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

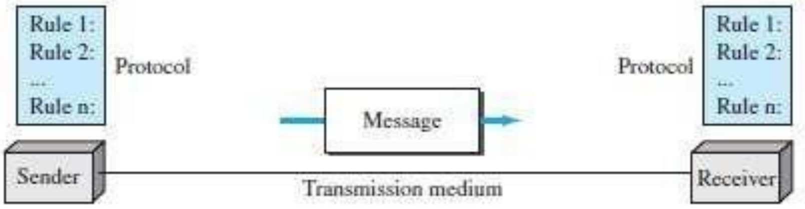


Figure 1.1 *Five components of data communication*

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.

1.1.3 Direction of Data Flow

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

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

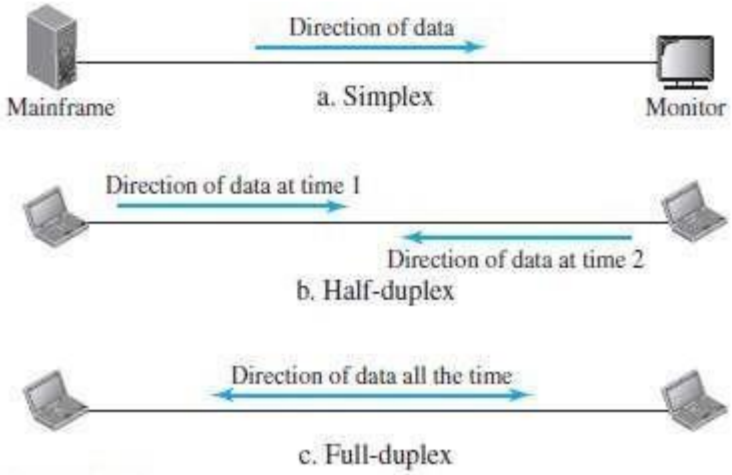

Direction of data
Mainframe
a. Simplex
Monitor
Direction of data at time 1
Direction of data at time 2
b. Half-duplex
Direction of data all the time
c. Full-duplex

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)

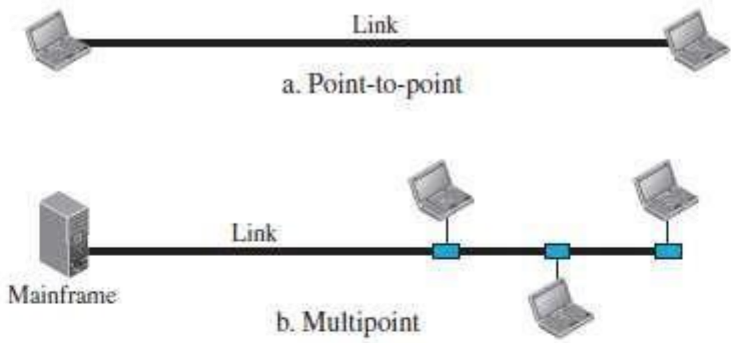


Figure 1.3 *Types of connections: point-to-point and multipoint*

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.

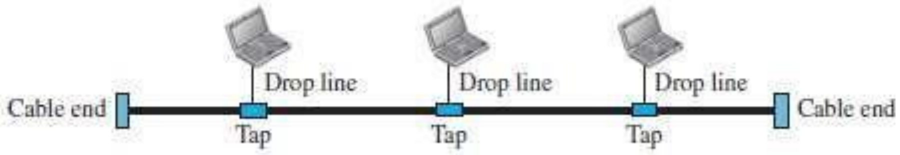


Figure 1.4 *A bus topology connecting three stations*

- 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.

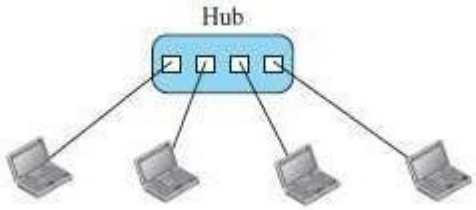


Figure 1.5 *A star topology connecting four stations*

- 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.

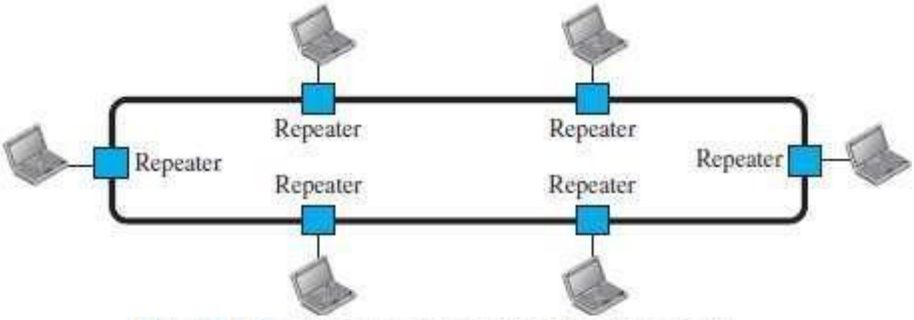


Figure 1.6 *A ring topology connecting six stations*

- 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.

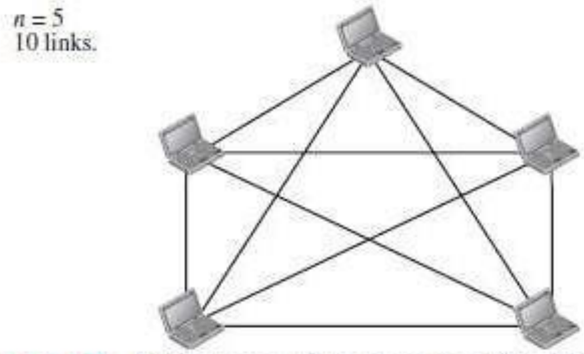


Figure 1.7 *A fully connected mesh topology (five devices)*

- 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.

1.3.3 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.

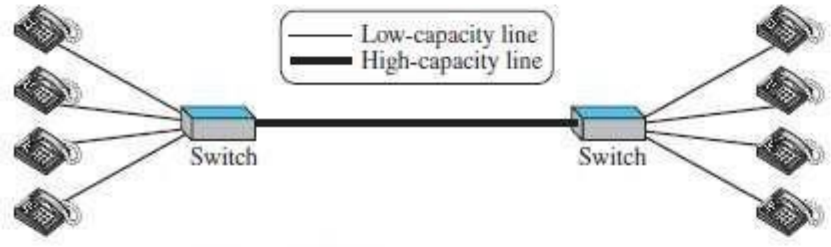


Figure 1.13 *A circuit-switched network*

¤ 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.

- 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.

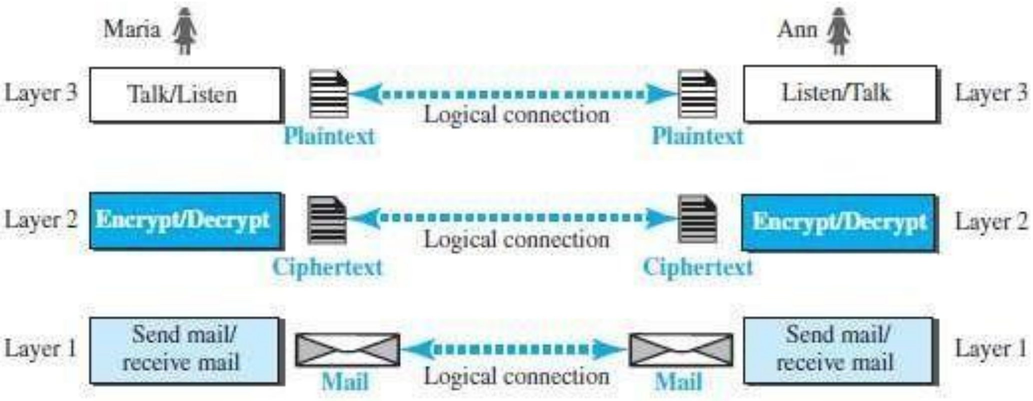
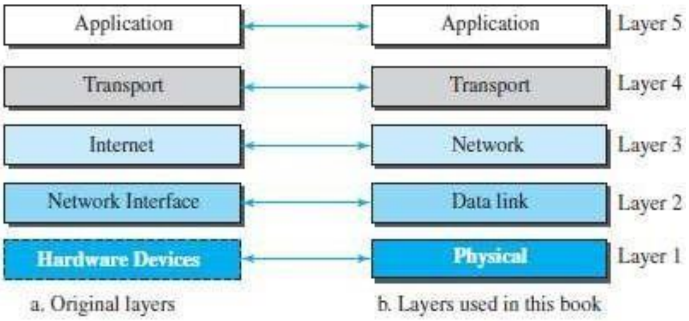


Figure 2.3 *Logical connection between peer layers*

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*

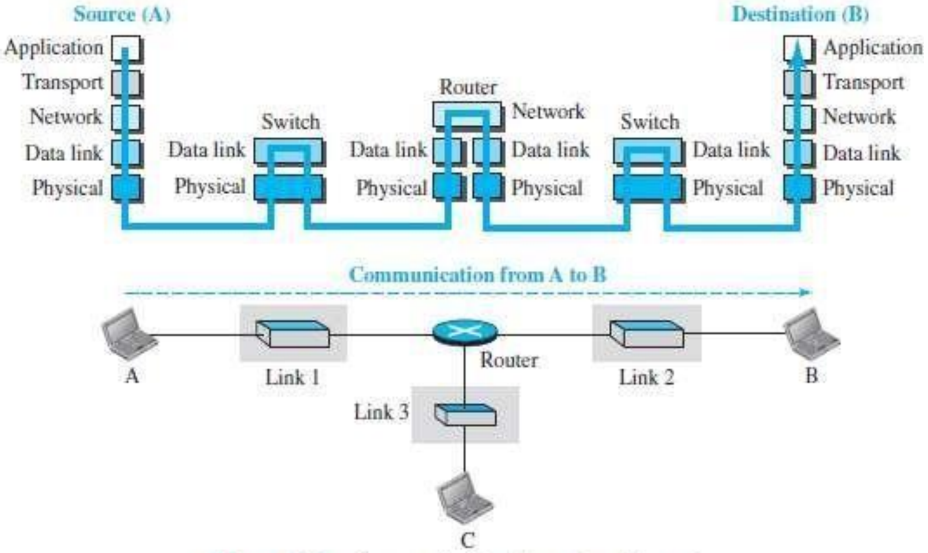


Figure 2.5 *Communication through an internet*

- 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

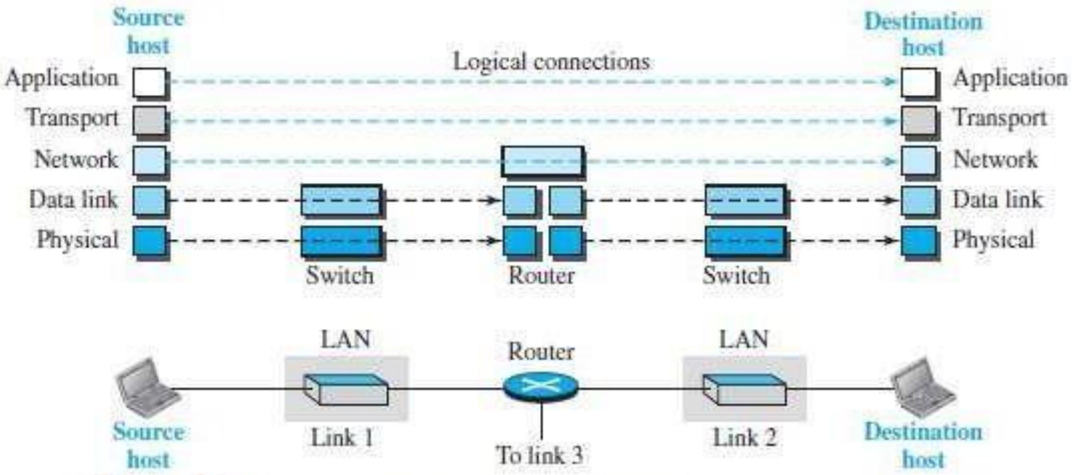


Figure 2.6 *Logical connections between layers of the TCP/IP protocol suite*

- 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.

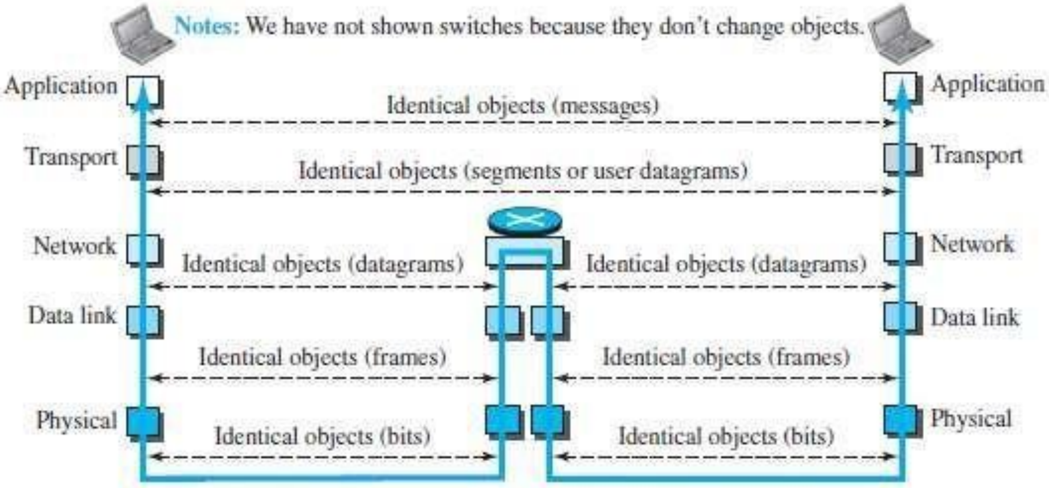

Notes: We have not shown switches because they don't change objects.
Application
Transport
Network
Data link
Physical
Application
Transport
Network
Data link
Physical
Identical objects (messages)
Identical objects (segments or user datagrams)
Identical objects (datagrams)
Identical objects (datagrams)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

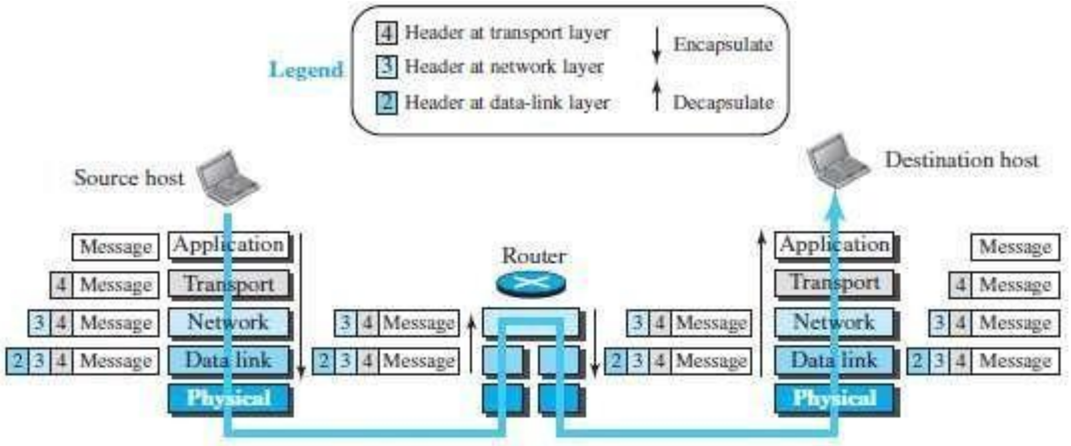


Figure 2.8 *Encapsulation/Decapsulation*

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 are application specific channels for device to device communication at transport layer level.

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.

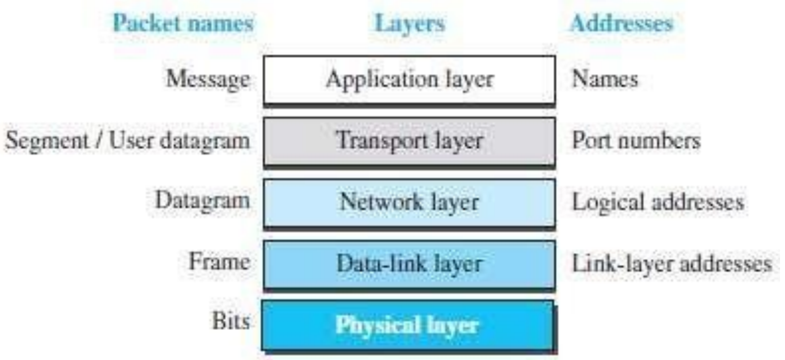


Figure 2.9 *Addressing in the TCP/IP protocol suite*

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).

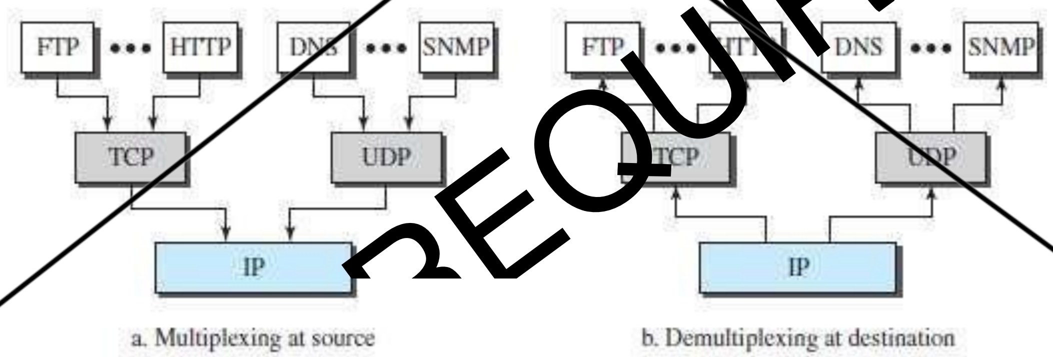
  1) At transport layer, either UDP or TCP can accept a message from several application-layer protocols.

  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*

REQUIRED

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.

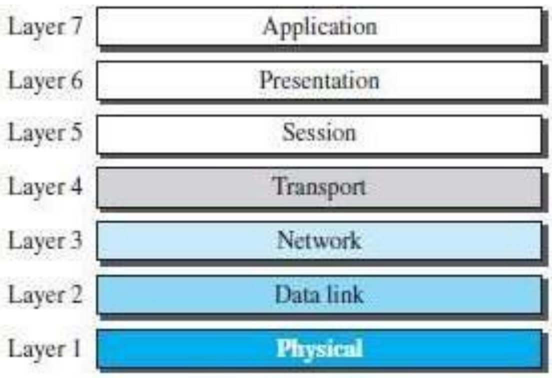


Figure 2.11 *The OSI model*

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.

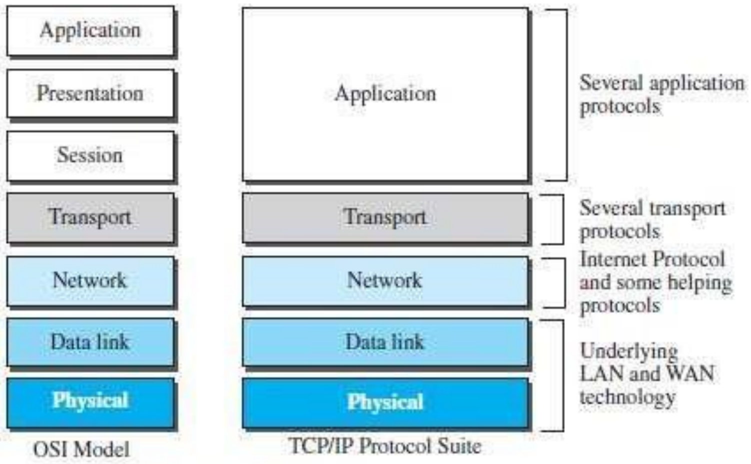


Figure 2.12 *TCP/IP and OSI model*

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

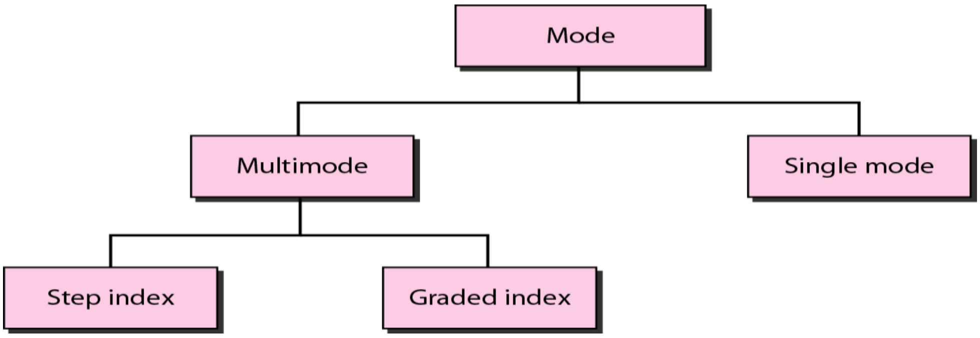
Two different types of **light sources** are used in fiber optic system.

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

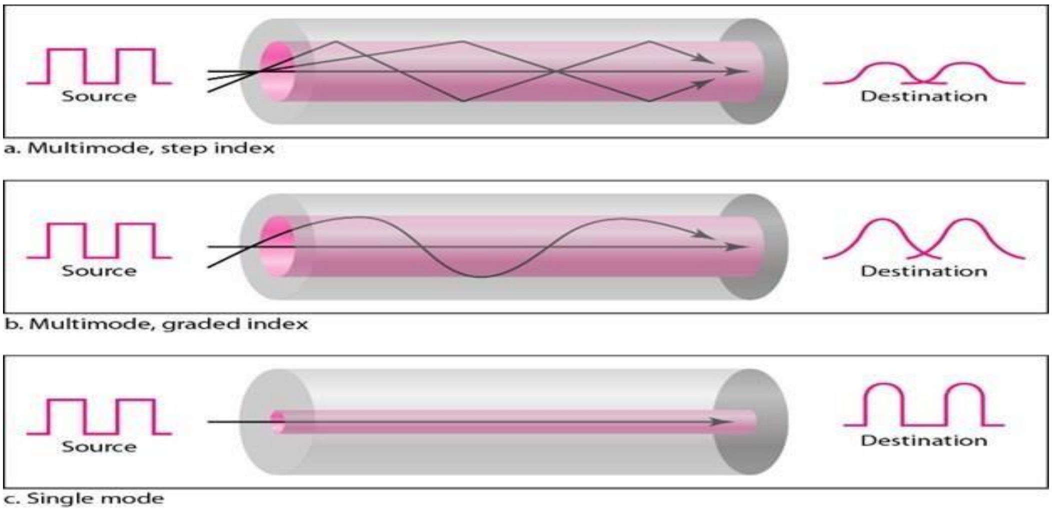
Both are semiconductor devices that emit a beam of light when voltage is applied. Led is less costly than ILD. ILD operates on laser principle, is more efficient, and can sustain greater data rate.

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