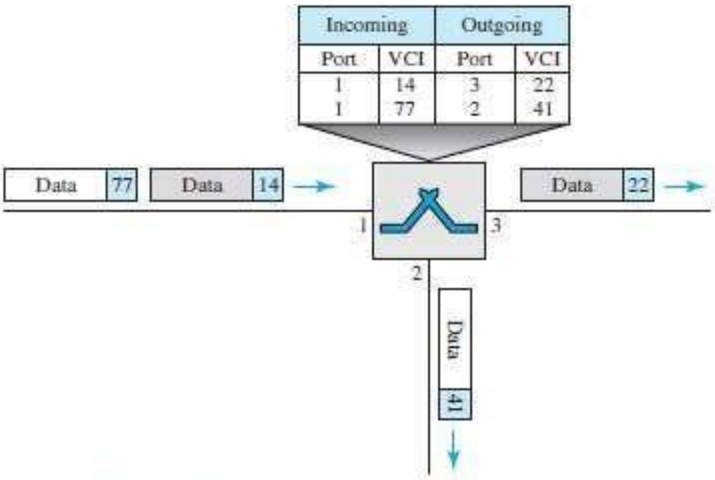


Figure 8.12 *Switch and tables in a virtual-circuit network*

- ➢ As shown in Figure 8.12, a frame arrives at port 1 with a VCI of 14.
- ➢ When the frame arrives, the switch looks in its table to find port 1 and a VCI of 14.
- ➢ When it is found, the switch knows to change the VCI to 22 & send out the frame from port 3.

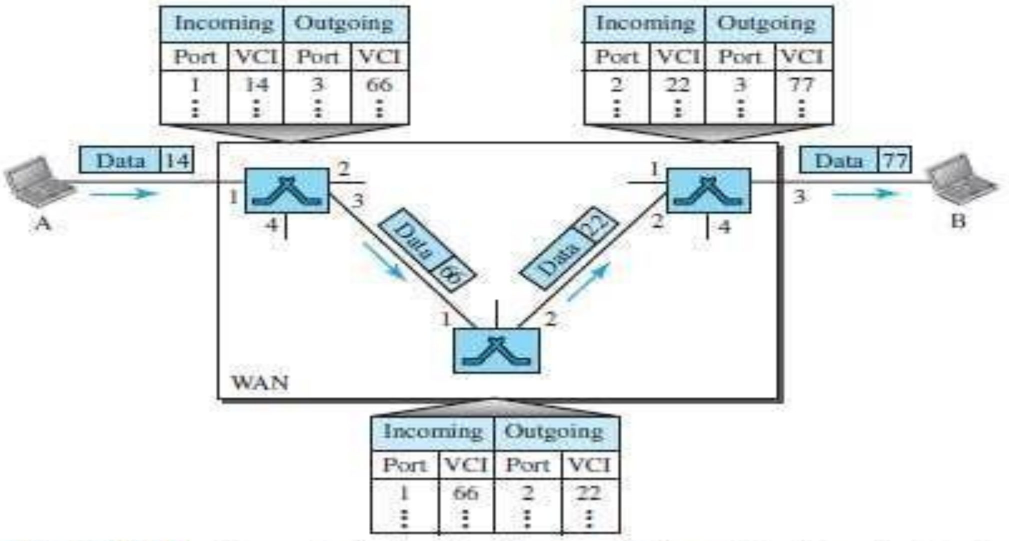


Figure 8.13 *Source-to-destination data transfer in a virtual-circuit network*

- ➢ As shown in Figure 8.13, each switch changes the VCI and routes the frame.
- ➢ The data-transfer phase is active until the source sends all its frames to the destination.
- ➢ The procedure at the switch is the same for each frame of a message.
- ➢ The process creates a virtual circuit, not a real circuit, between the source and destination.

1.1.2.2.2 Setup Phase

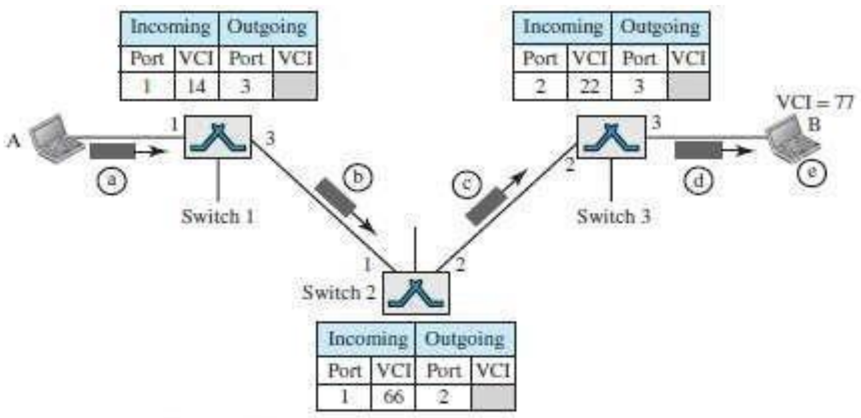
A switch creates an entry for a virtual-circuit.

For example, suppose source A needs to create a virtual-circuit to B.

Two steps are required: 1) Setup-request and
2) Acknowledgment.

1) Setup Request

➢ A setup-request frame is sent from the source to the destination (Figure 8.14).



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	

Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	

Figure 8.14 *Setup request in a virtual-circuit network*

➢ Following events occurs:

a) Source-A sends a setup-frame to switch-1.

b) Switch-1 receives the setup-frame.

¤ Switch-1 knows that a frame going from A to B goes out through port 3.

¤ The switch-1 has a routing table.

¤ The switch

→ creates an entry in its table for this virtual-circuit

→ is only able to fill 3 of the 4 columns.

¤ The switch

→ assigns the incoming port (1) and

→ chooses an available incoming-VCI (14) and the outgoing-port (3).

→ does not yet know the outgoing VCI, which will be found during the acknowledgment step.

¤ The switch then forwards the frame through port-3 to switch-2.

c) Switch-2 receives the setup-request frame.

¤ The same events happen here as at switch-1.

¤ Three columns of the table are completed: In this case, incoming port (1), incoming-VCI (66), and outgoing port (2).

d) Switch-3 receives the setup-request frame.

¤ Again, three columns are completed: incoming port (2), incoming-VCI (22), and outgoing-port (3).

e) Destination-B

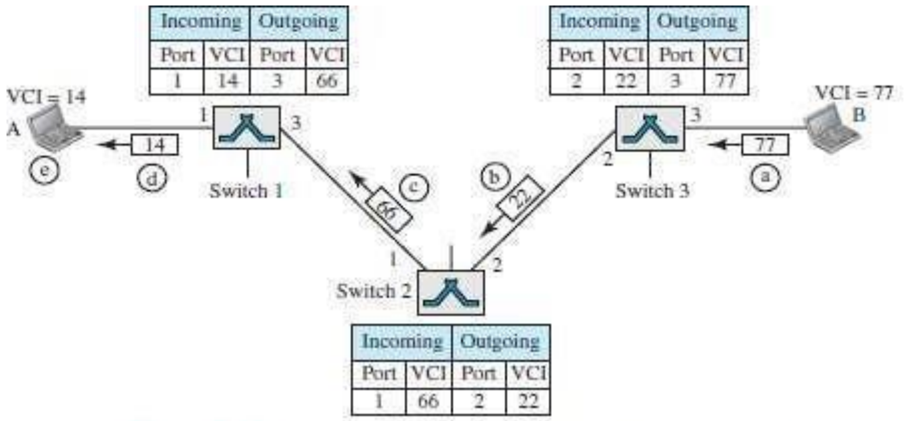
→ receives the setup-frame

→ assigns a VCI to the incoming frames that come from A, in this case 77.

¤ This VCI lets the destination know that the frames come from A, and no other sources.

2) Acknowledgment

➢ A special frame, called the acknowledgment-frame, completes the entries in the switching- tables (Figure 8.15).



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	66

Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	77

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	22

Figure 8.15 *Setup acknowledgment in a virtual-circuit network*

a) The destination sends an acknowledgment to switch-3.

¤ The acknowledgment carries the global source and destination-addresses so the switch knows which entry in the table is to be completed.

¤ The frame also carries VCI 77, chosen by the destination as the incoming-VCI for frames from A.

¤ Switch 3 uses this VCI to complete the outgoing VCI column for this entry.

b) Switch 3 sends an acknowledgment to switch-2 that contains its incoming-VCI in the table, chosen in the previous step.

¤ Switch-2 uses this as the outgoing VCI in the table.

c) Switch-2 sends an acknowledgment to switch-1 that contains its incoming-VCI in the table, chosen in the previous step.

¤ Switch-1 uses this as the outgoing VCI in the table.

d) Finally switch-1 sends an acknowledgment to source-A that contains its incoming-VCI in the table, chosen in the previous step.

e) The source uses this as the outgoing VCI for the data-frames to be sent to destination-B.

1.1.2.3 Teardown Phase

- Source-A, after sending all frames to B, sends a special frame called a teardown request.
- Destination-B responds with a teardown confirmation frame.
- All switches delete the corresponding entry from their tables.

1.1.2.4 Efficiency

- Resource reservation can be made in 2 cases:
  1) During the setup: Here, the delay for each packet is the same.
  2) On demand: Here, each packet may encounter different delays.

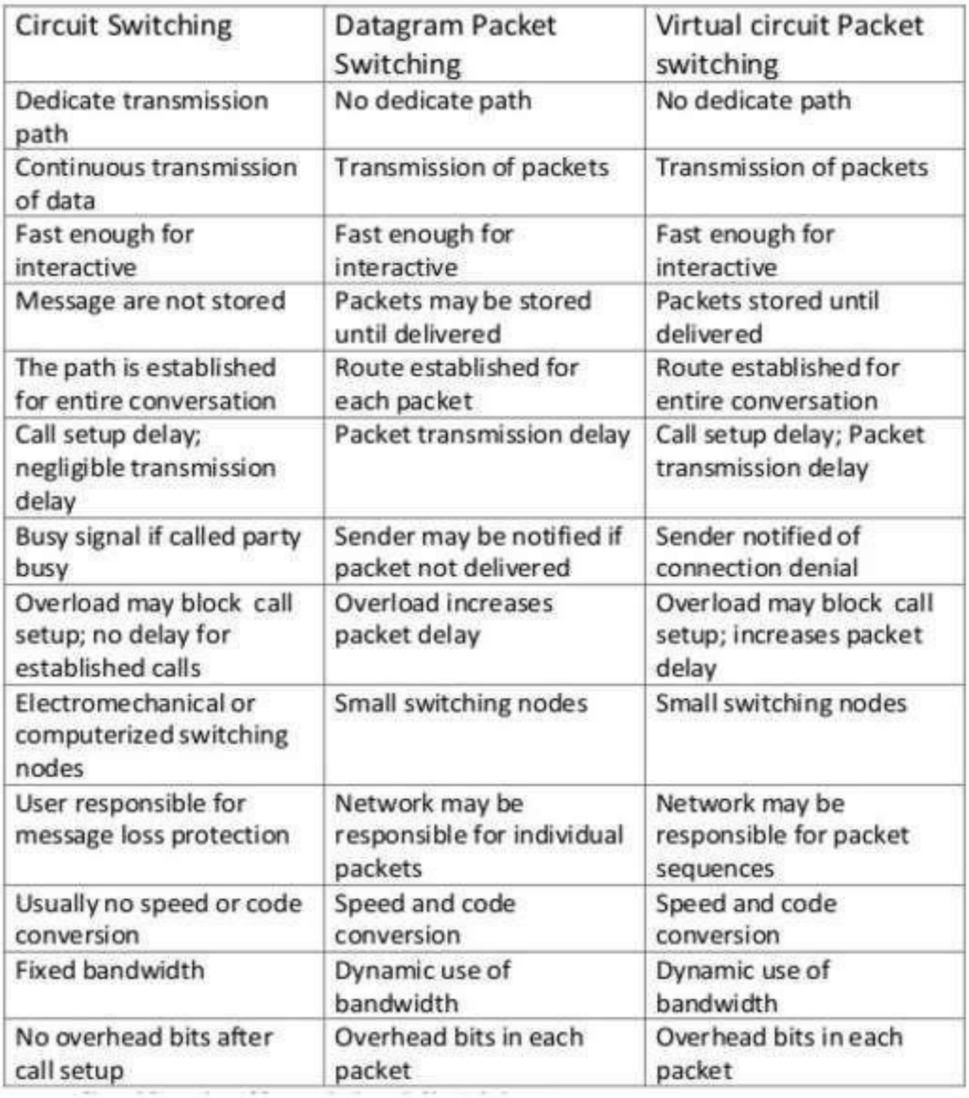
- Advantage of on demand resource allocation:

  The source can check the availability of the resources, without actually reserving it.

1.1.2.5 Delay in Virtual Circuit Networks

- There is a one-time delay for setup and a one-time delay for teardown (Figure 8.16).
- If resources are allocated during the setup phase, there is no wait time for individual packets.
- The packet is traveling through two switches (routers).
- There are three transmission times (3T), three propagation times (3τ), data transfer delay, a setup delay and a teardown delay.
- The total delay time is

$$\text{Total delay} + 3T + 3\tau + \text{setup delay} + \text{teardown delay}$$



Circuit Switching	Datagram Packet Switching	Virtual circuit Packet switching
Dedicate transmission path	No dedicate path	No dedicate path
Continuous transmission of data	Transmission of packets	Transmission of packets
Fast enough for interactive	Fast enough for interactive	Fast enough for interactive
Message are not stored	Packets may be stored until delivered	Packets stored until delivered
The path is established for entire conversation	Route established for each packet	Route established for entire conversation
Call setup delay; negligible transmission delay	Packet transmission delay	Call setup delay; Packet transmission delay
Busy signal if called party busy	Sender may be notified if packet not delivered	Sender notified of connection denial
Overload may block call setup; no delay for established calls	Overload increases packet delay	Overload may block call setup; increases packet delay
Electromechanical or computerized switching nodes	Small switching nodes	Small switching nodes
User responsible for message loss protection	Network may be responsible for individual packets	Network may be responsible for packet sequences
Usually no speed or code conversion	Speed and code conversion	Speed and code conversion
Fixed bandwidth	Dynamic use of bandwidth	Dynamic use of bandwidth
No overhead bits after call setup	Overhead bits in each packet	Overhead bits in each packet