MODULE 1: INTRODUCTION

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

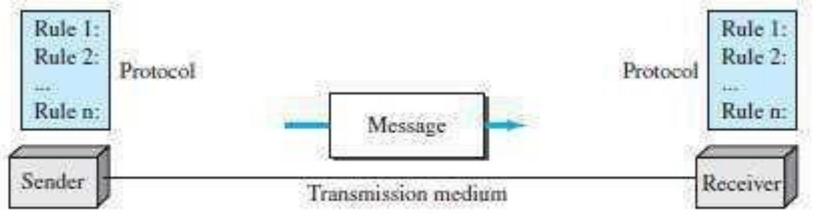


Figure 1.1 *Five components of data communication*

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

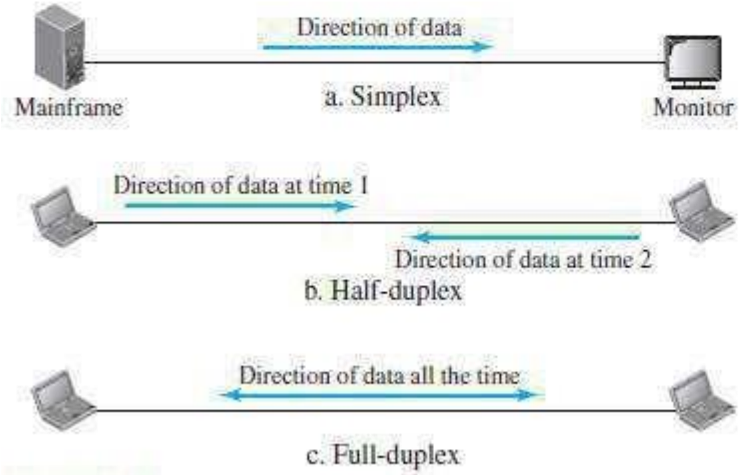

Direction of data
Mainframe
a. Simplex
Monitor
Direction of data at time 1
Direction of data at time 2
b. Half-duplex
Direction of data all the time
c. Full-duplex

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 the same time).
▯ For example (Figure 1.2c):
Mobile phones (When 2 people are communicating by a telephone line, both can listen and 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)

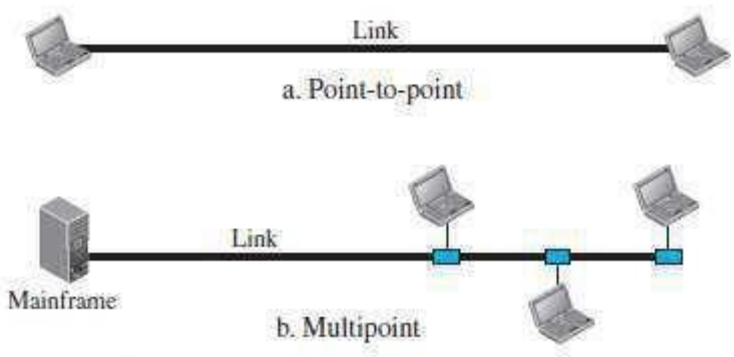


Figure 1.3 *Types of connections: point-to-point and multipoint*

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.

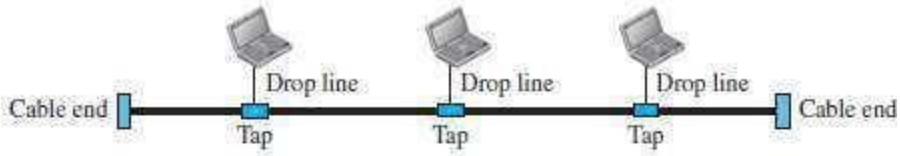


Figure 1.4 *A bus topology connecting three stations*

- 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.

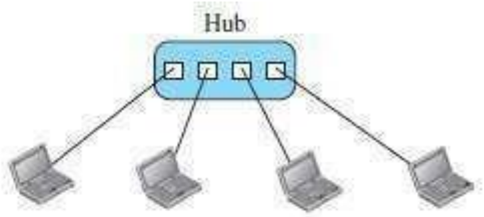


Figure 1.5 *A star topology connecting four stations*

- 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.

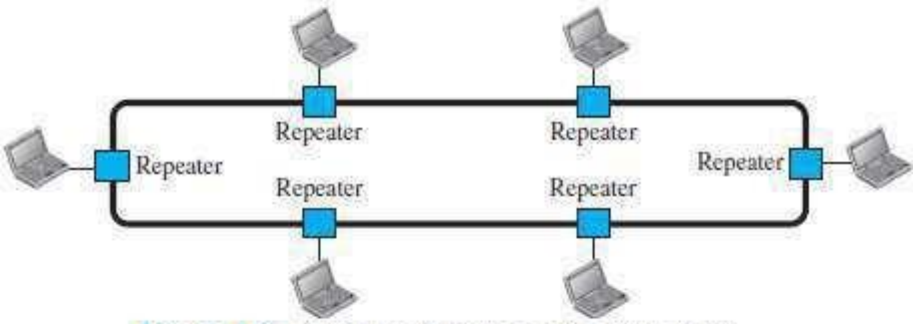


Figure 1.6 *A ring topology connecting six stations*

- 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.

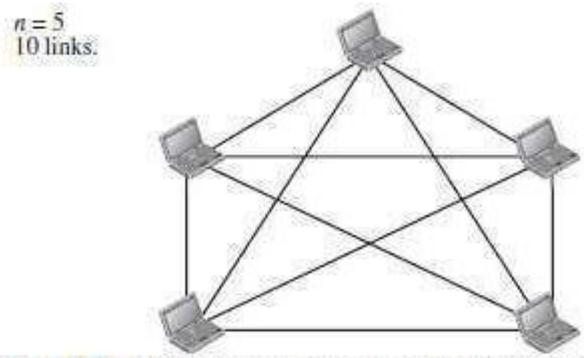


Figure 1.7 *A fully connected mesh topology (five devices)*

- 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 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.

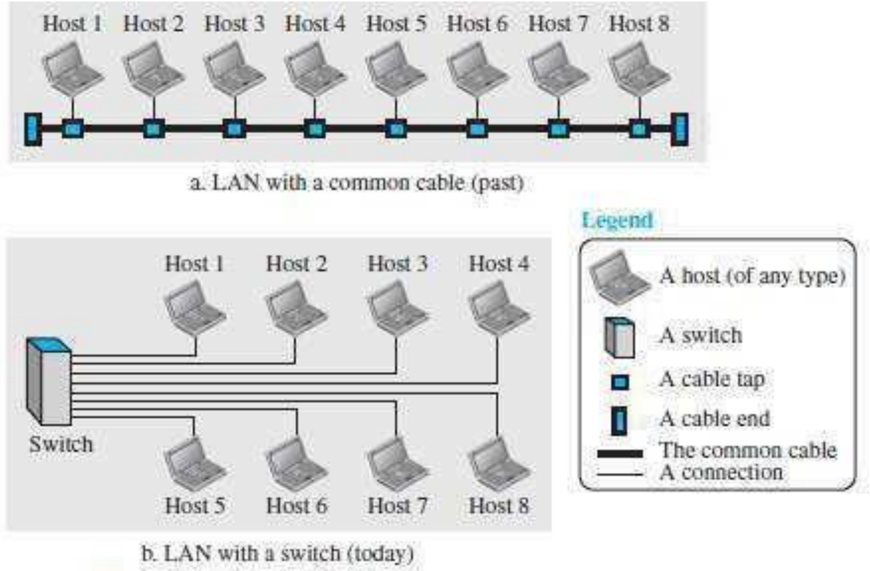


Figure 1.8 *An isolated LAN in the past and today*

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).

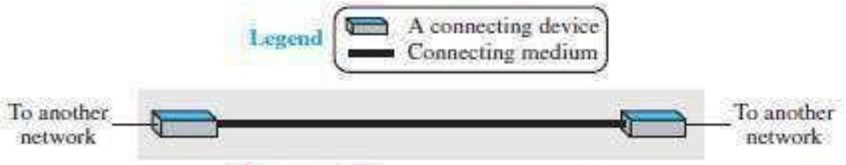


Figure 1.9 *A point-to-point WAN*

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).

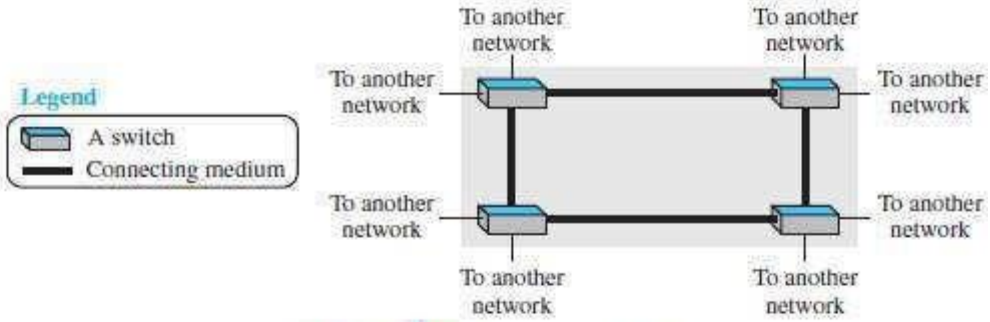


Figure 1.10 *A switched WAN*

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).

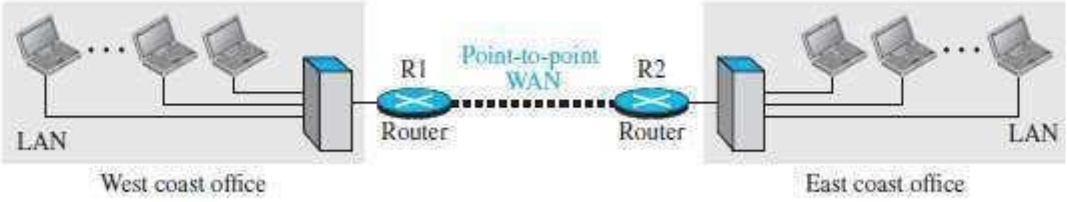


Figure 1.11 *An internetwork made of two LANs and one point-to-point WAN*

▯ When a host in the west coast office sends a message to another host in the same office, the router blocks the message, but the switch directs the message to the destination.

▯ On the other hand, when a host on the west coast sends a message to a host on the east coast, router R1 routes the packet to router R2, and the packet reaches the destination.

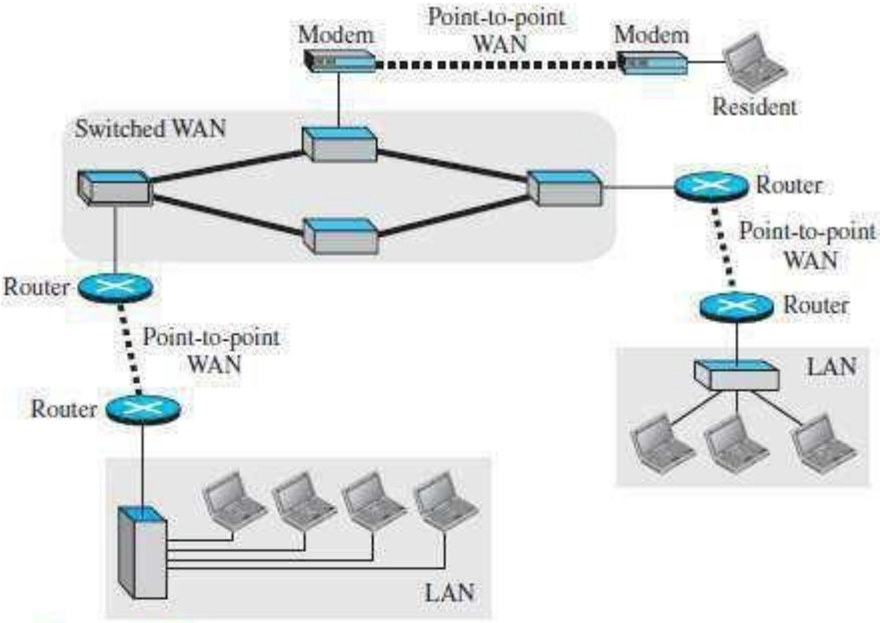


Figure 1.12 *A heterogeneous network made of four WANs and three LANs*

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 such as 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.

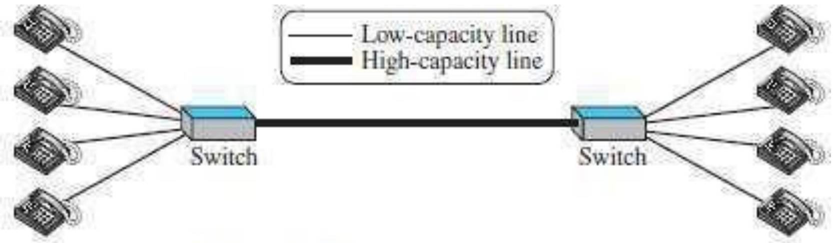


Figure 1.13 *A circuit-switched network*

¤ 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 entity that can be stored and sent later.

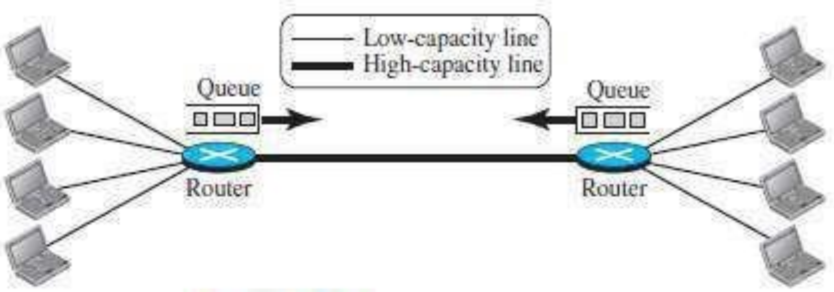


Figure 1.14 *A packet-switched network*

¤ 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 is no 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.

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.

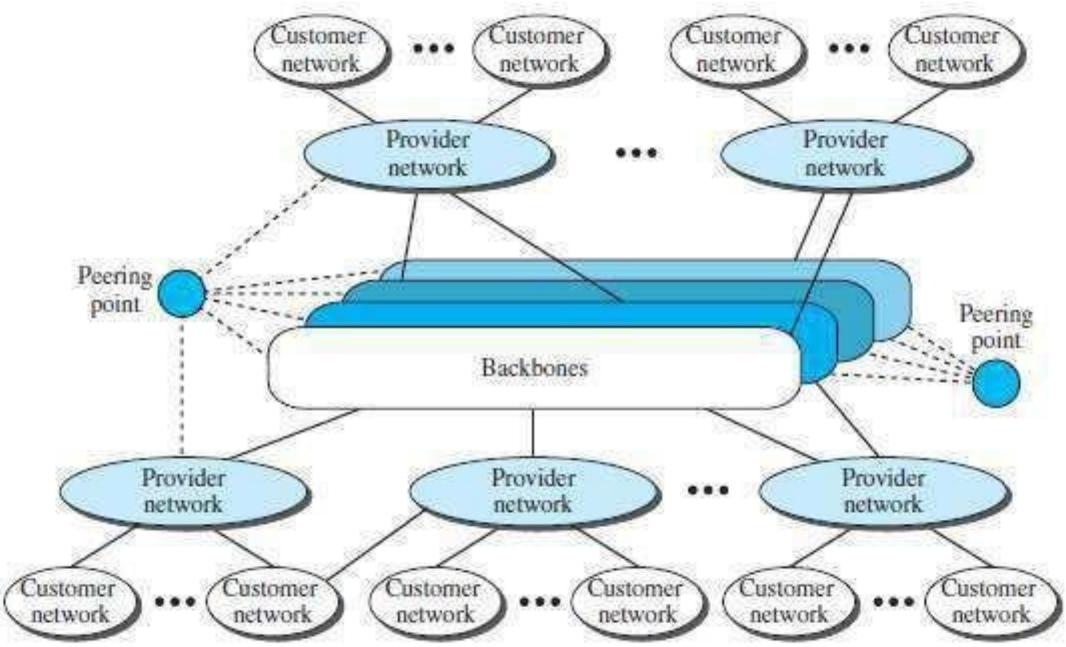


Figure 1.15 *The Internet today*

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 voice connection.
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 higher speed 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 STANDARDS AND ADMINISTRATION

1.4.1 Internet Standards

- An Internet standard is a thoroughly tested specification useful to those who work with the Internet.
- The Internet standard is a formalized-regulation that must be followed.
- There is a strict procedure by which a specification attains Internet standard status.
- A specification begins as an Internet draft.
- An Internet draft is a working document with no official status and a 6-month lifetime.
- Upon recommendation from the Internet authorities, a draft may be published as a RFC.
- Each RFC is edited, assigned a number, and made available to all interested parties.
- RFCs go through maturity levels and are categorized according to their requirement level.

(working document □ a work in progress RFC □ Request for Comment)

1.4.1.1 Maturity Levels

- An RFC, during its lifetime, falls into one of 6 maturity levels (Figure 1.16):

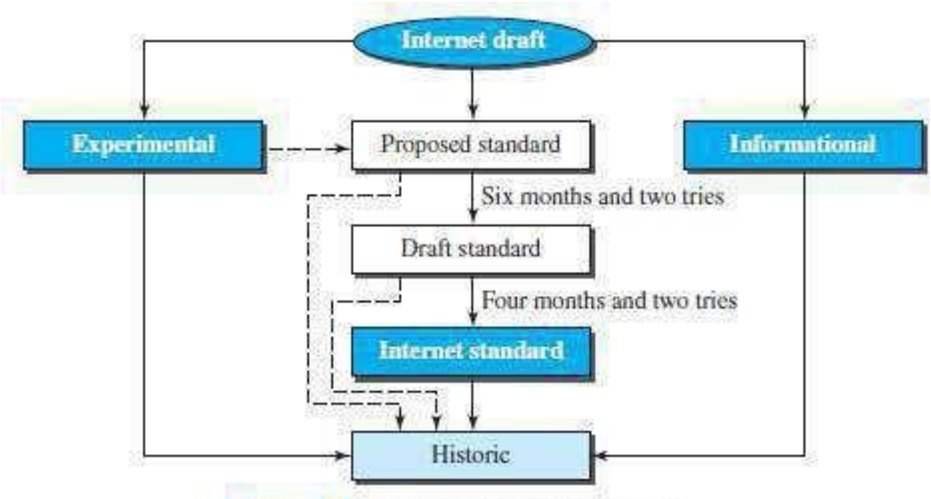


Figure 1.16 *Maturity levels of an RFC*

1) Proposed Standard

□ Proposed standard is specification that is stable, well-understood & of interest to Internet community.

□ Specification is usually tested and implemented by several different groups.

2) Draft Standard

□ A proposed standard is elevated to draft standard status after at least 2 successful independent and interoperable implementations.

3) Internet Standard

□ A draft standard reaches Internet standard status after demonstrations of successful implementation.

4) Historic

□ The historic RFCs are significant from a historical perspective. □ They either

→ have been superseded by later specifications or

→ have never passed the necessary maturity levels to become an Internet standard.

5) Experimental

□ An RFC classified as experimental describes work related to an experimental situation. □ Suchan RFC should not be implemented in any functional Internet service.

6) Informational

□ An RFC classified as informational contains general, historical, or tutorial information related to the Internet.

□ Usually, it is written by a vendor.

(ISOC □ Internet Society IAB □ Internet Architecture Board)
(IETF □ Internet Engineering Task Force IRTF □ Internet Research Task Force)
(IESG □ Internet Engineering Steering Group IRSG □ Internet Research Steering Group)

1.4.1.2 Requirement Levels

- RFCs are classified into 5 requirement levels:

1) Required

▫ An RFC labeled required must be implemented by all Internet systems to achieve minimum conformance.

▫ For example, IP and ICMP are required protocols.

2) Recommended

▫An RFC labeled recommended is not required for minimum conformance. ▫It is recommended because of its usefulness.

▫ For example, FTP and TELNET are recommended protocols.

3) Elective

▫ An RFC labeled elective is not required and not recommended. ▫ However, a system can use it for its own benefit.

4) Limited Use

▫An RFC labeled limited use should be used only in limited situations. ▫Mostof the experimental RFCs fall under this category.

5) Not Recommended

▫ An RFC labeled not recommended is inappropriate for general use. ▫ Normally a historic RFC may fall under this category.

1.4.2 Internet Administration

1) ISOC

- ISOC is a nonprofit organization formed to provide support for Internet standards process (Fig 1.17).
- ISOC maintains and supports other Internet administrative bodies such as IAB, IETF, IRTF, and IANA.

2) IAB

- IAB is the technical advisor to the ISOC.
- Two main purposes of IAB:
  i) To oversee the continuing development of the TCP/IP Protocol Suite
  ii) To serve in a technical advisory capacity to research members of the Internet community.
- Another responsibility of the IAB is the editorial management of the RFCs.
- IAB is also the external liaison between the Internet and other standards organizations and forums.
- IAB has 2 primary components: i) IETF and ii) IRTF.

i) IETF

▫ IETF is a forum of working groups managed by the IESG.

▫IETF is responsible for identifying operational problems & proposing solutions to the problems ▫IETF also develops and reviews specifications intended as Internet standards.

▫The working groups are collected into areas, and each area concentrates on a specific topic. ▫ Currently 9 areas have been defined. The areas include applications, protocols, routing, network management next generation (IPng), and security.

ii) IRTF

▫ IRTF is a forum of working groups managed by the IRSG.

▫ IRTF focuses on long-term research topics related to Internet protocols, applications, architecture, and technology.

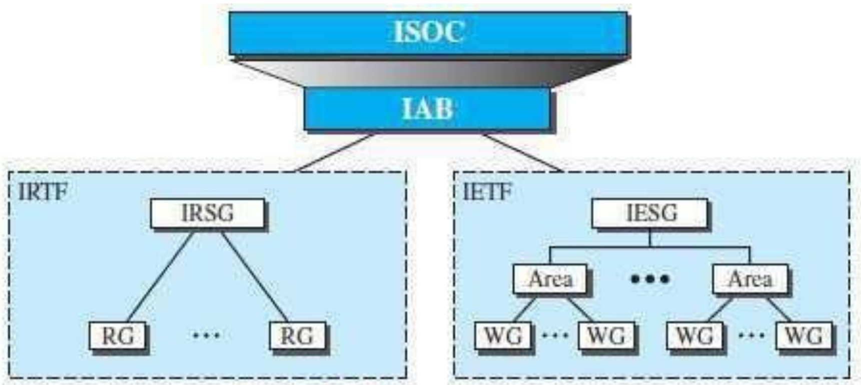


Figure 1.17 *Internet administration*

NETWORK MODELS

1.5 PROTOCOL LAYERING

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

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

1.5.1 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

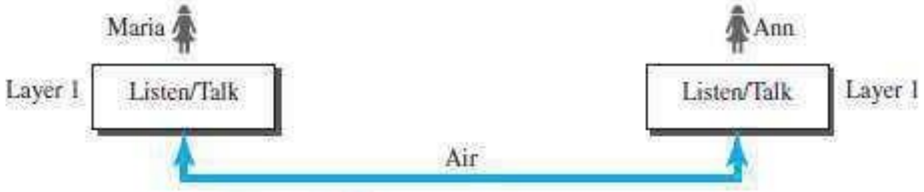


Figure 2.1 *A single-layer protocol*

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.

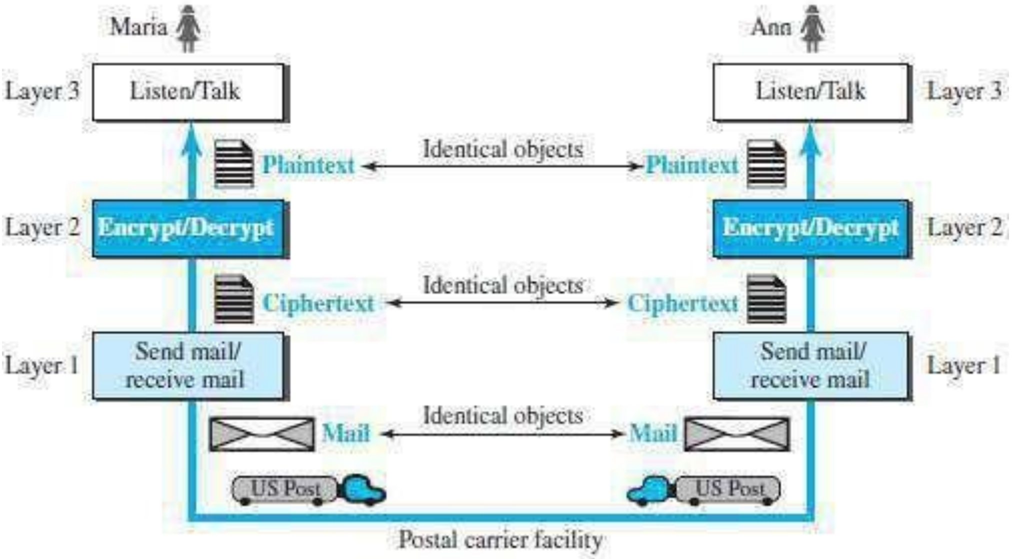


Figure 2.2 *A three-layer protocol*

1.5.1.1 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.

1.5.2 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.

1.5.3 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 created from that layer.

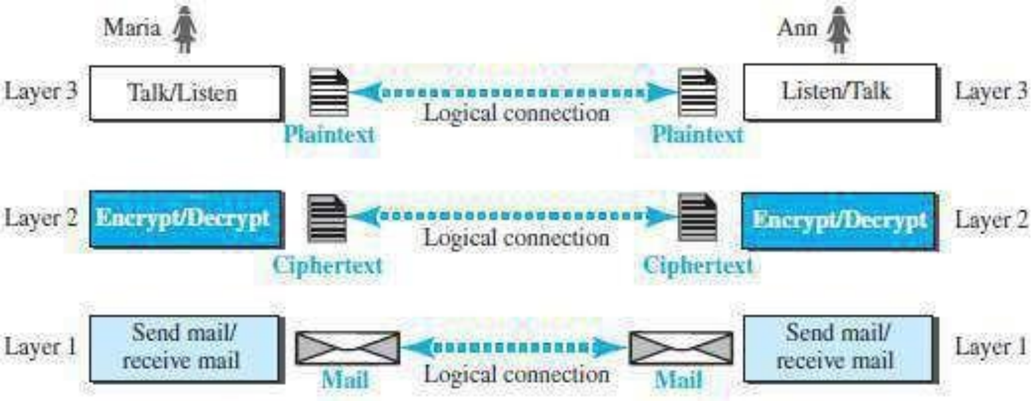


Figure 2.3 *Logical connection between peer layers*

1.6 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 by one or more lower level protocols.

1.6.1 Layered Architecture

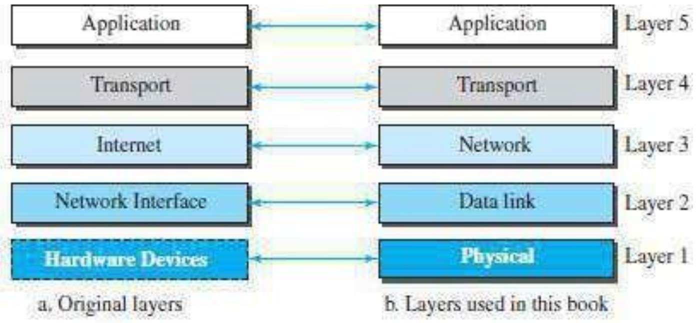


Figure 2.4 Layers in the TCP/IP protocol suite

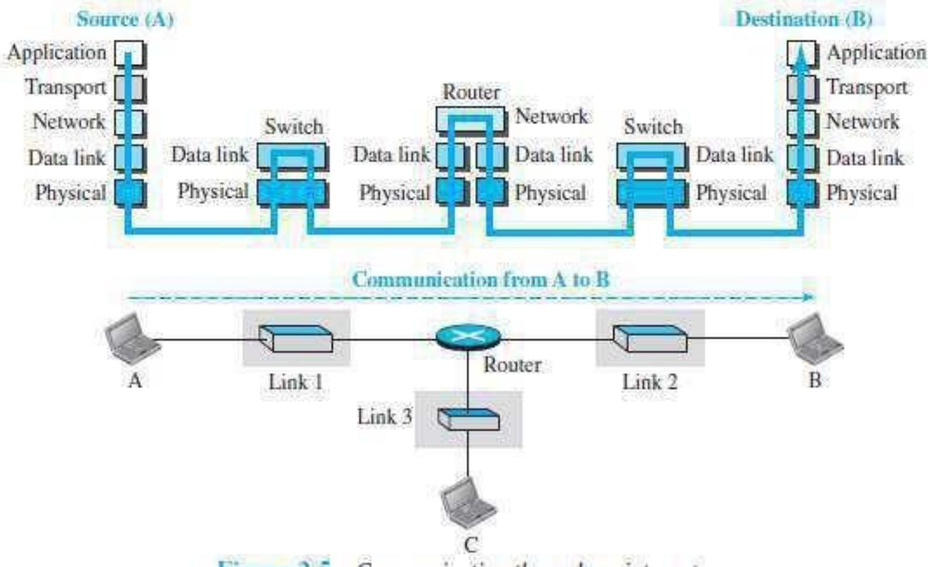


Figure 2.5 Communication through an internet

- 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.

1.6.2 Layers in the TCP/IP Protocol Suite

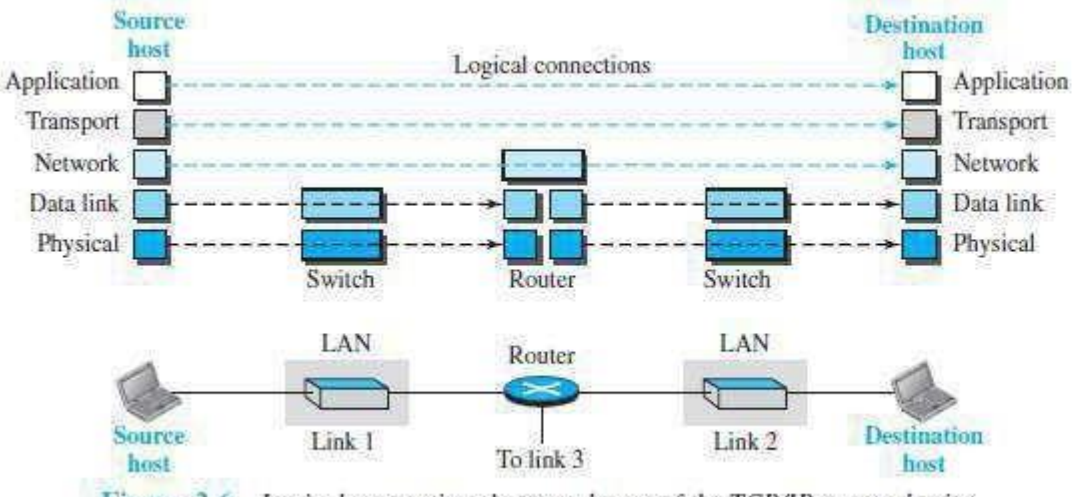


Figure 2.6 *Logical connections between layers of the TCP/IP protocol suite*

- 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.

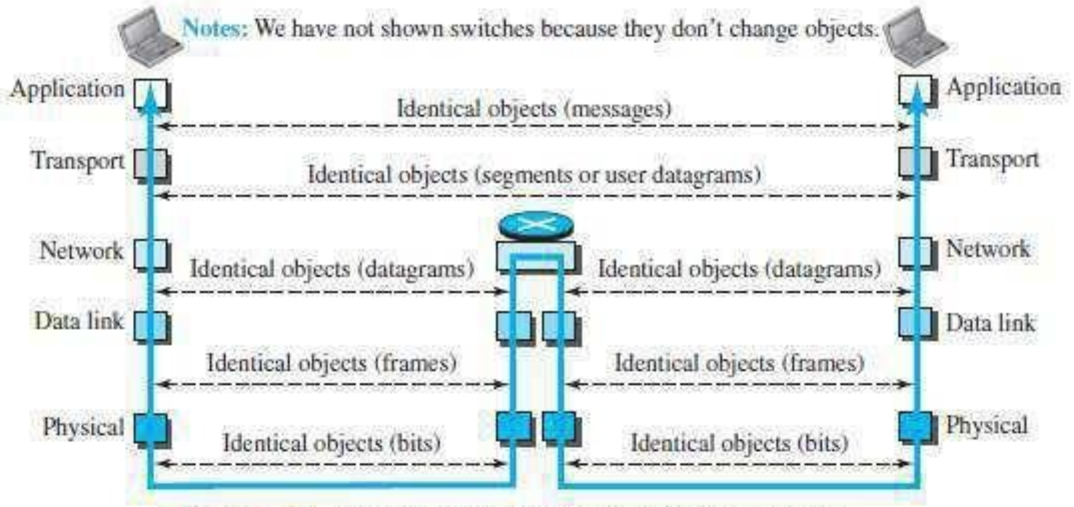

Notes: We have not shown switches because they don't change objects.
Application
Identical objects (messages)
Transport
Identical objects (segments or user datagrams)
Network
Identical objects (datagrams)
Identical objects (datagrams)
Data link
Identical objects (frames)
Identical objects (frames)
Physical
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 network layer and send more packets than received (Figure 2.7).
- The link between two hops does not change the object.

1.6.3 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 transportlayer 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)

1.6.4 Encapsulation and Decapsulation

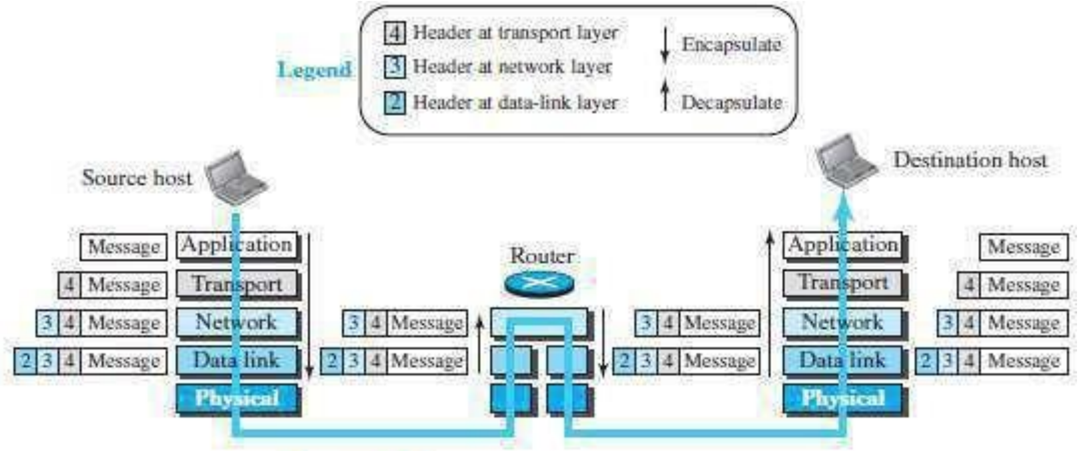


Figure 2.8 *Encapsulation/Decapsulation*

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 to two 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

1.6.5 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 the same 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.

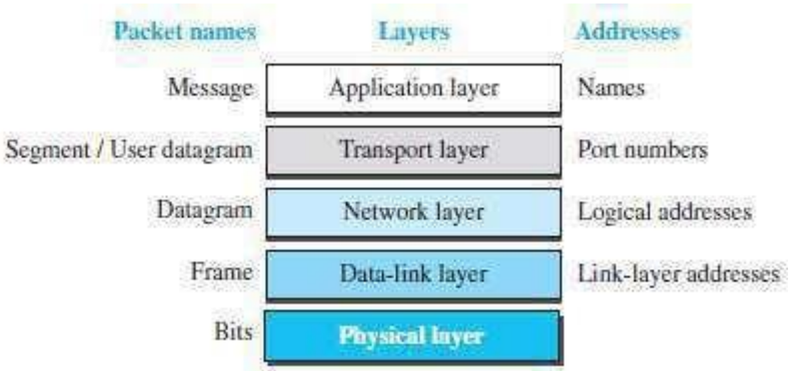


Figure 2.9 *Addressing in the TCP/IP protocol suite*

1.6.6 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).

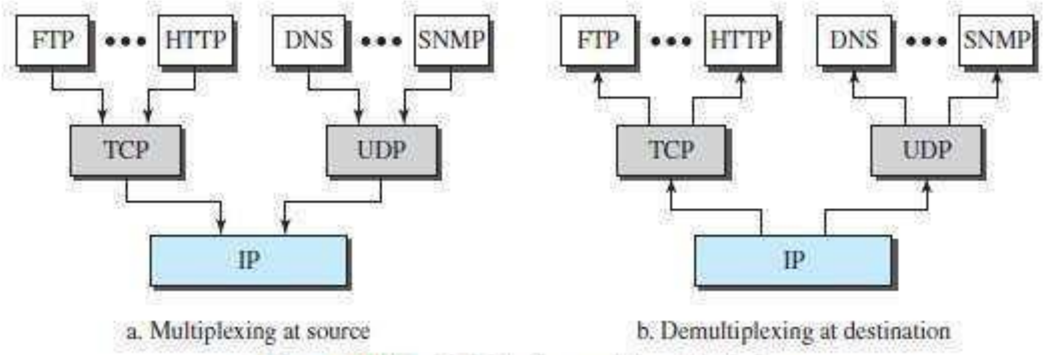
• Demultiplexing means a protocol can decapsulate and deliver a packet to several next-higher layer protocols (one at a time).

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*

1.7 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.

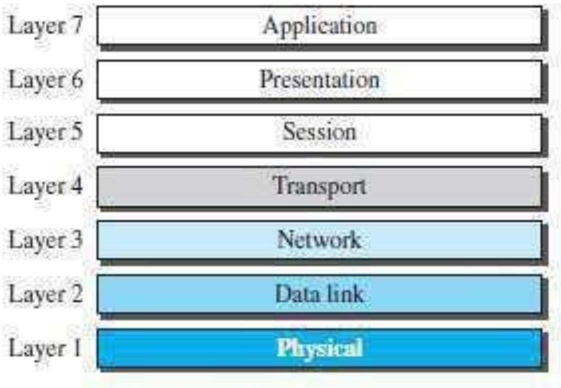


Figure 2.11 *The OSI model*

1.7.1 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 mixed and matched depending on the needs of the system.

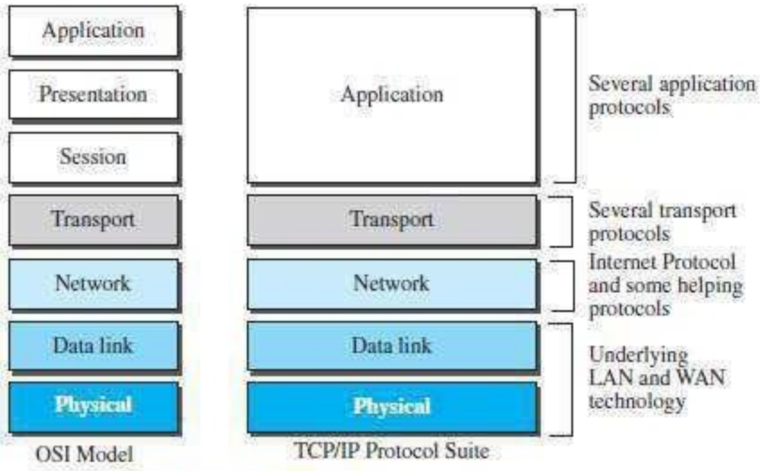


Figure 2.12 *TCP/IP and OSI model*

1.7.2 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 on the 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

LAYERS IN THE OSI MODEL (Detailed OSI layers not in syllabus, it's for your reference)
Physical Layer

• Main Responsibility:
Physical-layer (PL) is responsible for movements of individual bits from one node to another node.

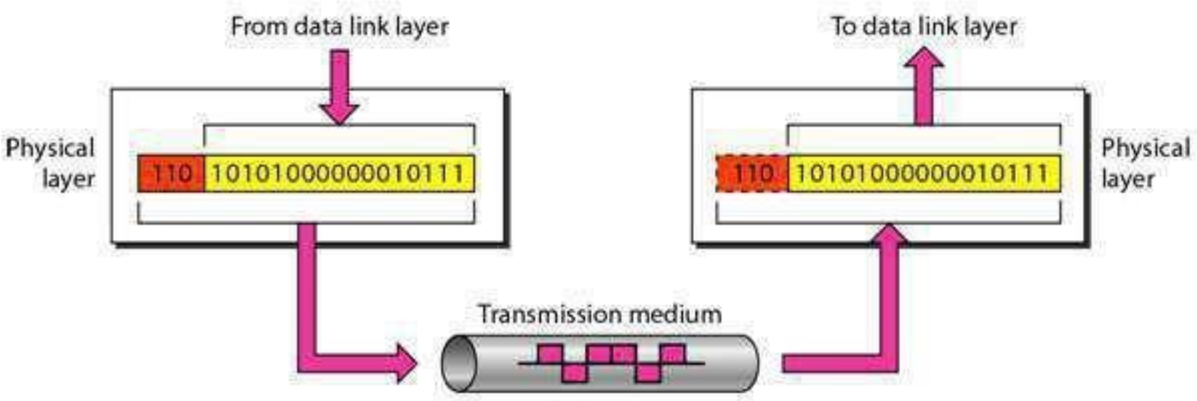


Figure 2.5 *Physical layer*

• Other responsibilities of Physical-layer (Figure 2.5):

1) Physical Characteristics of Interfaces and Medium

□ PL defines the mechanical/electrical characteristics of the interface & transmission-medium
i.e. Mechanical □cable, plugs, pins
Electrical □modulation, signal strength, voltage levels
□ PL also defines the type of transmission-medium. (Wired or wireless).

2) Representation of Bits

□PL defines the type of encoding i.e. how 0s and 1s are changed to signals. □Data consists of a stream of bits: 0s or 1s.
□ Bits must be encoded into signals for transmission.

3) Data Rate

□ PL defines the transmission-rate.
□ Transmission-rate refers to the number of bits sent per second.

4) Synchronization of Bits

□PL deals with the synchronization of the transmitter and receiver. □The sender and receiver are synchronized at bit-level.

5) Line Configuration

□ PL defines the nature of the connection.
i) In a point-to-point configuration, a dedicated-link is used to connect between 2 devices
ii) In a multipoint configuration, a shared-link is used to connect between 2 or more devices.

6) Physical Topology

□ PL defines the type of topology used for connecting the devices in the network. □ Topologies can be mesh, star, ring or bus.

7) Transmission Mode

□ PL defines the direction of data-transfer between 2 devices.
i) Simplex: Only one device can send; the other device can only receive.
ii) Half-duplex: Two devices can send and receive, but not at the same time. iii) Full-duplex: Two devices can send and receive at the same time.

Data Link Layer

- Main Responsibility:

Data-link-layer (DLL) is responsible for moving frames from one node to another node.

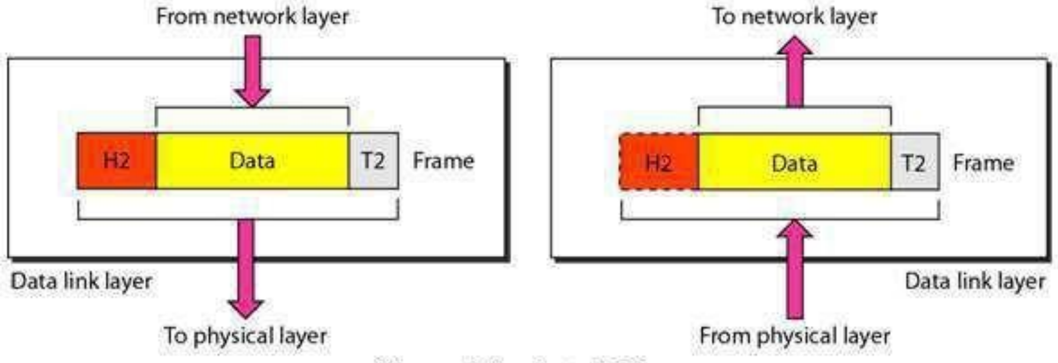


Figure 2.6 *Data link layer*

- Other responsibilities of data-link-layer (Figure 2.6 & 2.7):

1) Framing

▫ DLL receives & divides the stream of bits from network-layer into frames.

2) Physical-addressing

▫ DLL appends a header to the frame coming from the network-layer.
▫ Header contains the physical-address of sender & receiver of the frame.

3) Flow Control

▫ DLL provides flow-control.
▫ Flow-control ensures that source sends the data at a speed at which destination can receive it ▫ If there is an overflow at the receiver-side, the data will be lost.

4) Error Control

▫ DLL provides error-control.
▫ Error-control is process of identification or correction of error occurred in the transmitted data ▫ Error-control uses mechanisms to

→ detect damaged-frames
→ retransmit lost-frames
→ recognize duplicate frames.

▫ Normally, error control information is present in the trailer of a frame.

5) Access Control

▫ DLL provides access-control.
▫ Access-control determines which device has right to send the data in a multipoint connection.

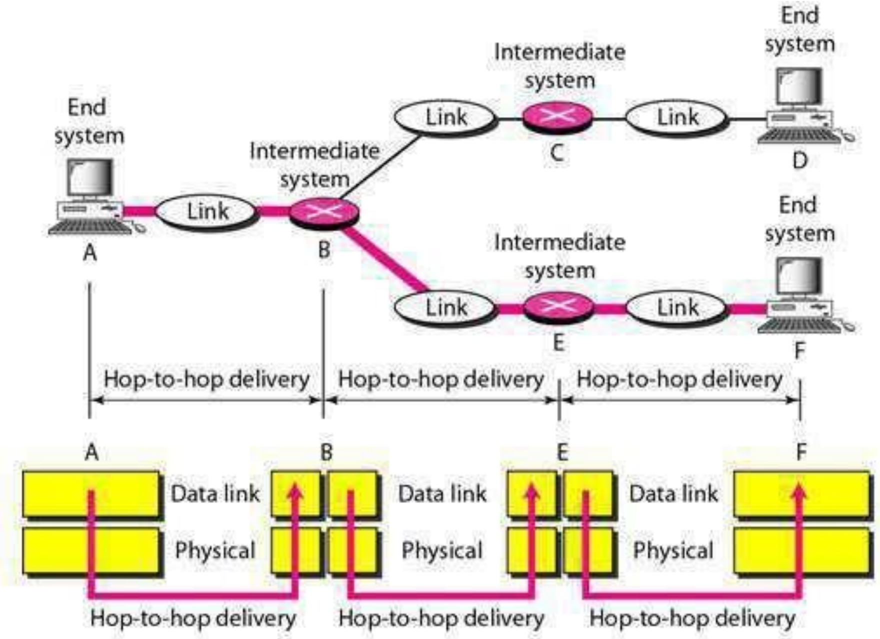


Figure 2.7 *Hop-to-hop delivery*

Network Layer

- Main Responsibility:

  Network-layer (NL) is responsible for source-to-destination delivery of a packet, possibly across multiple-networks.

- Data-link-layer vs. Network-layer:

  1) The data-link-layer ensures the delivery of the packet between 2 systems on the same link.

  2) The network-layer ensures that each packet gets from the source to the final destination.

- If 2 systems are connected to the same link, there is no need for a network-layer.

  However, if the 2 systems are attached to different links, there is often a need for the networklayer to accomplish source-to-destination delivery.

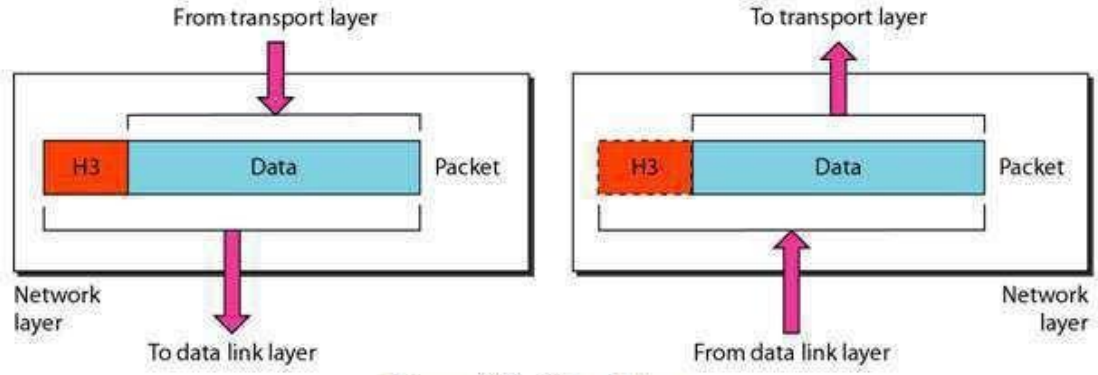


Figure 2.8 *Network layer*

- Other responsibilities of network-layer (Figure 2.8 & 2.9):

  1) Logical Addressing

  ▫ NL appends a header to the packet coming from the transport-layer. ▫ The header contains the IP addresses of the sender and receiver. ▫ An IP address is a universally unique address in the network.

  ▫ NL uses IP address to recognize devices on the network.

  2) Routing

  ▫ NL provides routing of packets.

  ▫ Routing is the process of finding the best path from a source to a destination. ▫ Routers/gateways are used for routing the packets to their final destination. ▫ NL is concerned with circuit, message or packet switching.

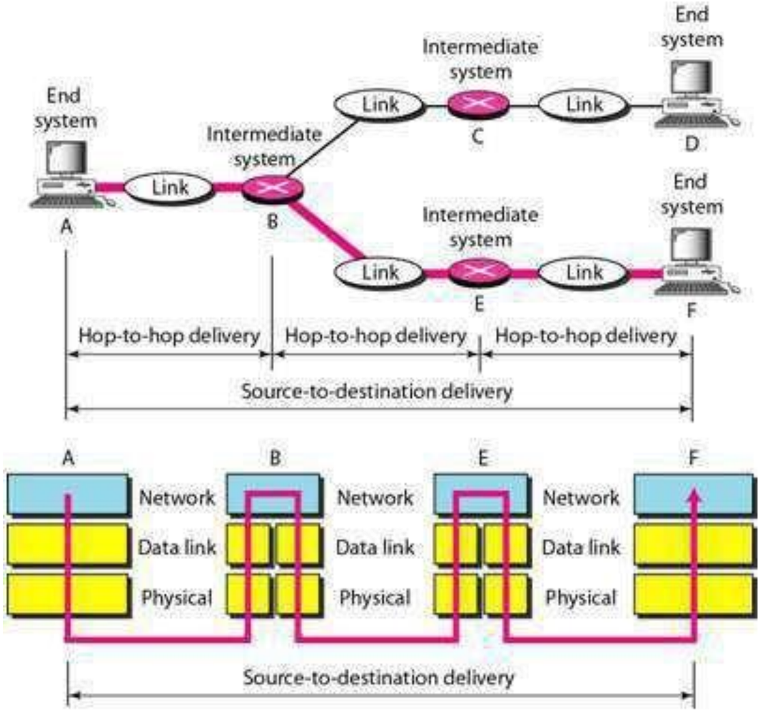


Figure 2.9 *Source-to-destination delivery*

Transport Layer

- Main Responsibility:

  Transport-layer (TL) is responsible for process-to-process delivery of the entire message.
- Process-to-process delivery means delivery from a specific process on one computer to a specific process on the other computer.
- A process is an application program running on a host.
- Network-layer vs. Transport-layer:

  1) Network-layer ensures source-to-destination delivery of individual packets.

  2) Transport-layer ensures that the whole message arrives in order

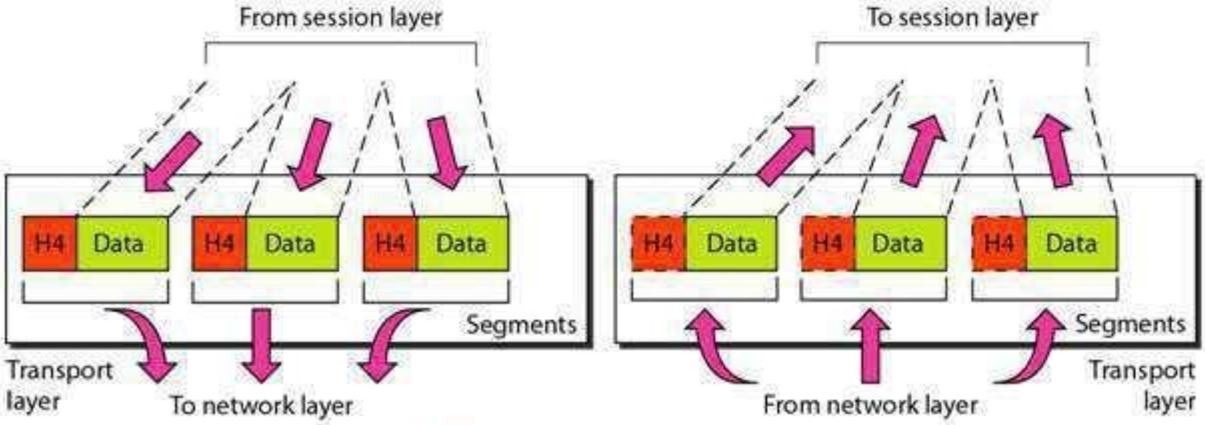


Figure 2.10 *Transport layer*

- Other responsibilities of transport-layer (Figure 2.10 & 2.11):

  1) Service Point Addressing

  ▫ NL appends a header to the segments coming from the network-layer. ▫
  Header contains the port-address of the sender and receiver.

  ▫ Network-layer vs. Transport-layer:

  i) The network-layer gets each packet to the correct computer.

  ii) The transport-layer gets the entire message to the correct process on that computer.

  2) Segmentation & Reassembly

  ▫ A message is divided into segments.

  ▫ Each segment contains a sequence-number.

  ▫ At receiver, the sequence-numbers are used to

  → rearrange the segments in proper order

  → identify lost/duplicate segments

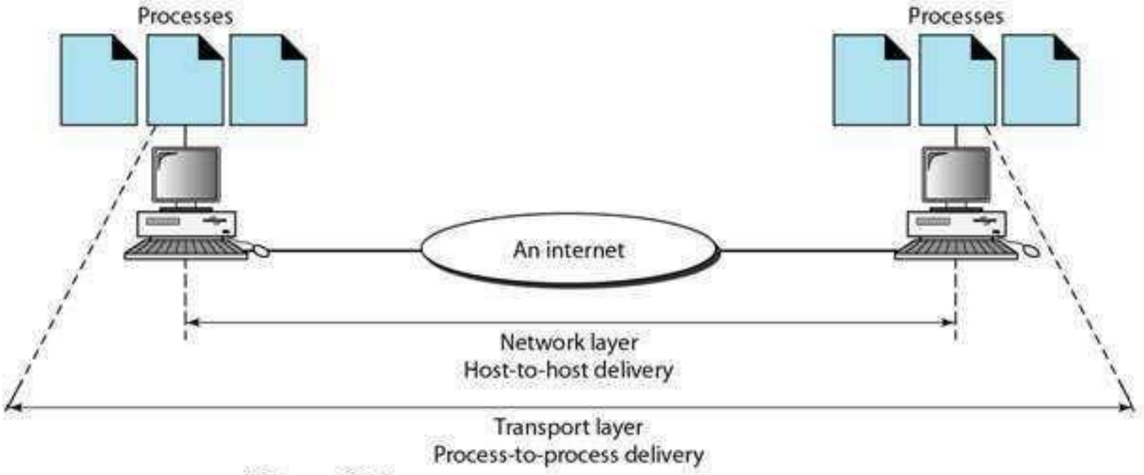


Figure 2.11 *Reliable process-to-process delivery ofa message*

3) Connection Control

▫ TL can be either i) connectionless or ii) connection-oriented.

i) In connectionless, TL

→ treats each segment as an independent packet and

→ delivers the segment to the transport-layer at the destination-machine. ii) In connection-oriented, TL

→ first, makes a connection with the destination-machine.

→ then, delivers the packets to the destination-machine.

4) Flow Control & Error Control

▫ Like DLL, TL is responsible for flow-control & error-control.

However, flow-control & error-control are performed end-to-end rather than node-to-node.

Session Layer

• Main Responsibility:

Session-layer (SL) establishes, maintains, and synchronizes the interaction between 2 systems.

• Other responsibilities of session-layer (Figure 2.12):

1) Dialog Control

▫ SL allows 2 systems to start communication with each other in half-duplex or full-duplex.

2) Synchronization

▫ SL allows a process to add checkpoints into stream of data.

▫ The checkpoint is a way of informing the status of the data transfer. ▫ For example:

A checkpoint after first 500 bits of data will ensure that those 500 bits are not sent again in case of retransmission at 650th bit. (Checkpoints ▫ Synchronization Points)

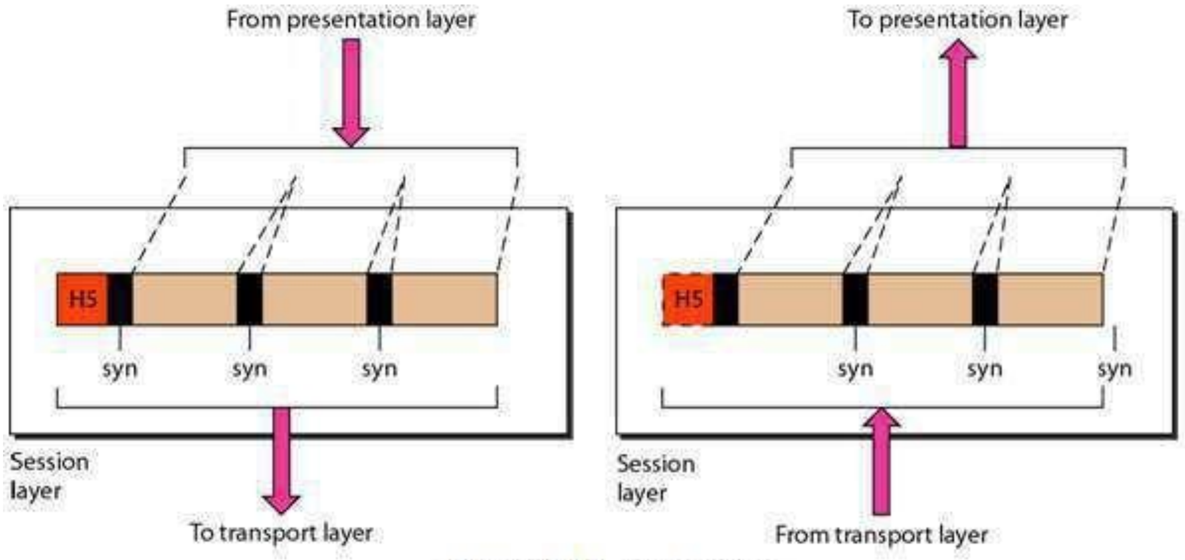


Figure 2.12 *Session layer*

Presentation Layer

• Main Responsibility:

Presentation-layer (PL) is concerned with syntax & semantics of the info. exchanged b/w 2 systems.

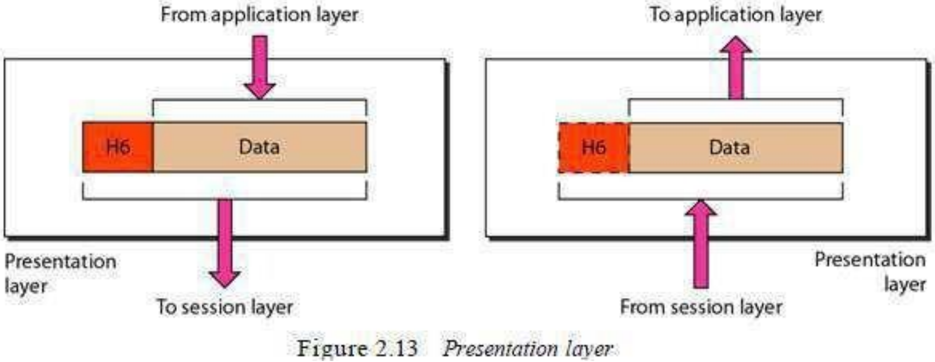


Figure 2.13 *Presentation layer*

• Other responsibilities of presentation-layer (Figure 2.13):

1) Translation

▫ PL translates data between

→ format the network requires and

→ format the computer understands.

▫ PL is responsible for interoperability between encoding methods as different computers use different encoding-methods.

2) Encryption

▫ PL performs

→ encryption at the sender and

→ decryption at the receiver.

▫ Encryption means the sender transforms the original information to another.

▫ Decryption means the receiver transforms the encrypted-message back to its original form.

3) Compression

▫ PL carries out data compression to reduce the size of the data to be transmitted. ▫ Data compression reduces the number of bits contained in the information.

▫ Data compression ensures faster data transfer.

▫ Data compression is important in transmitting multimedia such as audio, video, etc.

Application Layer

• Main Responsibility: The application-layer (AL)

→ provides services to the user

→ enables the user to access the network.

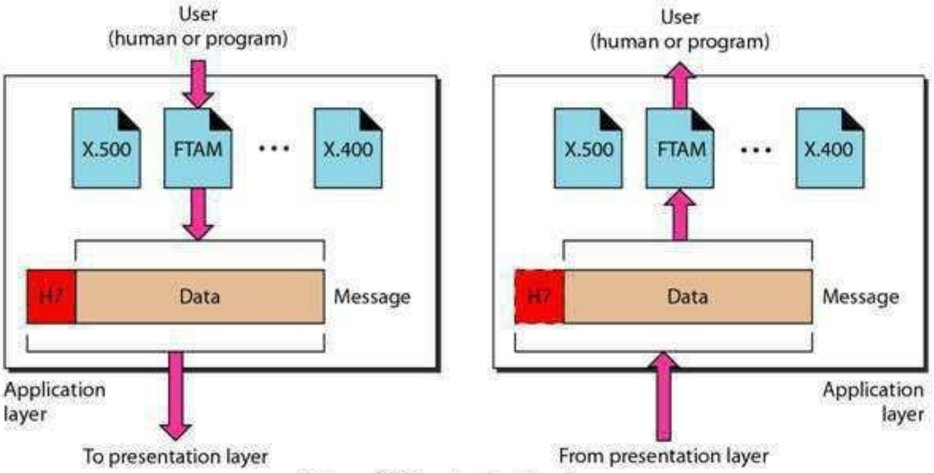


Figure 2.14 *Application layer*

• Other responsibilities of application-layer (Figure 2.14):

1) Mail Services

2) Directory Services

3) File Transfer, Access, and Management