Advanced Computer Networks

Module-1

Module-1:

Overview of Computer Networks and the Internet:

- Overview of Computer Networks and the Internet. History.
- Protocols, Packet switching.
- Basic ideas about delay queuing throughput.
- Concept of Quality of Service, Protocol layering .
- OSI model and TCP model.
- Application layer protocols - Client-server architecture.
- Network layer 7 application architecture, Web, HTTP, FTP, SMTP, POP3, and DNS, Peer-to-peer file sharing networks.

Networks

- A network is the interconnection of a set of devices capable of communication.

Device:

- A device can be a host such as a large computer, desktop, laptop, workstation, cellular phone, or security system.
- A device can also be a connecting device such as a router a switch, a modem that changes the form of data, and so on.

Networks (cntd..)

- Local Area Networks
- Wide Area Networks
  - Point-to-Point WANs
  - Switched WANs
- Internetwork

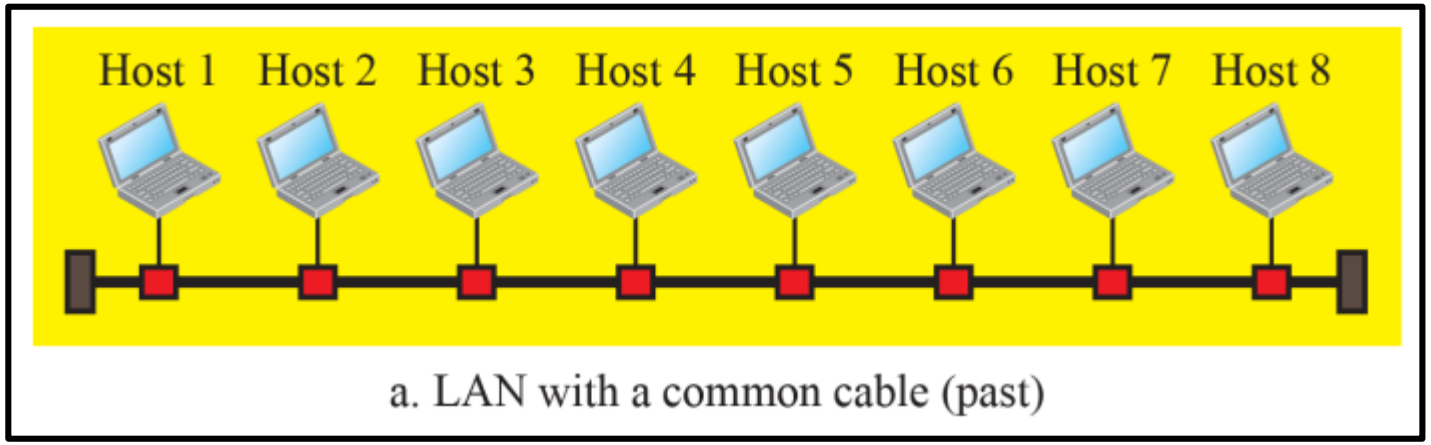
Personal Area Networks

- A personal area network (PAN) is a computer network that connects electronic devices within an individual person's workspace.
- It allows for data transmission among devices such as computers, smartphones, tablets, and personal digital assistants.
- PANs are typically wireless and have a range of approximately 10 meters or 33 feet.
- One popular technology used for PAN communication is Bluetooth.
- Other technologies such as Wi-Fi and Near Field Communication (NFC) can also be used for PAN communication.

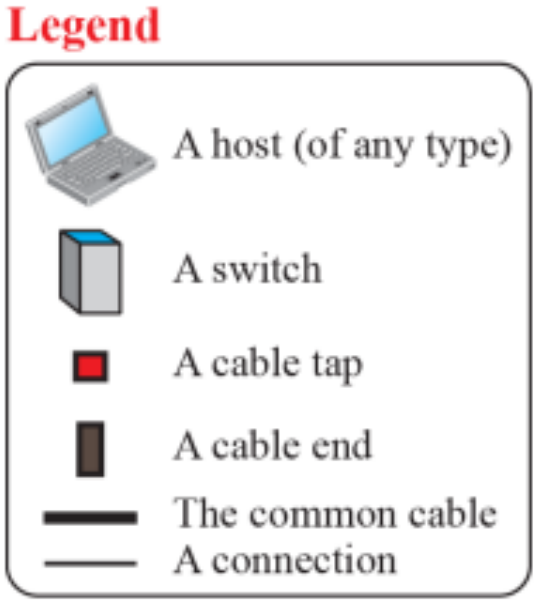
Local Area Network(LAN)

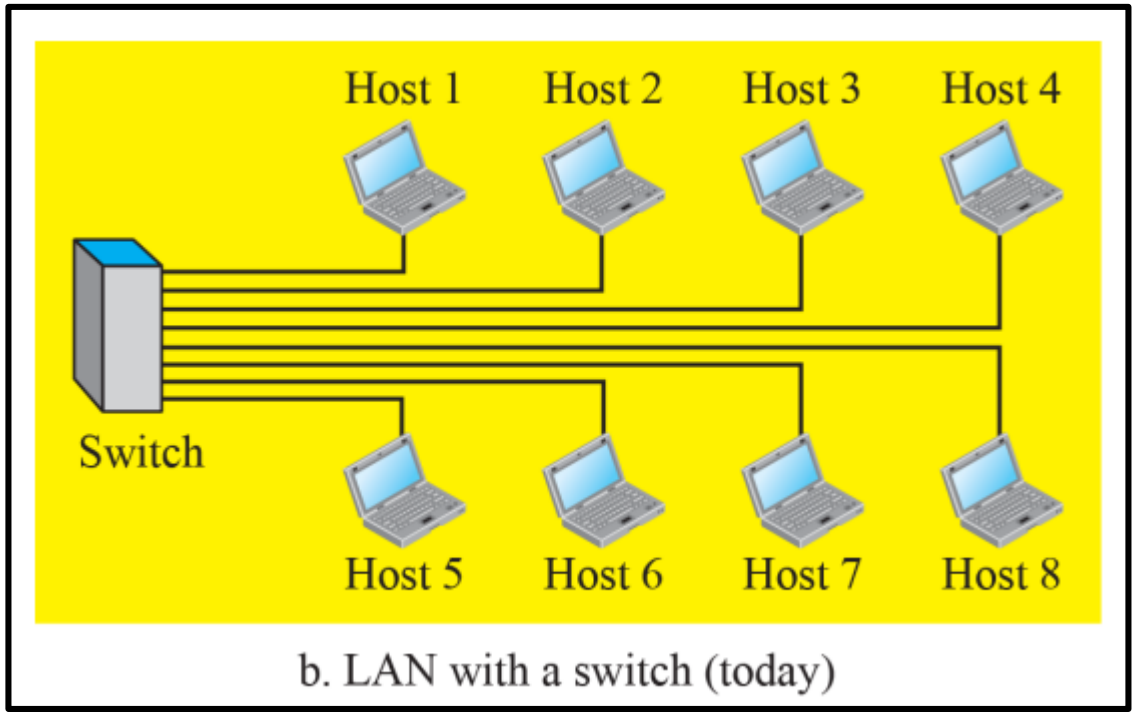
- LAN is usually privately owned and connects some hosts in a single office, building, or campus.
- A LAN can be as simple as two PCs and a printer in someone's home office, or it can extend throughout a company and include audio and video devices.
- Each host in a LAN has an identifier, an address, that uniquely defines the host in the LAN.
- The most common type of LAN is Ethernet LAN, which use Ethernet cables.
- WLAN is Wireless LAN, that uses wireless communication instead of wired communication.
- WLAN has Wi-Fi routers or Wireless access points.

Figure : An Isolated LAN in the past and today



a. LAN with a common cable (past)





b. LAN with a switch (today)

Wide Area Network

- A WAN has a wider geographical span, spanning a town, a state, a country, or even the world.
- A LAN interconnects hosts; a WAN interconnects connecting devices such as switches, routers, or modems.
- A LAN is normally privately owned by the organization that uses it;
- a WAN is normally created and run by communication companies and leased by an organization that uses it.
- A good example of WAN is the Internet
- Two distinct examples of WANs:
  1. point-to-point WANs
  2. switched WANs

Figure: A Point-to-Point WAN

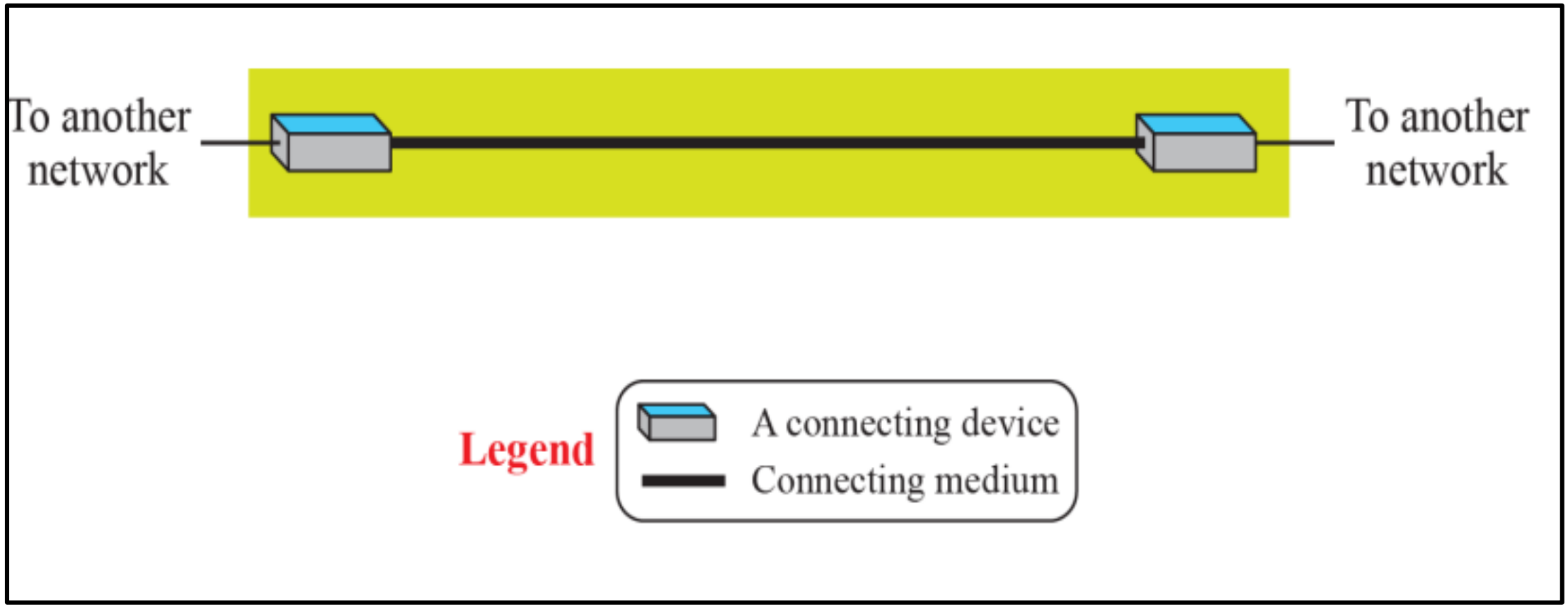
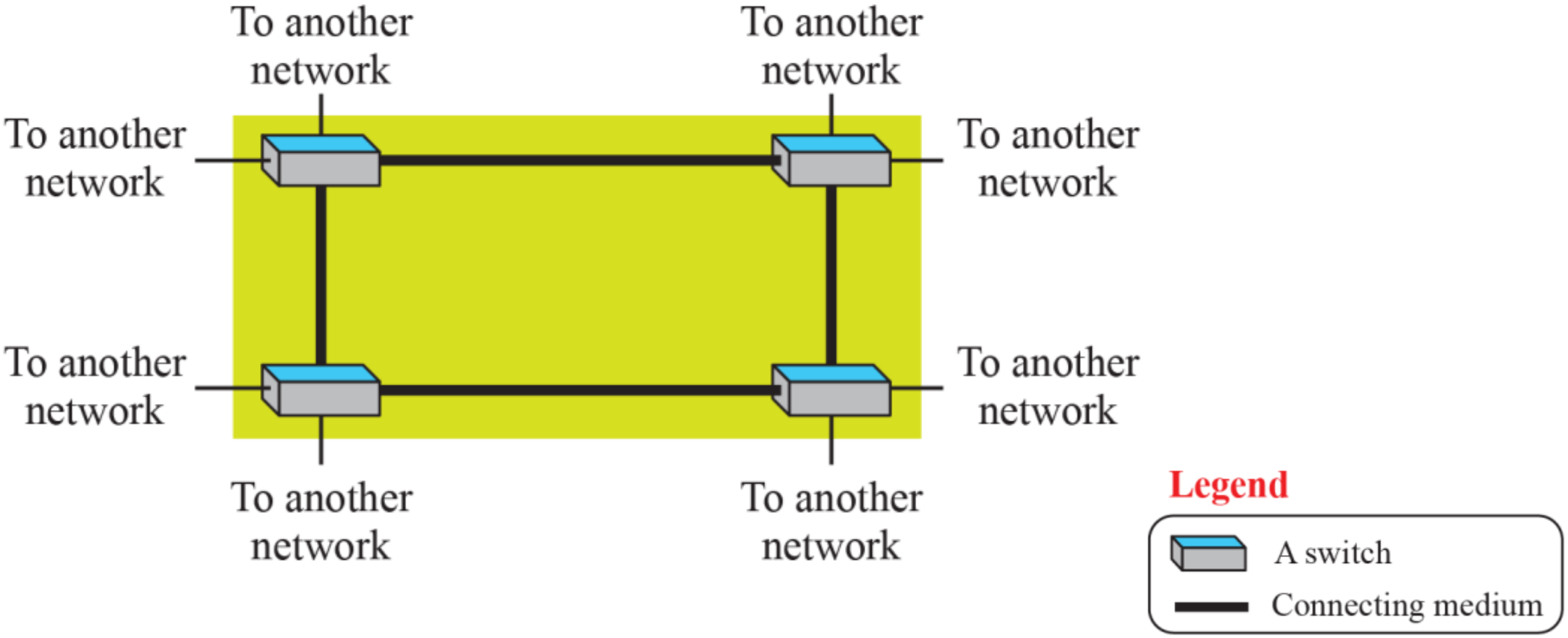


Figure: A Switched WAN



Internetwork

- Internetworking refers to the practice of connecting multiple computer networks together so that they can exchange messages.
- This allows hosts in different networks to communicate with each other, regardless of their networking technology.
- The resulting interconnected system of networks is known as an internetwork or an internet.

Fig: An Internetwork made of two LANs and one WAN.

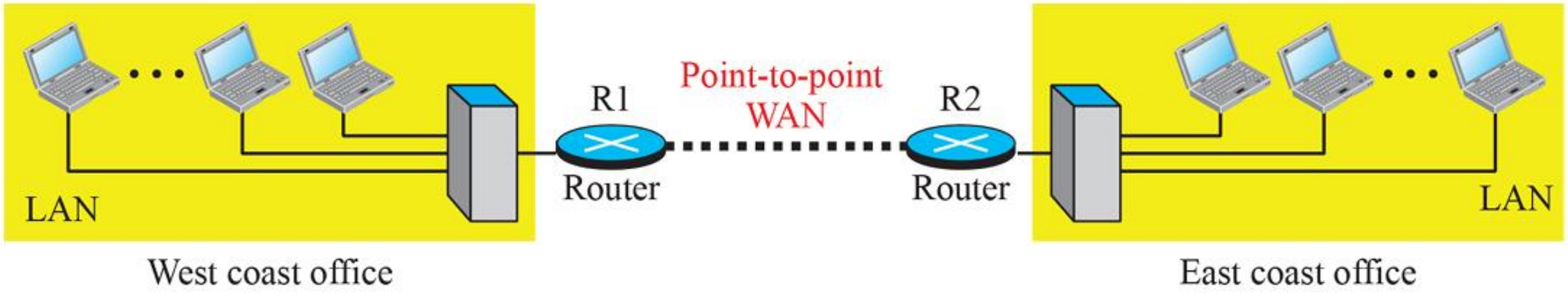
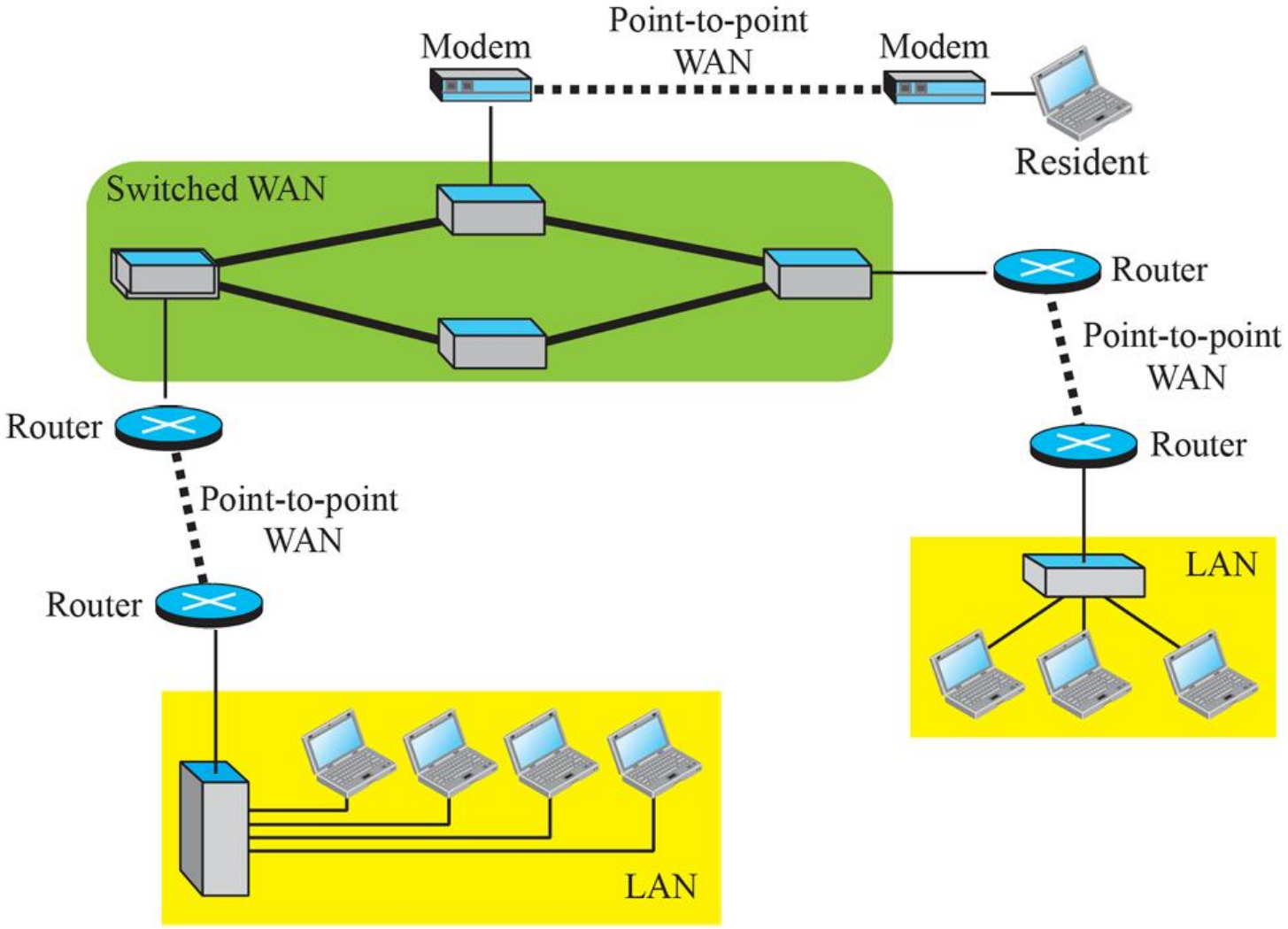


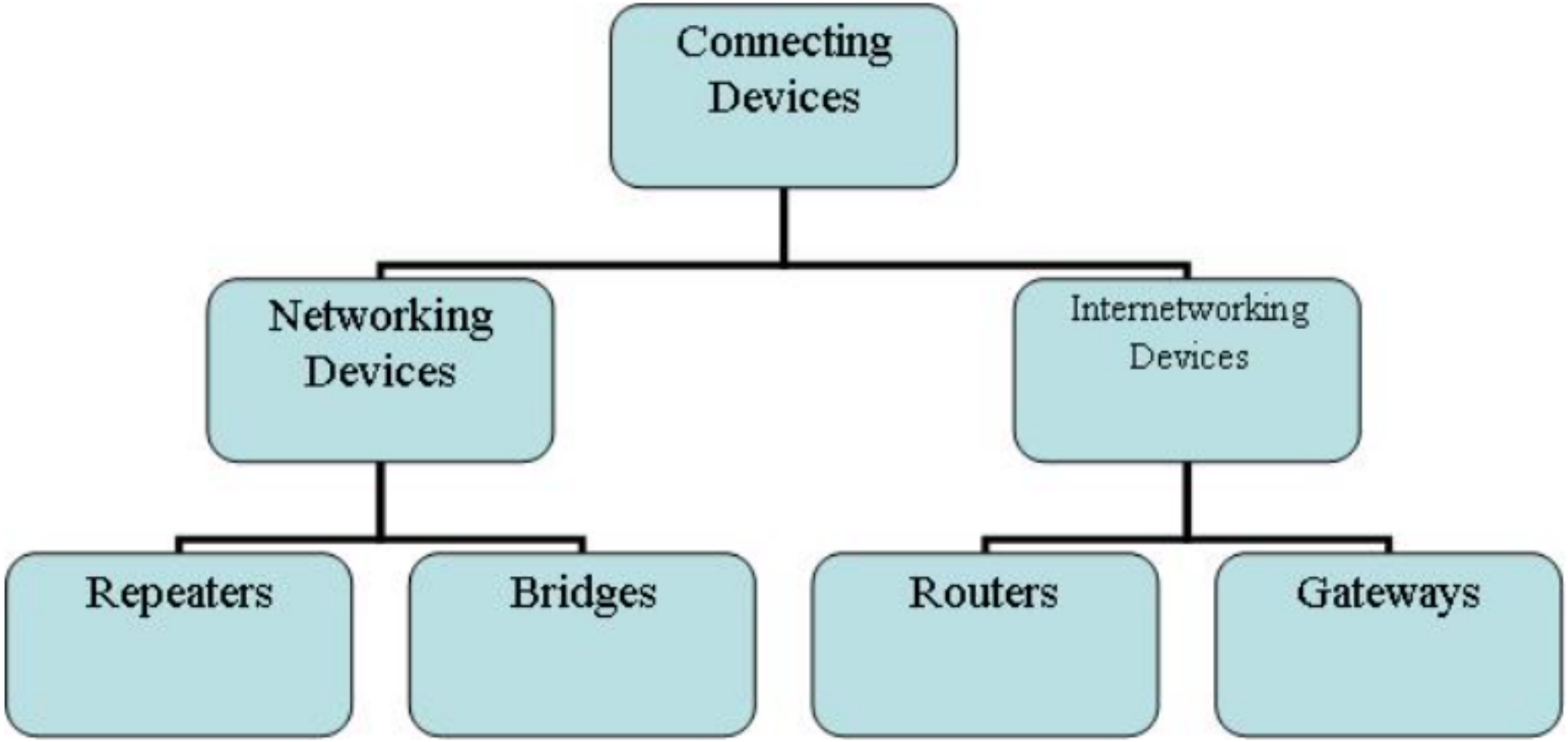
Fig: A heterogeneous network made of WANs and LANs



Metropolitan Area Network (MAN)

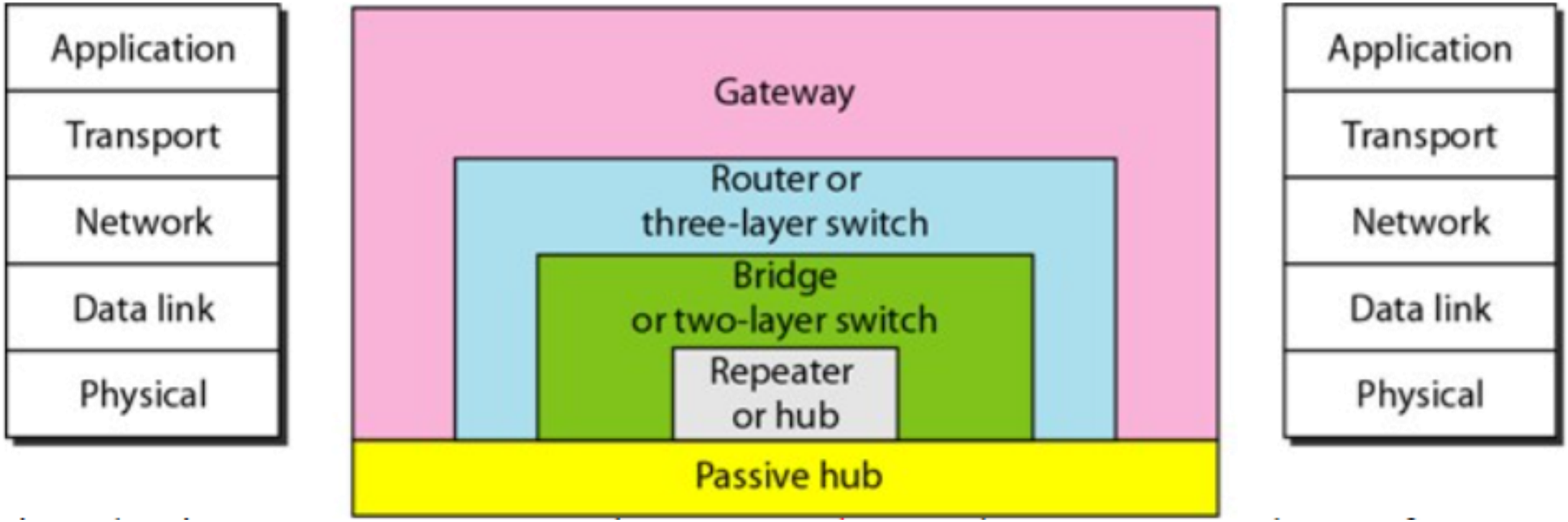
- A metropolitan area network is a network that covers a larger geographic area by interconnecting different LANs to form a larger network.
- It connect several buildings in a city.
- Connected using high speed connection such as Fiber optic cable.
- Eg:- Government agencies use MAN to connect to the citizens and private industries.
- It has a higher range than Local Area Network(LAN)

Networking and Internetworking Devices



Networking and Internetworking Devices

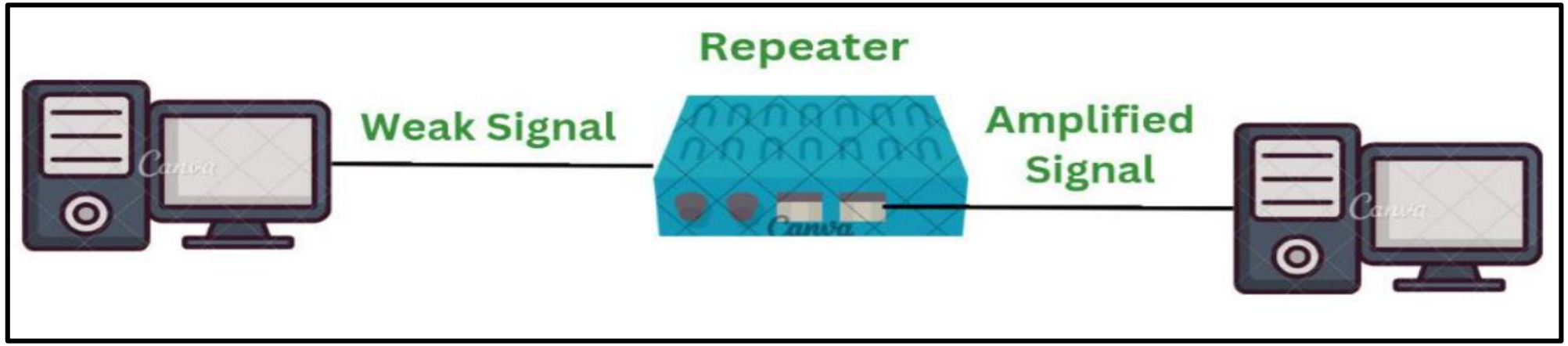
Five Categories of Connecting Devices

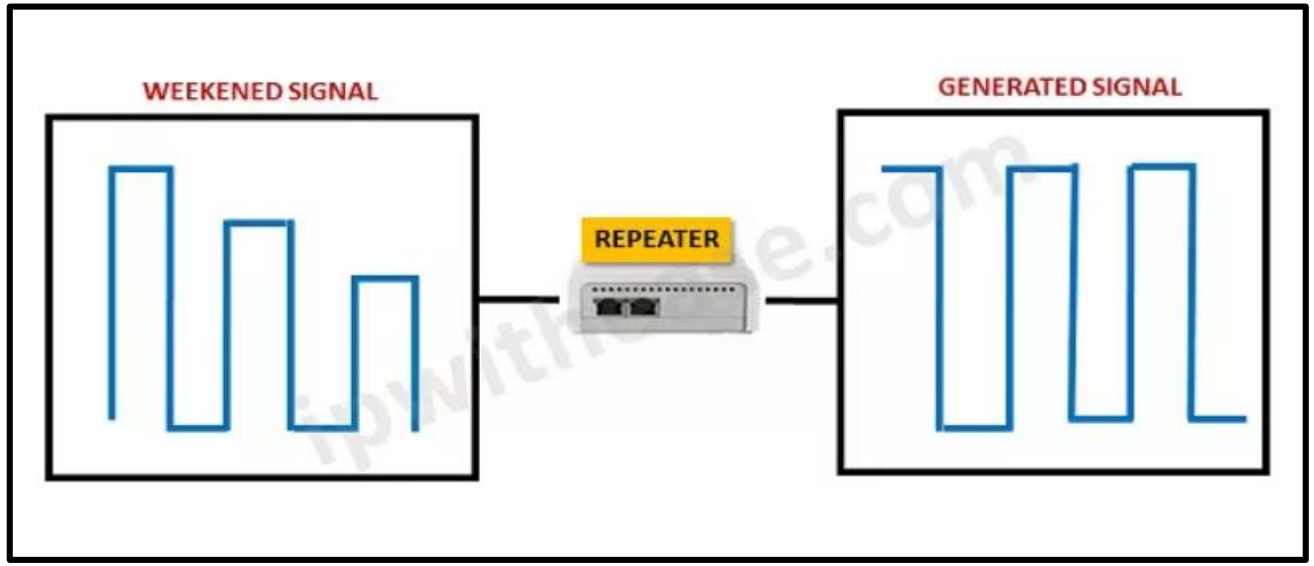


Repeaters

- A networking device that is used to amplify and generate the incoming signal.
- Layer 1 device
- Eg:- Repeaters work at the physical layer of the OSI model.
- The main aim of using a repeater is to increase the networking distance by increasing the strength and quality of signals.
- Used In Local Area Networks (LANs) and Wide Area Networks (WANs).
- It helps to reduce error, and loss of data and provides with delivery of data at specified locations only.
- It transfer data with more security and over a long distance.

Repeaters


Repeater
Weak Signal
Amplified Signal

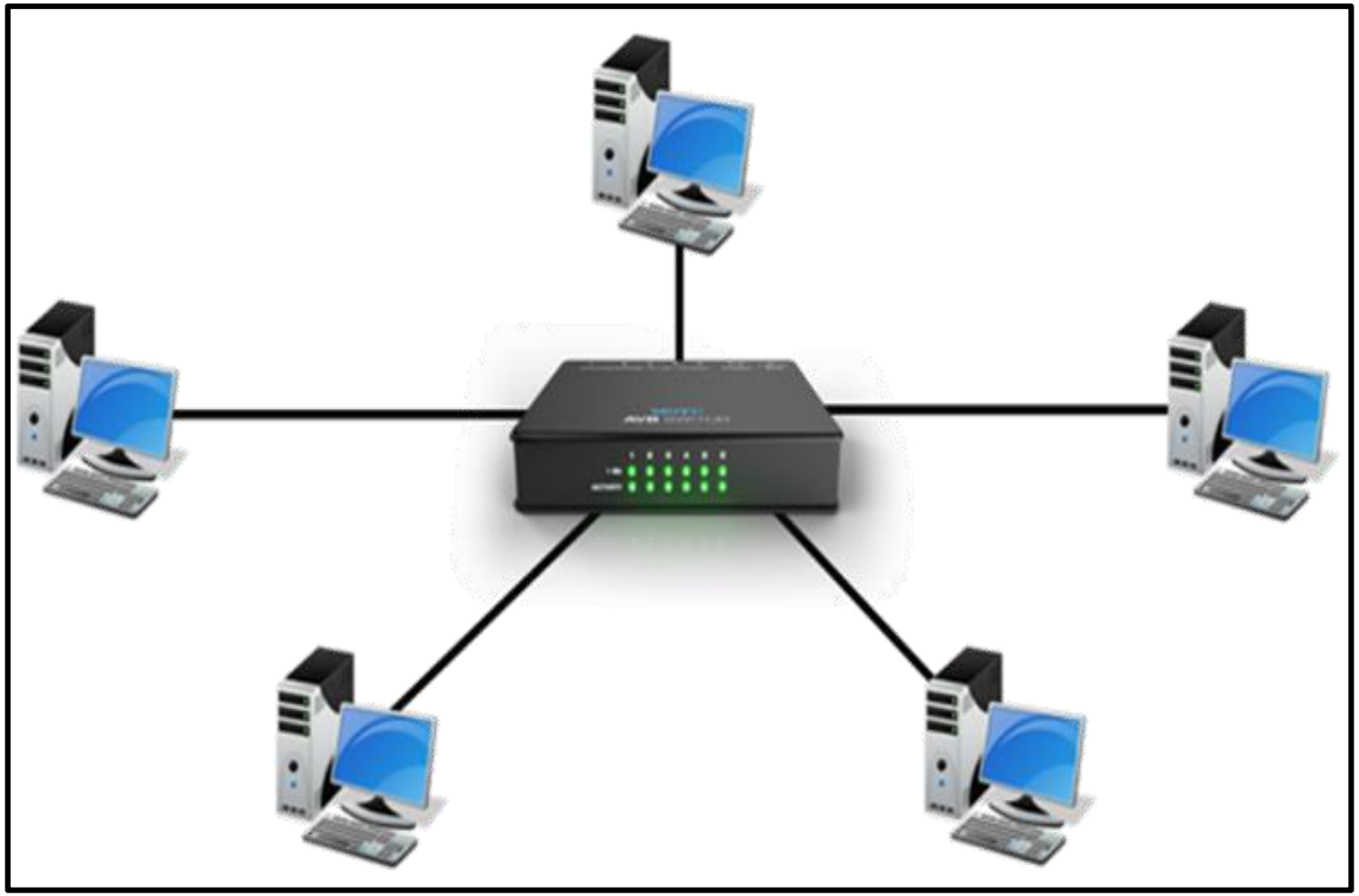

WEEKENED SIGNAL
REPEATER
GENERATED SIGNAL


Repeater

Hub(Broadcasting)

- In networking, a hub is a device that links multiple computers and devices together.
- Hubs can also be referred to as Repeaters or Concentrators;
- They serve as the center of a Local Area Network (LAN).
- In a hub, each connected device is on the same subnet and receives all data sent to the hub.

Hub



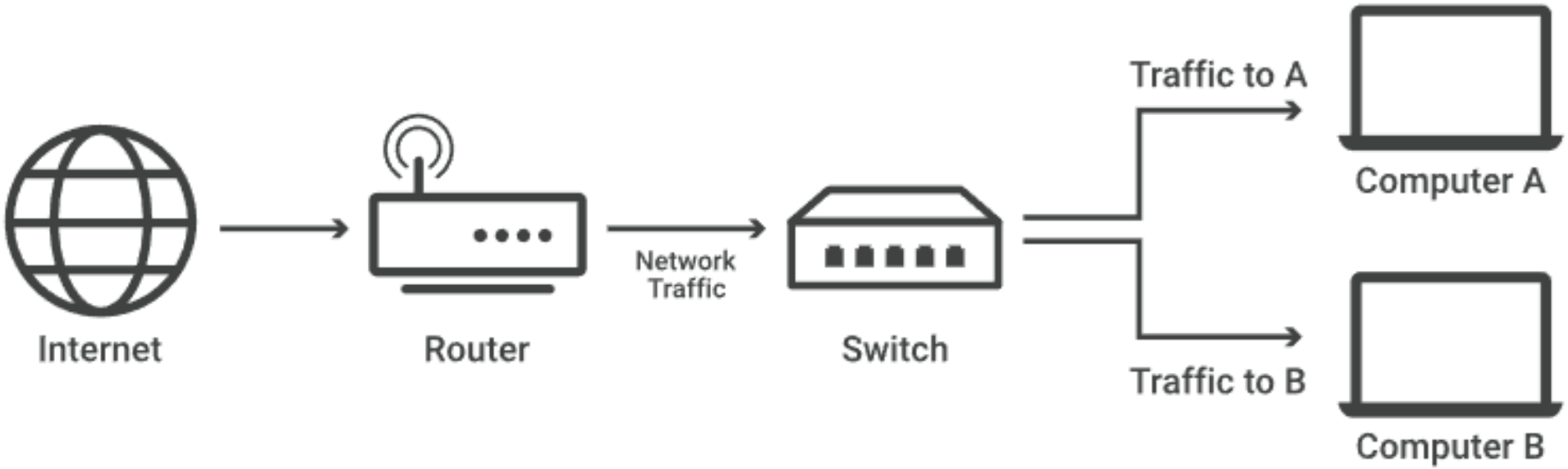
Hub

- Several networks need a central location to connect media segments together. These central locations are called as hubs.
- It is like a distribution center.
- When a computer request information from a network or a specific computer, it sends the request to the hub through a cable.
- The hub will receive the request and transmit it to the entire network.
- Each computer in the network should then figure out whether the broadcast data is for them or not.
- The three types of hubs are:
  i. Passive hub
  ii. Active Hub
  iii. Intelligent Hub

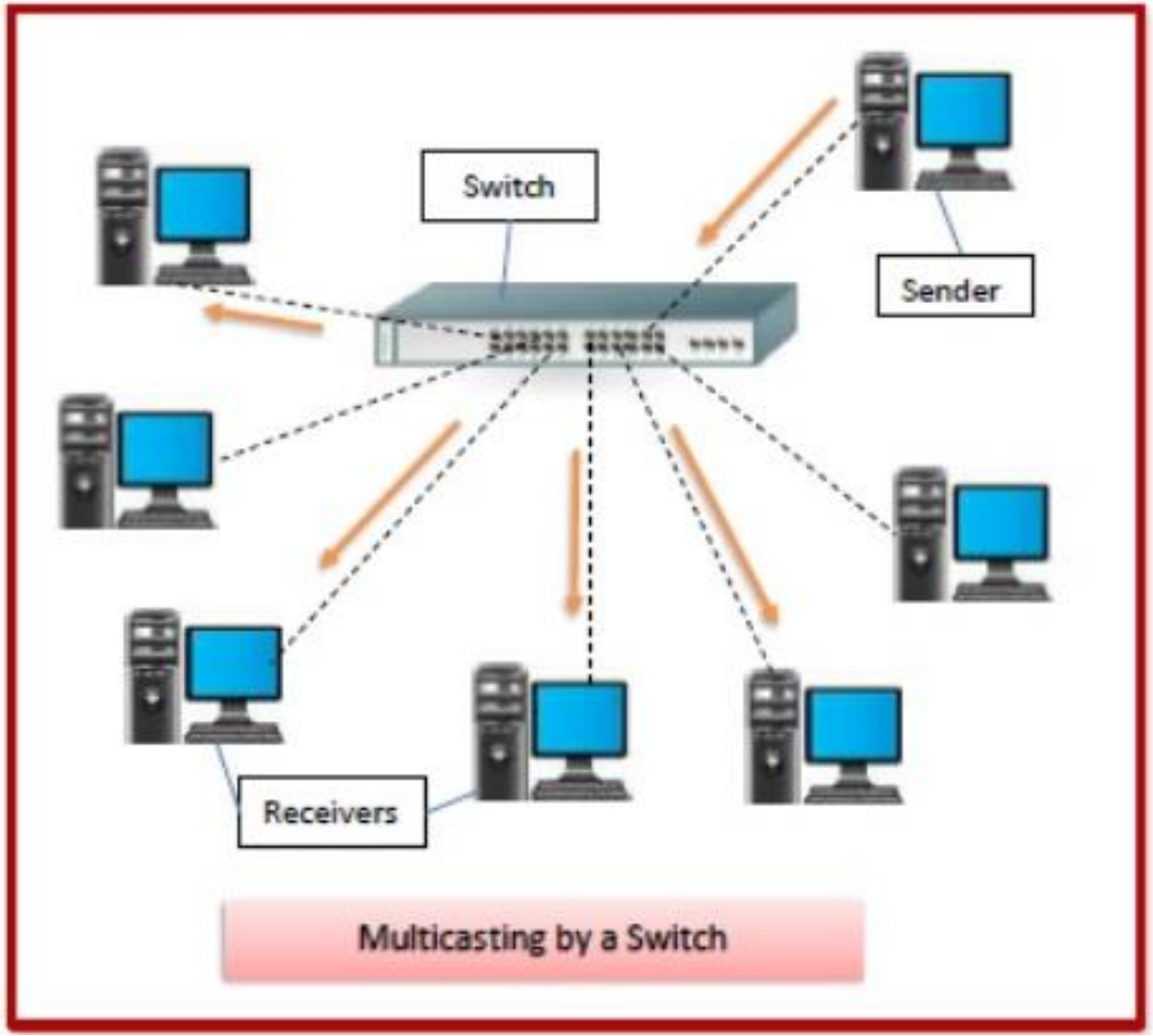
Switch

- It supports transmitting, receiving and controlling of traffic with other computers on the network.
- Switch is used for filtering & forwarding the data. So this is the more clever technique to deal with the data packets.
- Whenever a data packet is obtained from the interfaces in the switch, then the data packet can be filtered & transmits to the interface of the proposed receiver.
- It allows one-to-one (unicast), one-to-many (multicast), and one-to-all (broadcast) communications.
- Full duplex transmission means that communication in the channel happens in both directions at once. As a result, collisions do not happen.
- Switches are operational hardware that has network management and software capabilities.
- Switches have the ability to carry out some error checking before sending data to the target port.

Switch


Internet
Router
Network Traffic
Switch
Traffic to A
Traffic to B
Computer A
Computer B

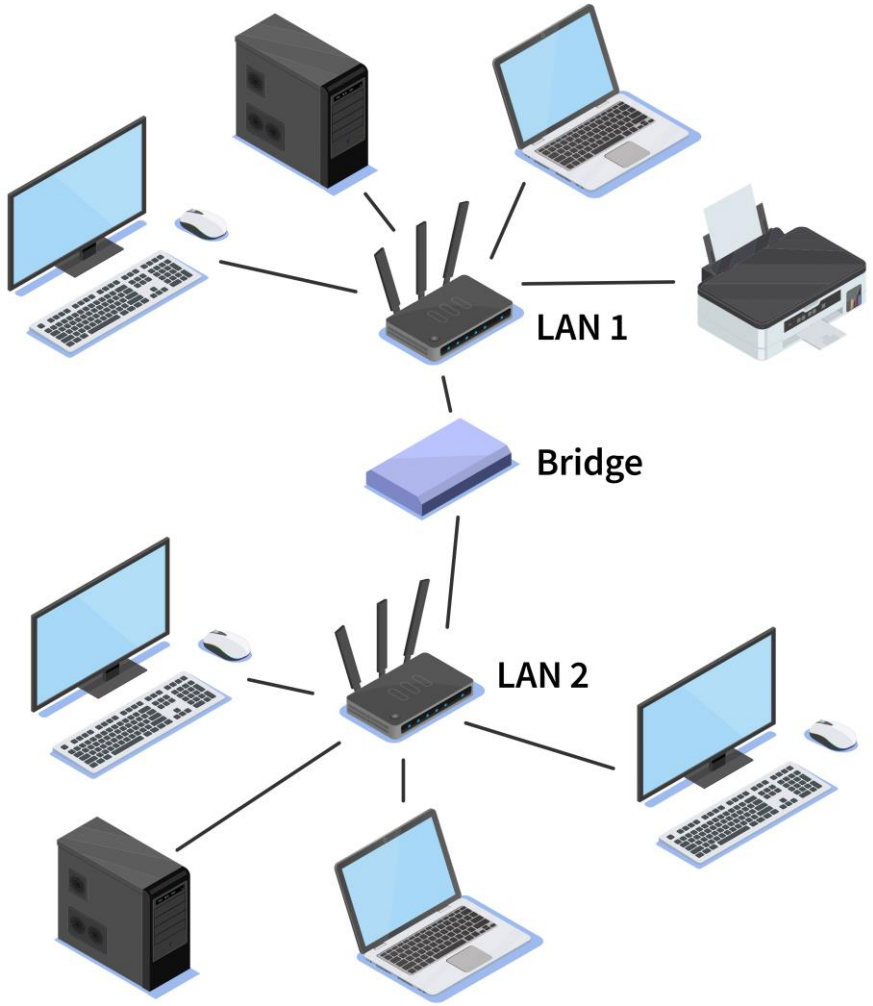
Switch



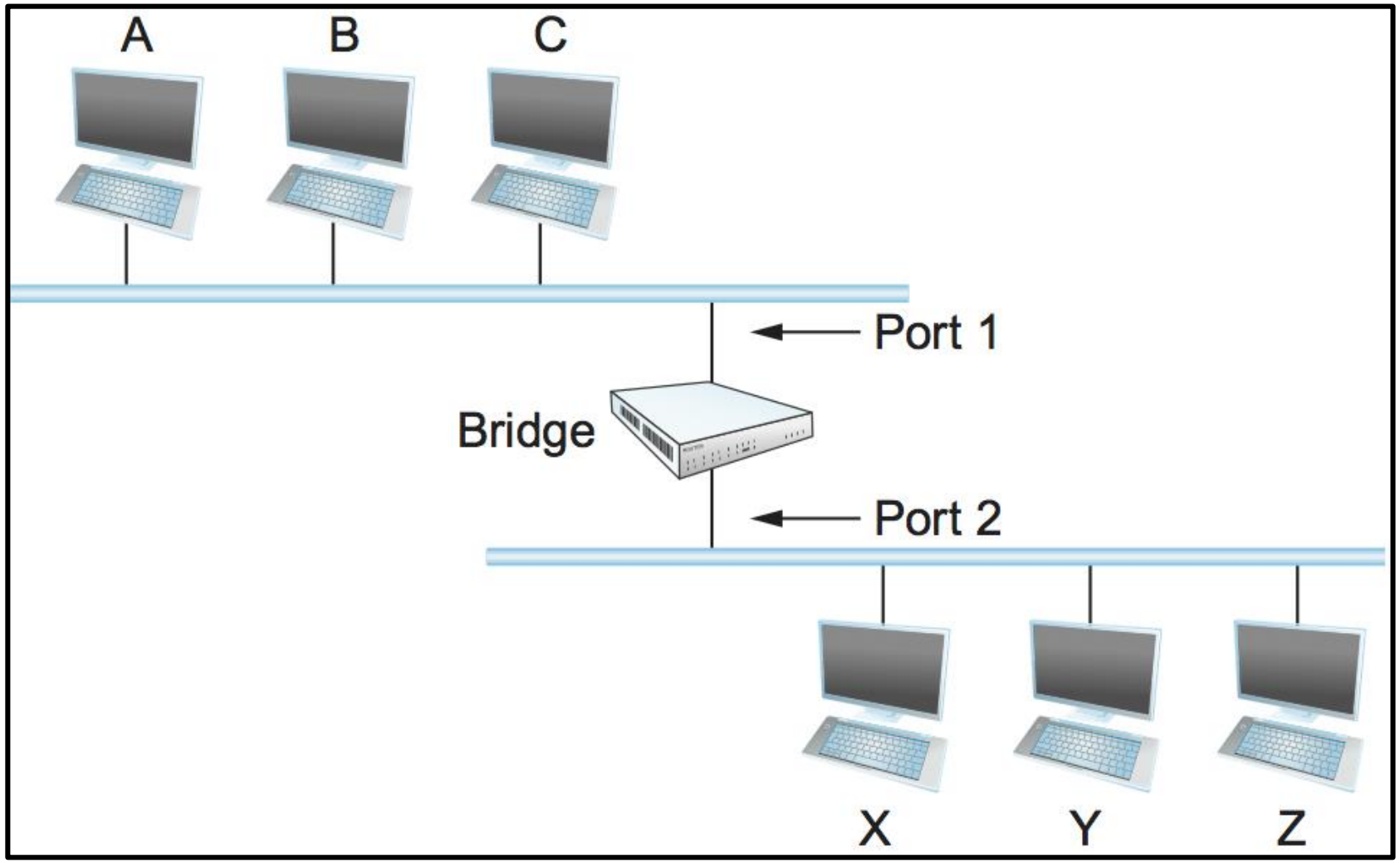
Bridges

- In a network, different LANs can be connected to form a larger LAN.
- This form of aggregating networks is called as network bridging.
- The bridge connects different LANs(with same protocols) so that they appear as a part of single network.
- A network bridge acts to divide a network into such logical segments that the collision between the data packets being sent over the network is reduced.
- The bridge is a networking device in a computer network that is used to connect multiple LANs to a larger LAN.

Bridges



Bridges



Router

- The router connects the different network segments.
- A router is a device that connects two or more packet-switched networks or subnetworks.
- Routers operate at the Layer 3 (network layer) of OSI Model.
- *Two primary functions:*
  i. Managing traffic between the networks by forwarding data packets to their intended IP addresses, and
  ii. Allowing multiple devices to use the same Internet connection.
- To forward a data packet to its destination, router keeps the records of connected networks.
- These records are maintained in a database table known as the Routing table.

Router

- It is also known as an Intelligent Device as it can calculate the best route to pass the network packets from source to the destination automatically.
- More capable as compared to other network devices, such as a hub, switch, etc., as these devices are only able to execute the basic functions of the network.

Working of Routers:

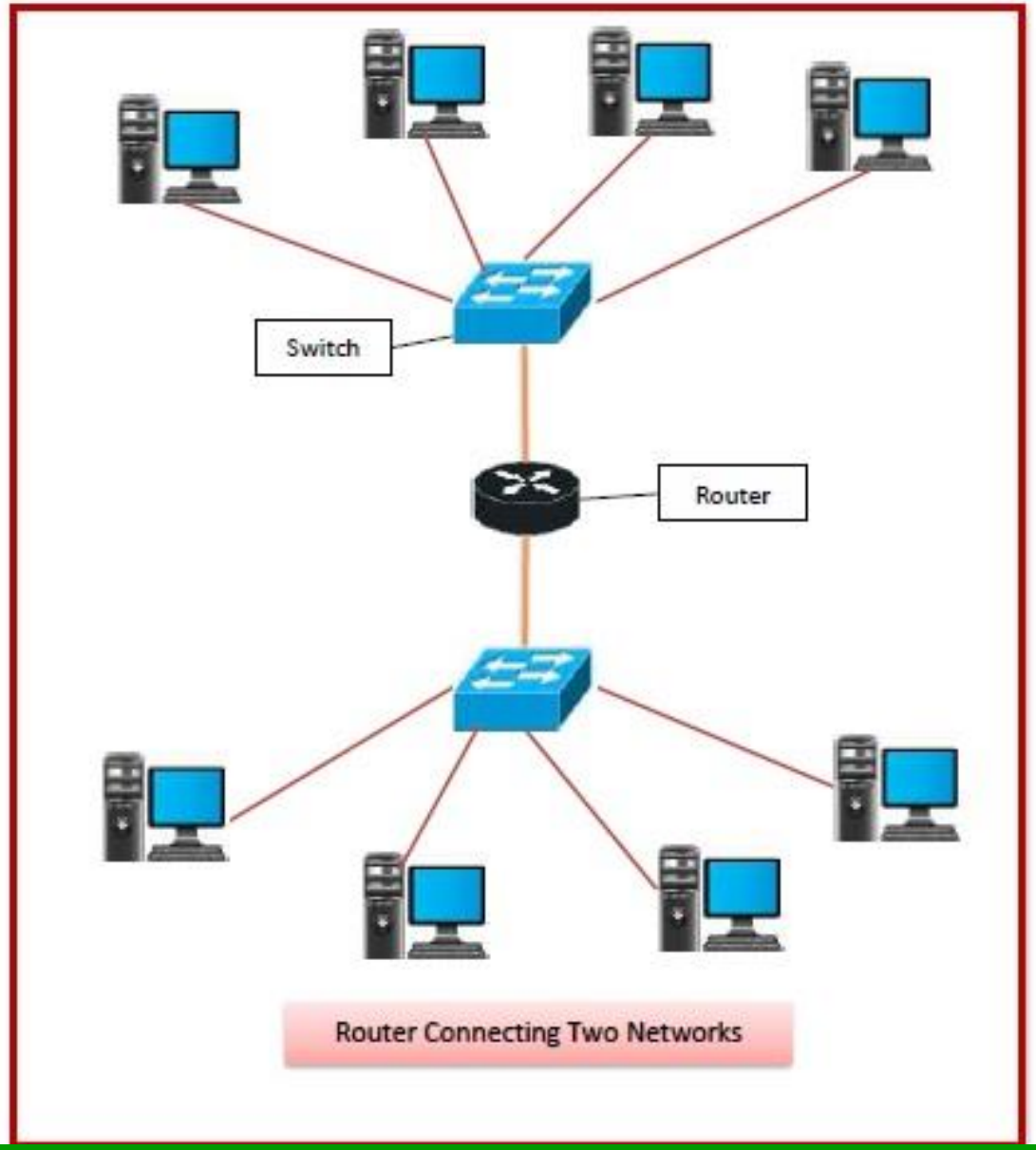
- A router examines the destination IP address of a given data packet, and it uses the headers and forwarding tables(Routing Tables) to decide the best way to transfer the packets.
- There are some popular companies that develop routers;
  - Cisco, 3Com, HP, Juniper, D-Link, Nortel, etc.

Router

Switch Vs Router:

- ✓A network switch forwards data packets between groups of devices in the same network, whereas a router forwards data between different networks.

Router



Router

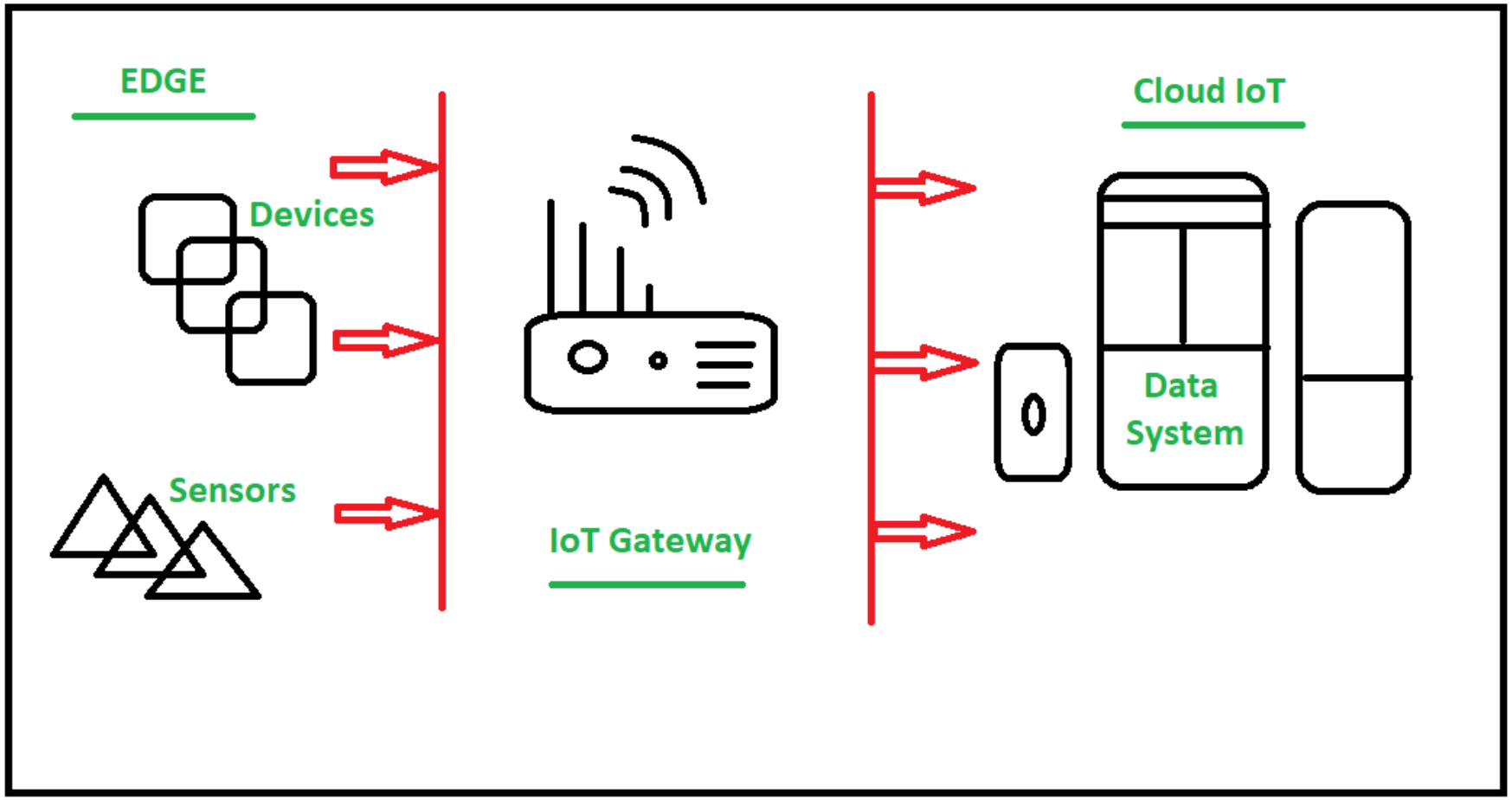
Gateways

- Gateway is a network device used to connect two or more dissimilar networks.
- A gateway is a network node that forms a passage between two networks operating with different transmission protocols.
- Networks that use different protocols are Dissimilar Networks.
- The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model.

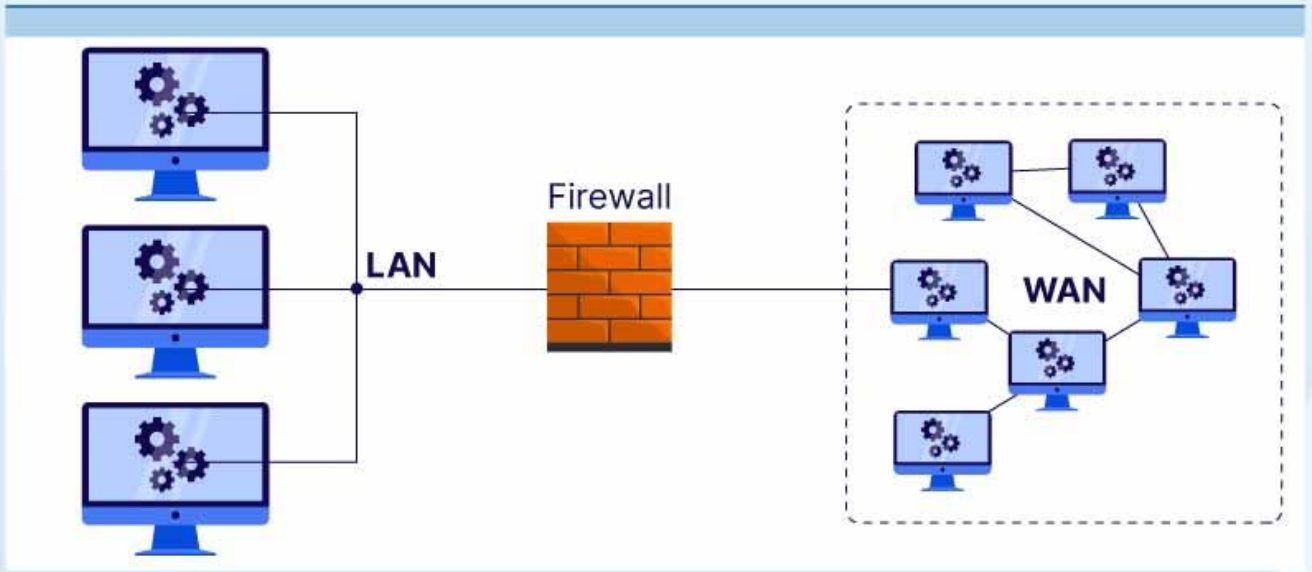
Gateways

- In a network, a Gateway is a translator between two systems that use different communication protocols, data formats or architectures.
- Thus, they serve a Transitional Task.
- They help in the conversion of one type of protocol into another.
- A gateway could be used for both, LAN and WAN interconnections.

Gateways



What is a Gateway in Networking?



NETWORK CARD

- A computer hardware component that connects a computer to a computer network.
- Network card is a necessary component of a computer without which a computer cannot be connected over a network.
- It is also known as Network Adapter or Network Interface Card (NIC).
- Most branded computers have network card pre-installed.
- Two types :
  i. Internal Network Cards.
  ii. External Network Cards.

1. Internal Network Cards:

- **Motherboard has a slot** for internal network card where it is to be **inserted.**
- Internal network cards are of two types:
  i. First type uses **Peripheral Component Interconnect (PCI) connection.**
  ii. Second type uses **Industry Standard Architecture (ISA).**
- **Network cables** are required to provide network access.

2. External Network Cards:

- External network cards come in two flavours :
  i. Wireless &
  ii. USB based.
- Wireless network card need to be inserted into the motherboard but no network cable is required to connect to network.

Unique Identifiers Of Network

- **Unique Network Identifiers:**

1. **IP Address**
2. **DNS Server**
3. **MAC Address**
4. **Port**

Unique Identifiers Of Network:

IP Address:

- IP (Internet Protocol) address is as a unique identifier for each device on the Internet.
- Length of the IP address is 32-bits.
- IPv6 address is 64 bits.

DNS Server:

- DNS → Domain Name System.
- It is a server which translates URL or web addresses into their corresponding IP addresses.

MAC Address:

- MAC (Media Access Control Address) is known as a physical hardware address is a unique identifier of each host and
- It is associated with the NIC (Network Interface Card).
- General length of MAC address is : 48 bits long (6 Bytes), which is equivalent to 12 hexadecimal digits.

Port:

- Port is a logical channel which allows network users to send or receive data to an application.
- Every host can have multiple applications running.
- Each of these applications are identified using the port number on which they are running.

Switching

- Switching is the process of transferring data packets from one device to another in a network, or from one network to another, using specific devices called switches.
- Eg: A computer user experiences switching all the time.
  - For accessing the Internet from your computer device, whenever a user requests a webpage to open, the request is processed through switching of data packets only.
- A Switch is a dedicated piece of computer hardware that facilitates the process of switching.
- i.e., incoming data packets and transferring them to their destination.

Switching(cntd.)

- An Internet is a switched network in which a switch connects at least two links together.
- A switch needs to forward data from a link to another link when required.
- The two most common types of switched networks are:
  1. Circuit-switched Networks.
  2. Packet-switched Networks.

1. Circuit-Switched Network:

- In a 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.
- Eg: Circuit switching was very common in telephone networks in the past, although part of the telephone network today is a packet-switched network.

A Circuit-switched Network:

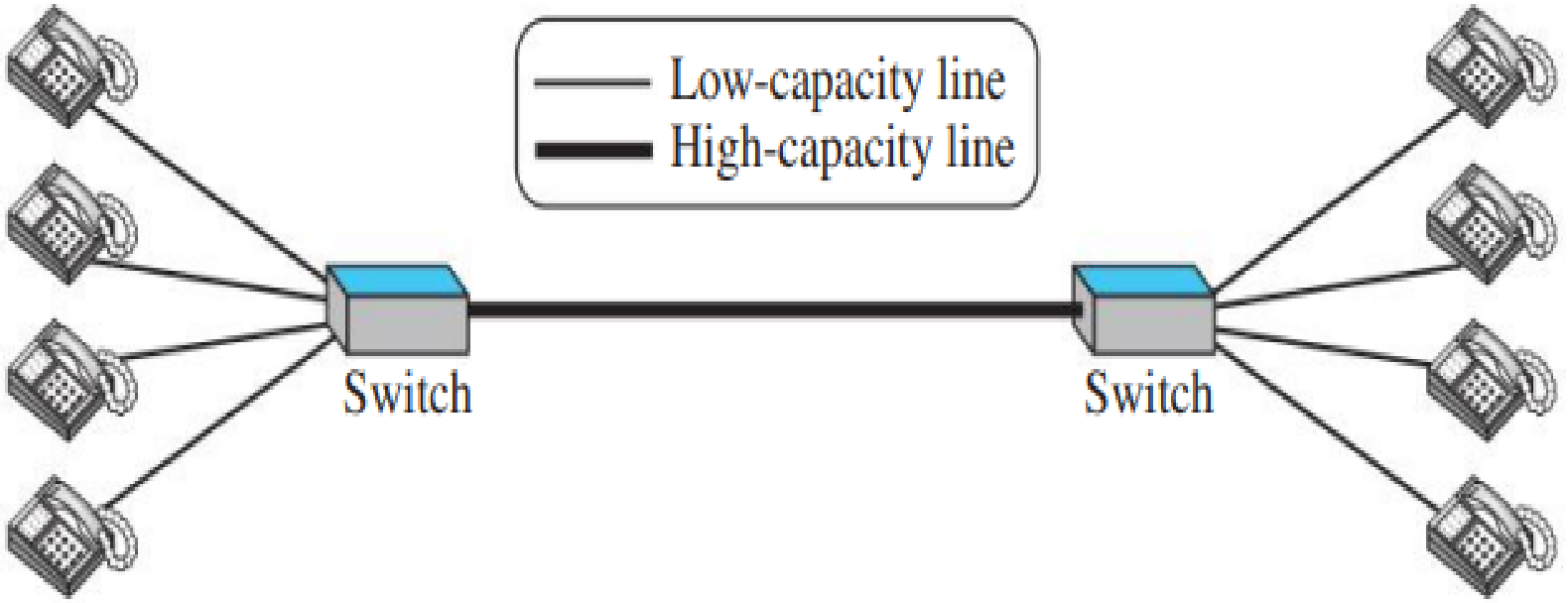


Fig: Four telephones at each side are connected to a switch. The switch connects a telephone set at one side to a telephone set at the other side. The thick line connecting two switches is a high-capacity communication line that can handle four voice communications at the same time; the capacity can be shared between all pairs of telephone sets. The switches used in this example have forwarding tasks but no storing capability.

Drawbacks:

- **Circuit switching is not very efficient for small messages and the analogue circuits make the data subject to noise and errors.**

2. Packet-Switched Network:

- In a computer network, the communication between the two ends is done in blocks of data called packets.
- In other words, instead of the continuous communication we see between two telephone sets when they are being used, we see the exchange of individual data packets between the two computers.
- This allows us to make the switches function for both storing and forwarding because a packet is an independent entity that can be stored and sent later.
- One of the biggest examples of the Packet-switched network is the Internet.

Packet-switched Network (cntd.):

- The message splits into smaller pieces known as packets.
- The packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.

2. Packet-Switched Network:

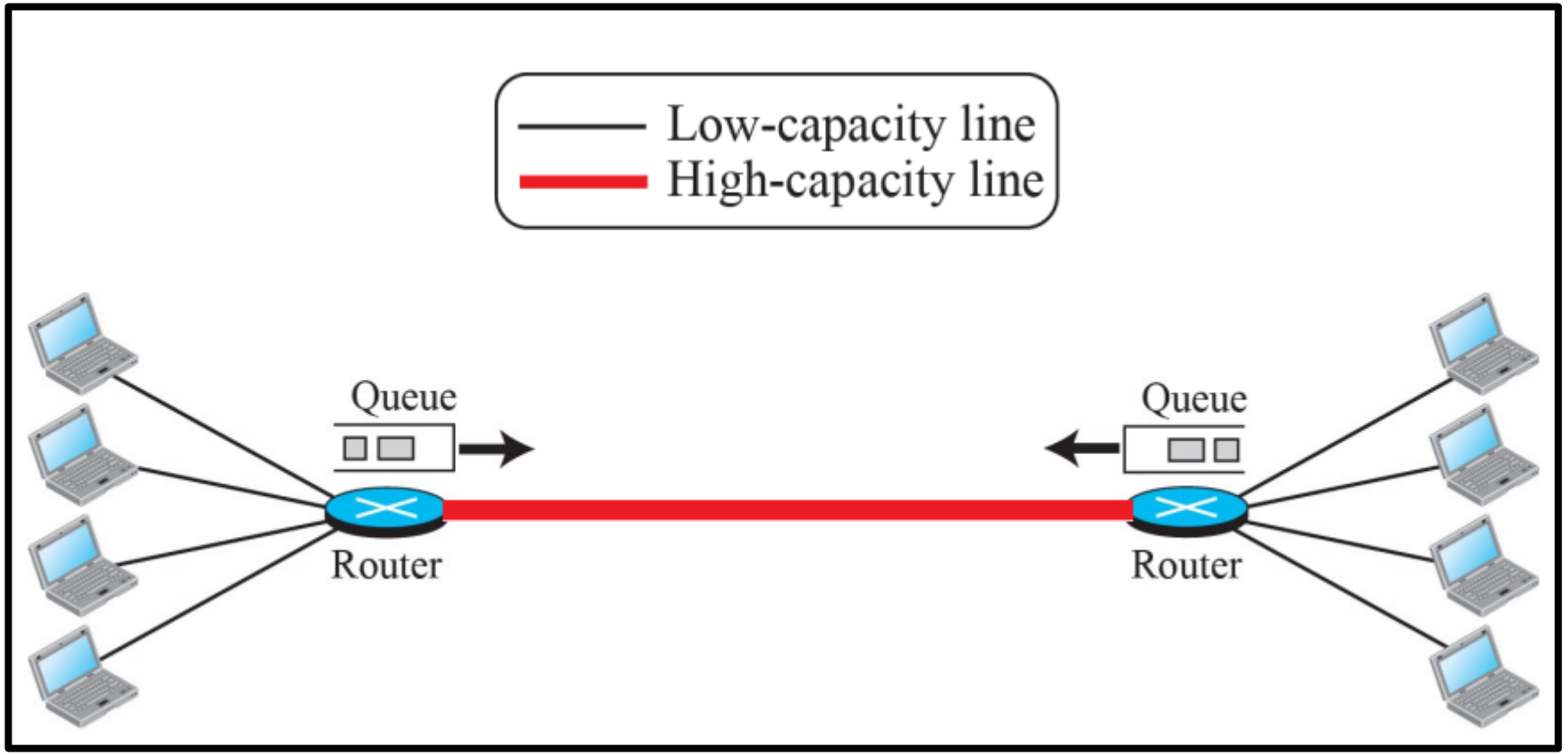
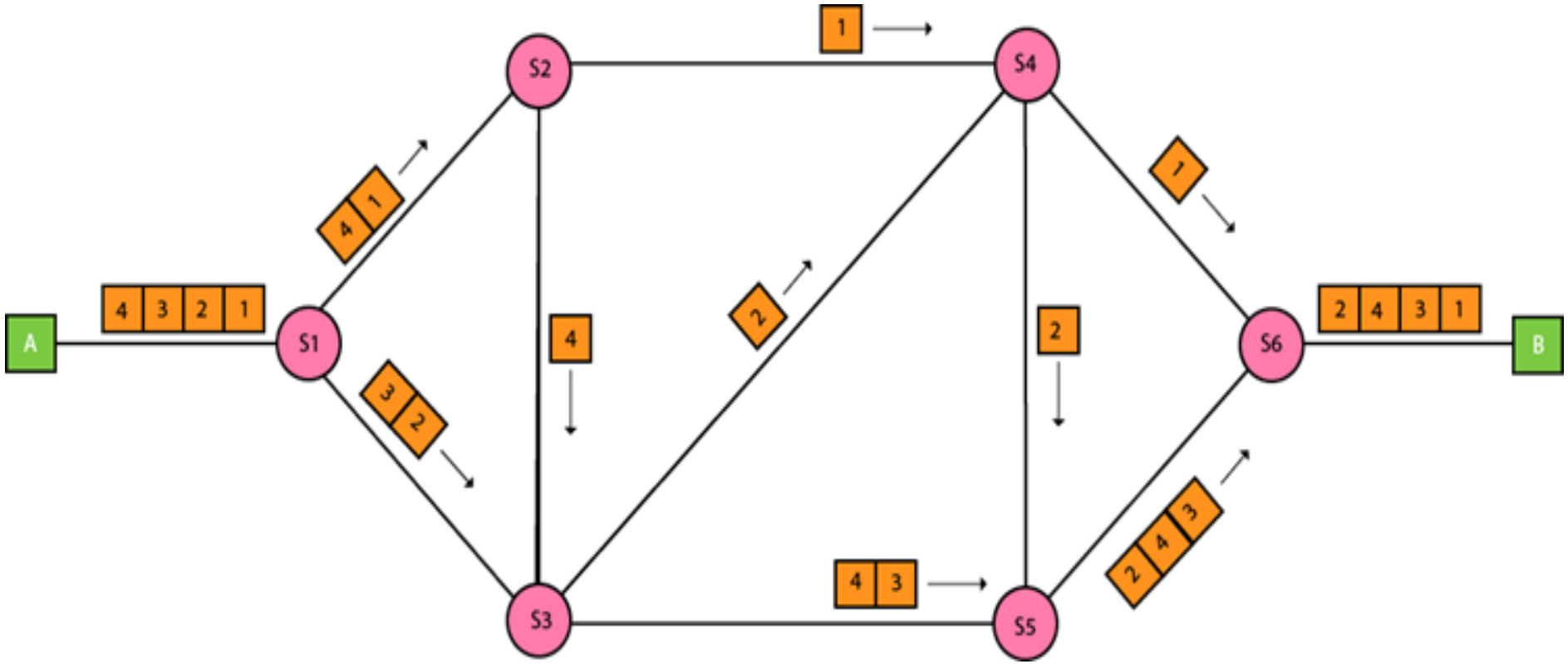


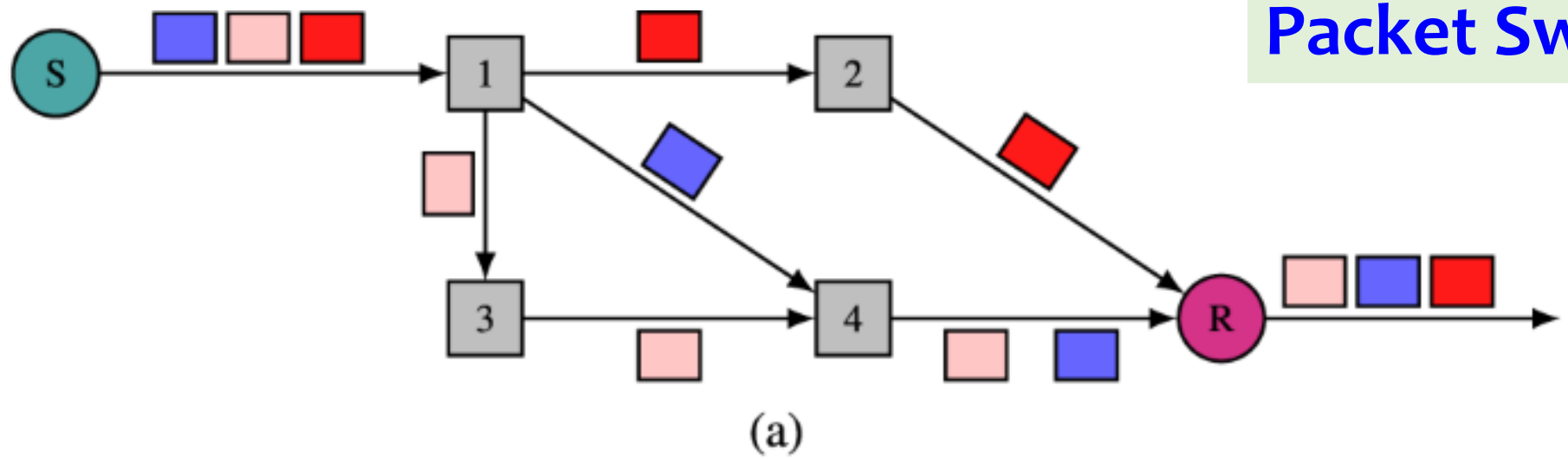
Figure: shows a small packet-switched network that connects four computers at one site to four computers at the other site.

Packet Switching:

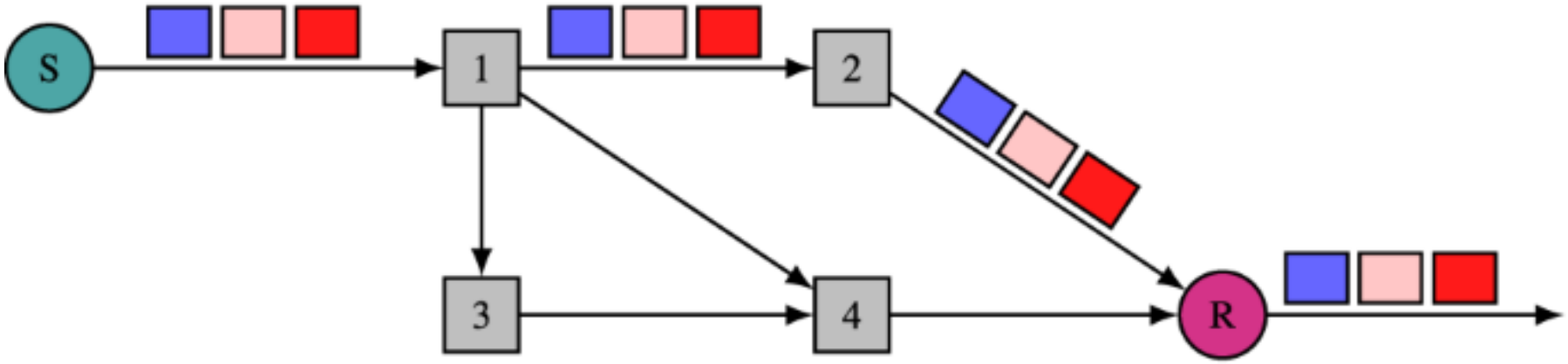


Packet-switched Network:

Packet Switching:

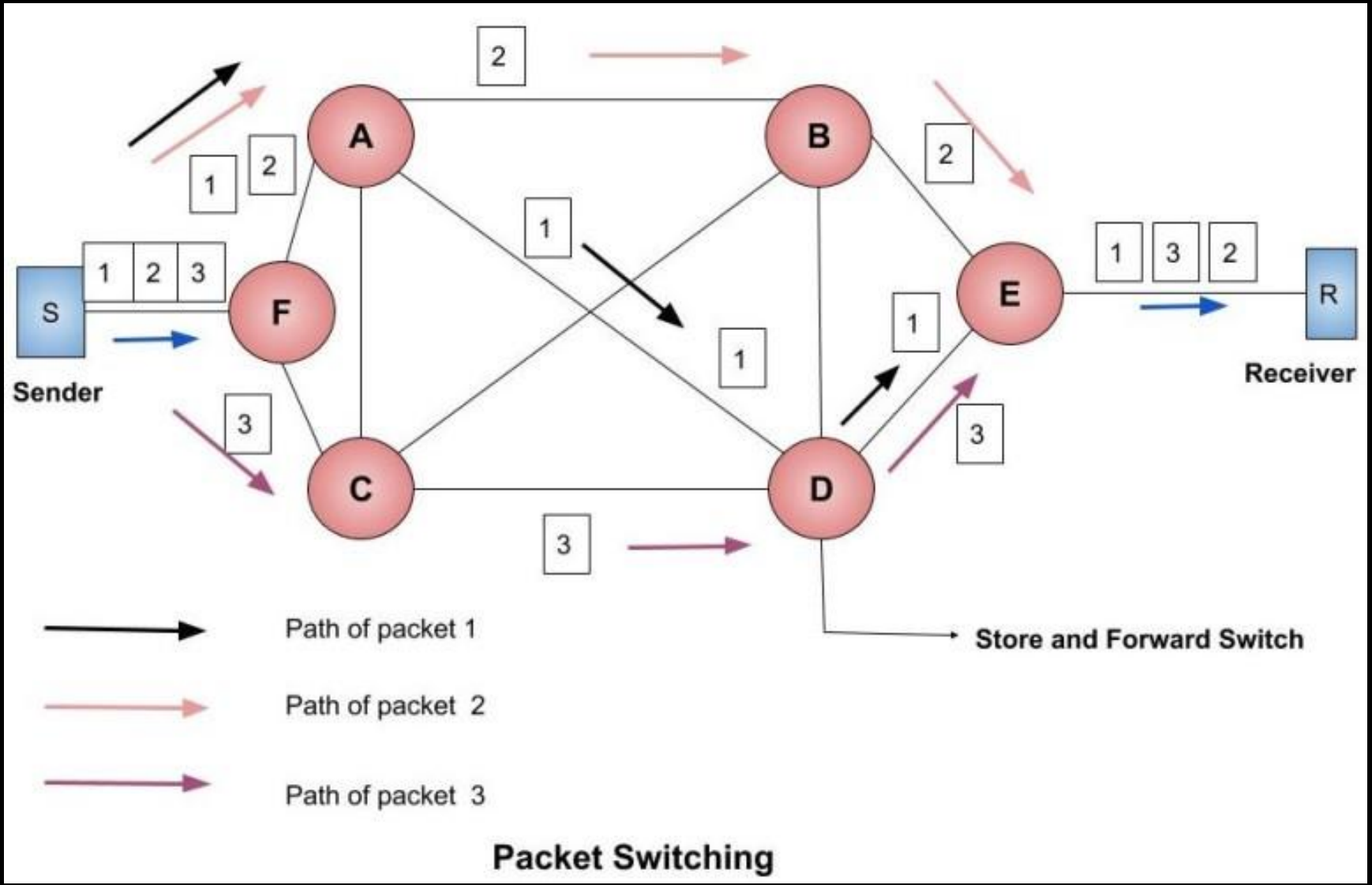


(a)



(b)

Packet-switched Network:



Packet-switched Network:

- A router in a packet-switched network has a queue that can store and forward the packet.
- Now assume that the capacity of the thick line is only twice the capacity of the data line connecting the computers to the routers.

❖Eg: If only two 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 the thick line is already working at its full capacity, the packets should be stored and forwarded in the order they arrived.
- The two simple examples show that a packet-switched network is more efficient than a circuit switched network, but the packets may encounter some delays.

Packet-switched Network:

Advantage:

- Packet-switched network is more efficient than a circuit switched network.

Disdvantage:

- Packets may encounter some delays.

Packet-switched Network:

- **Two approaches to Packet Switching:**

1. **Datagram Packet switching.**
2. **Virtual Circuit Switching**

i. Datagram Packet switching:

- It is a **packet switching technology** in which **packet** is known as a **datagram**, is considered as an **independent entity.**
- **Each packet** contains the **information about the destination** and **switch uses this information to forward** the packet to the **correct destination.**
- The packets are **reassembled** at the **receiving end** in correct order.
- In Datagram Packet Switching technique, the **path is not fixed.**
- **Intermediate nodes take the routing decisions** to forward the packets.
- Datagram Packet Switching is also known as **connectionless switching**.

ii. Virtual Circuit Packet Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Packet-Switching Techniques

- Datagram
  - each packet treated independently and referred to as a datagram
  - packets may take different routes, arrive out of sequence
- Virtual Circuit
  - preplanned route established for all packets
  - similar to circuit switching, but the circuit is not dedicated

H.w

1. Write the advantages & Disadvantages of Circuit Switching & Packet Switching.

Or

2. Differentiate between Circuit Switching & Packet Switching.

Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	Virtual Circuit approach
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

Packet-switched Network:

Advantages Of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

- More efficient in terms of bandwidth, since the concept of reserving circuit is not there.
- Minimal transmission latency.
- More reliable as destination can detect the missing packet.
- More fault tolerant because packets may follow different path in case any link is down, Unlike Circuit Switching.

Packet-switched Network:

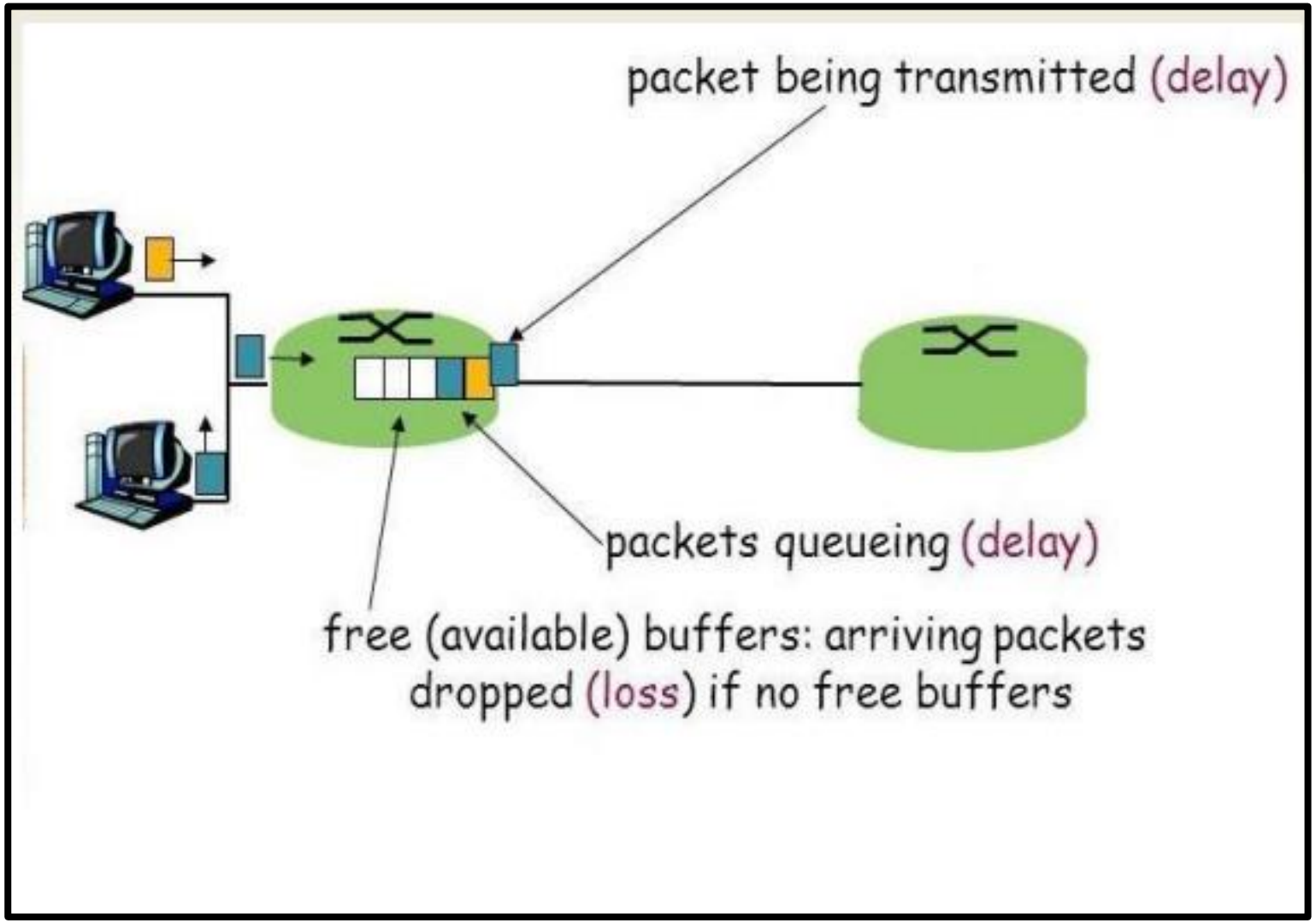
Disadvantage of Packet Switching:

- Packet Switching don't give packets in order, whereas Circuit Switching provides ordered delivery of packets because all the packets follow the same path.
- Since the packets are unordered, we need to provide sequence numbers to each packet.
- Complexity is more at each node because of the facility to follow multiple path.
- Transmission delay is more because of rerouting.
- Packet Switching is beneficial only for small messages, but for bursty data (large messages) Circuit Switching is better.
- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are not recovered.

QUEUING

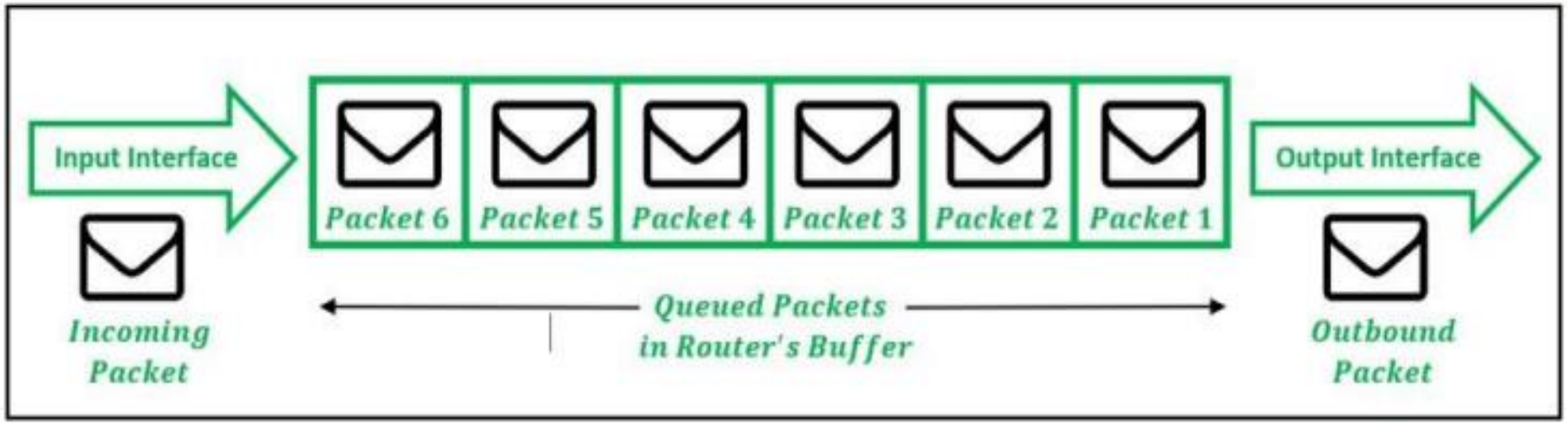
- Routers are essential networking devices that direct the flow of data over a network.
- Routers have one or more input and output interfaces which receive and transmit packets respectively.
- Since the router's memory is finite, a router can run out of space to accommodate freshly arriving packets.
- This occurs if the rate of arrival of the packets is greater than the rate at which packets exit from the router's memory.
- In such a situation, new packets are ignored or older packets are dropped.
- So, As part of the resource allocation mechanisms, routers must implement some queuing discipline that governs how packets are buffered or dropped when required.

QUEUE


packet being transmitted (delay)
packets queueing (delay)
free (available) buffers: arriving packets
dropped (loss) if no free buffers

QUEUE

- A queue, in computer networking, is a collection of data packets collectively waiting to be transmitted by a network device using a pre-defined structure methodology.
- A queue consists of a number of packets.



QUEUE:

Queue Congestion and Queuing Disciplines:

- **Router queues are susceptible to congestion by virtue of the limited buffer memory available to them.**
- ***The causes of such a situations are:***
  a) **Speed of incoming traffic exceeds the rate of outgoing traffic.**
  b) **The combined traffic from all the input interfaces exceeds overall output capacity.**
  c) **The router processor is incapable of handling the size of the forwarding table to determine routing paths.**

- To manage the allocation of router memory to the packets in such situations of congestion, different disciplines might be followed by the routers to determine which packets to keep and which packets to drop.

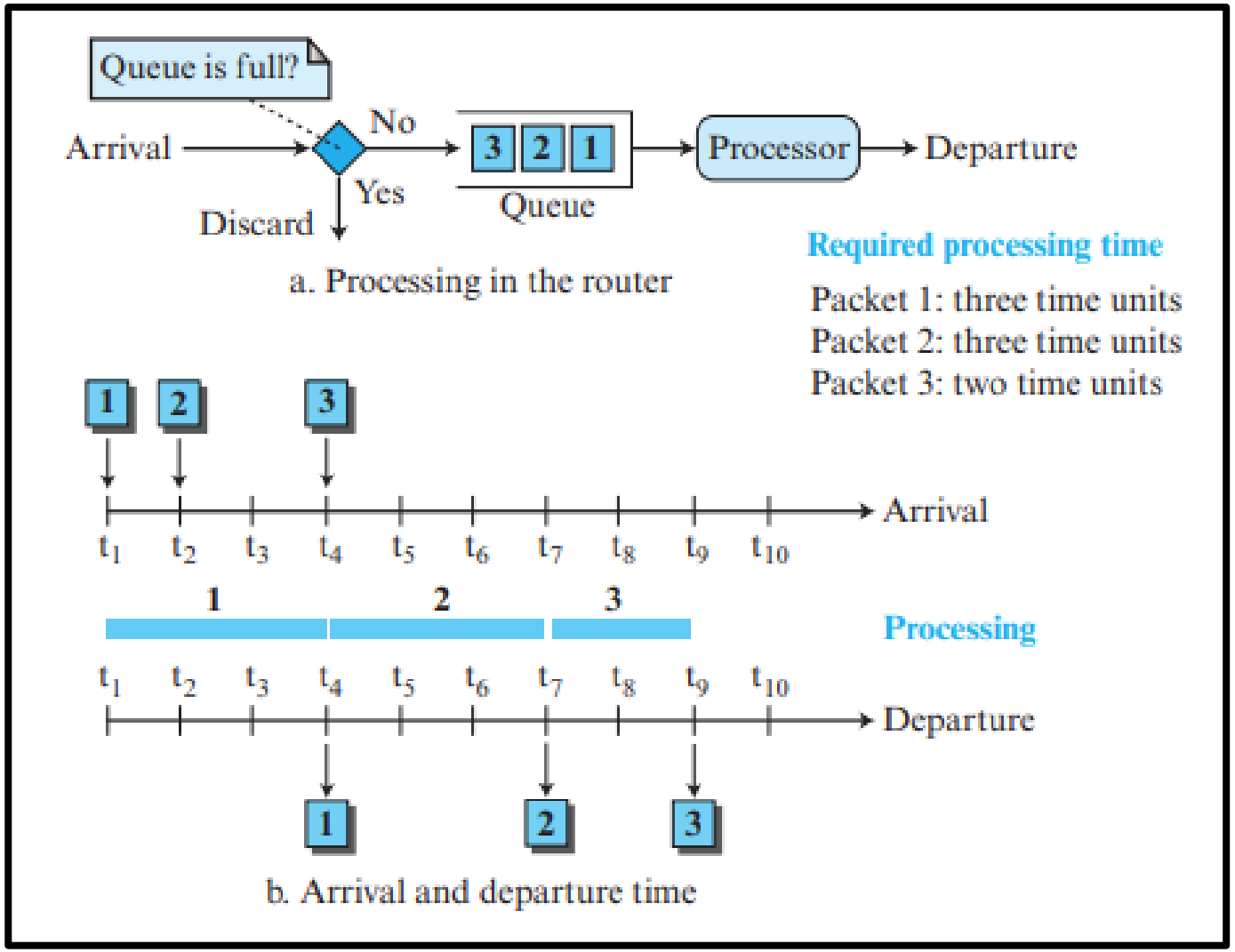
Queuing Disciplines In Routers:

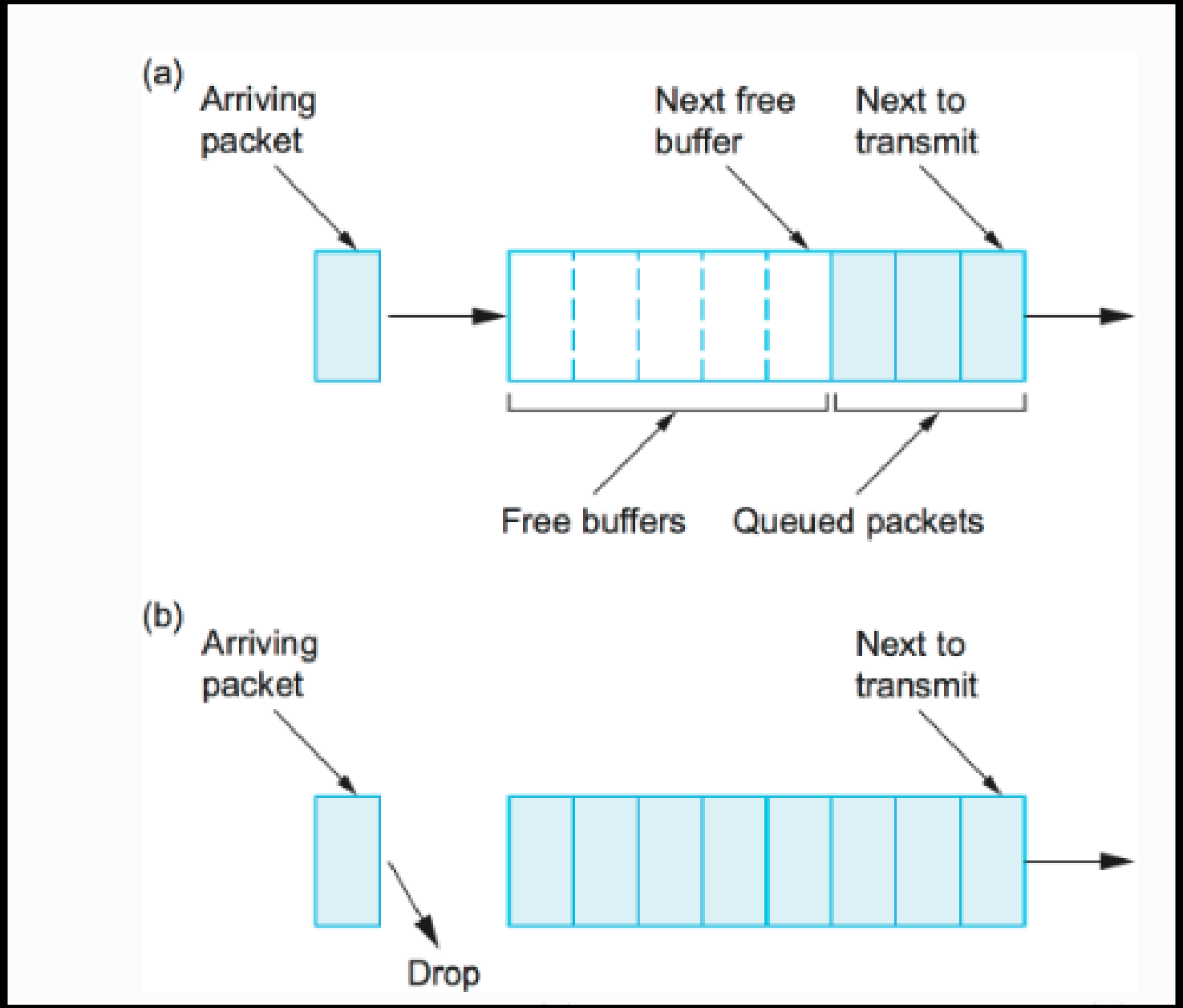
i. First-In, First-Out Queuing (FIFO)
ii. Priority Queuing (PQ)
iii. Fair queuing
iv. Weighted Fair Queuing (WFQ)

1. FIRST-IN, FIRST-OUT QUEUING (FIFO)

- The default queuing scheme followed by most routers is FIFO.
- This generally requires little or no configuration to be done on the server.
- All packets in FIFO are serviced in the same order as they arrive in the router.
- On reaching saturation within the memory, new packets attempting to enter the router are dropped (tail drop).
- Such a scheme, however, is not apt for real-time applications, especially during congestion.
- Eg:- *A real-time application such as VoIP (Voice over Internet Protocol), which continually sends packets, may be starved during times of congestion and have all its packets dropped.*

FIFO QUEUE


Queue is full?
No
Arrival
3 2 1
Processor
Departure
Yes
Discard
Queue
a. Processing in the router
Required processing time
Packet 1: three time units
Packet 2: three time units
Packet 3: two time units
1 2 3
Arrival
t1 t2 t3 t4 t5 t6 t7 t8 t9 t10
1 2 3
Processing
t1 t2 t3 t4 t5 t6 t7 t8 t9 t10
Departure
1 2 3
b. Arrival and departure time



a) FIFO queuing:
b) Tail drop at a FIFO queue

2. PRIORITY QUEUING (PQ)

- In priority queuing, packets are first assigned to a priority class.
- Each priority class has its own queue.
- The packets in the highest-priority queue are processed first.
- Packets in the lowest-priority queue are processed last.
- the system does not stop serving a queue until it is empty.
- A packet priority is determined from a specific field in the packet header:
  - the ToS (type of service) field of an IPv4 header;
  - the priority field of IPv6
  - a priority number assigned to a destination address, or
  - a priority number assigned to an application (destination port number), and so on.

PRIORITY QUEUING (PQ)....

- A priority queue can provide better QoS than the FIFO queue because higher-priority traffic, such as multimedia, can reach the destination with less delay.

Drawback:

- If there is a continuous flow in a high-priority queue, the packets in the lower-priority queues will never have a chance to be processed.
- This is a condition called Starvation.
- Severe starvation may result in dropping of some packets of lower priority.
- In the figure, the packets of higher priority are sent out before the packets of lower priority.

PRIORITY QUEUING (PQ)….

- **Traffic flows are distinguished and identified based on various header fields in the packets, such as:**

➢ **Source and Destination IP address**

➢ **Source and Destination TCP (or UDP) port**

➢ **IP Protocol number**

➢ **Type of Service value**

QUEUE

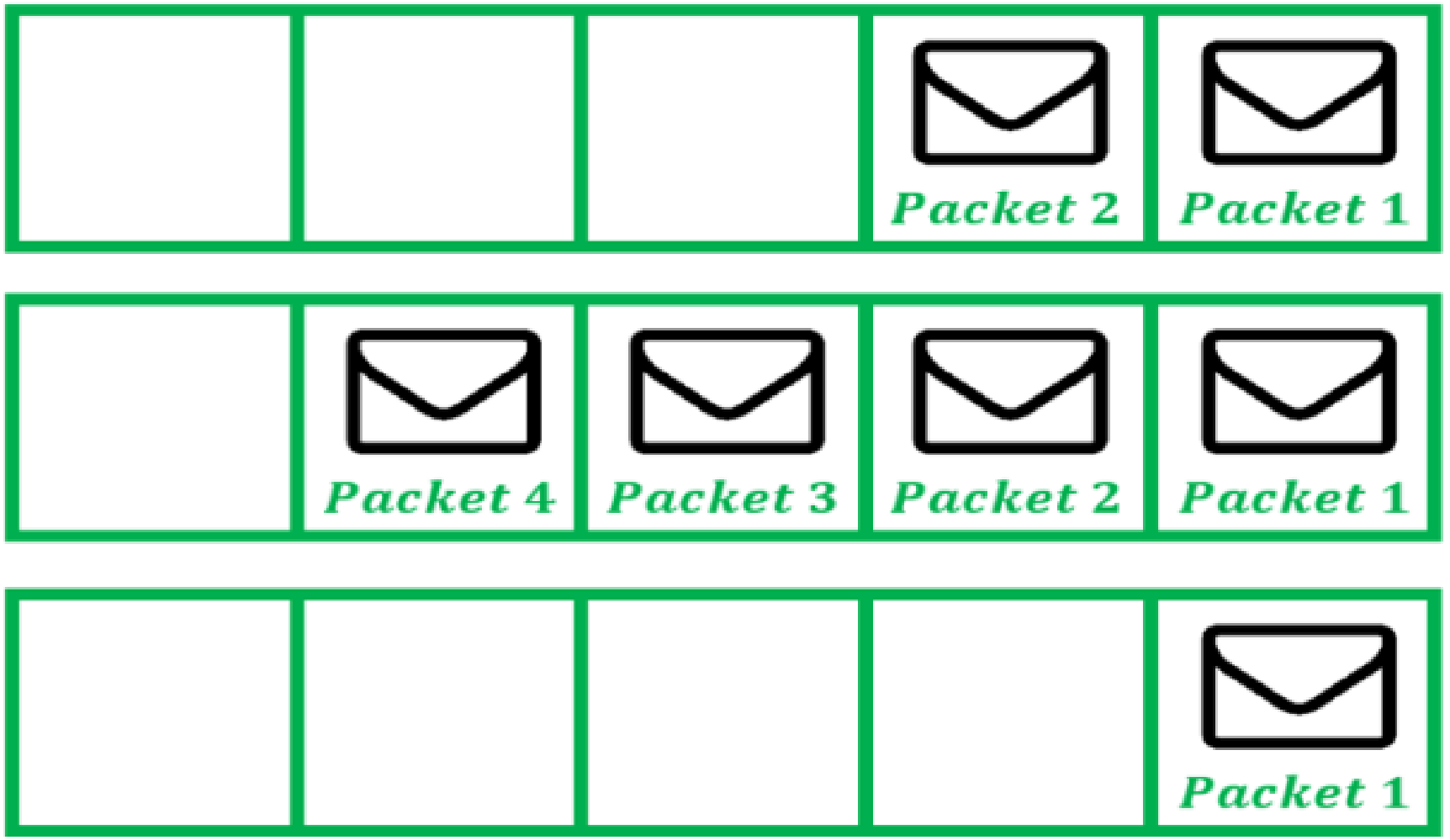
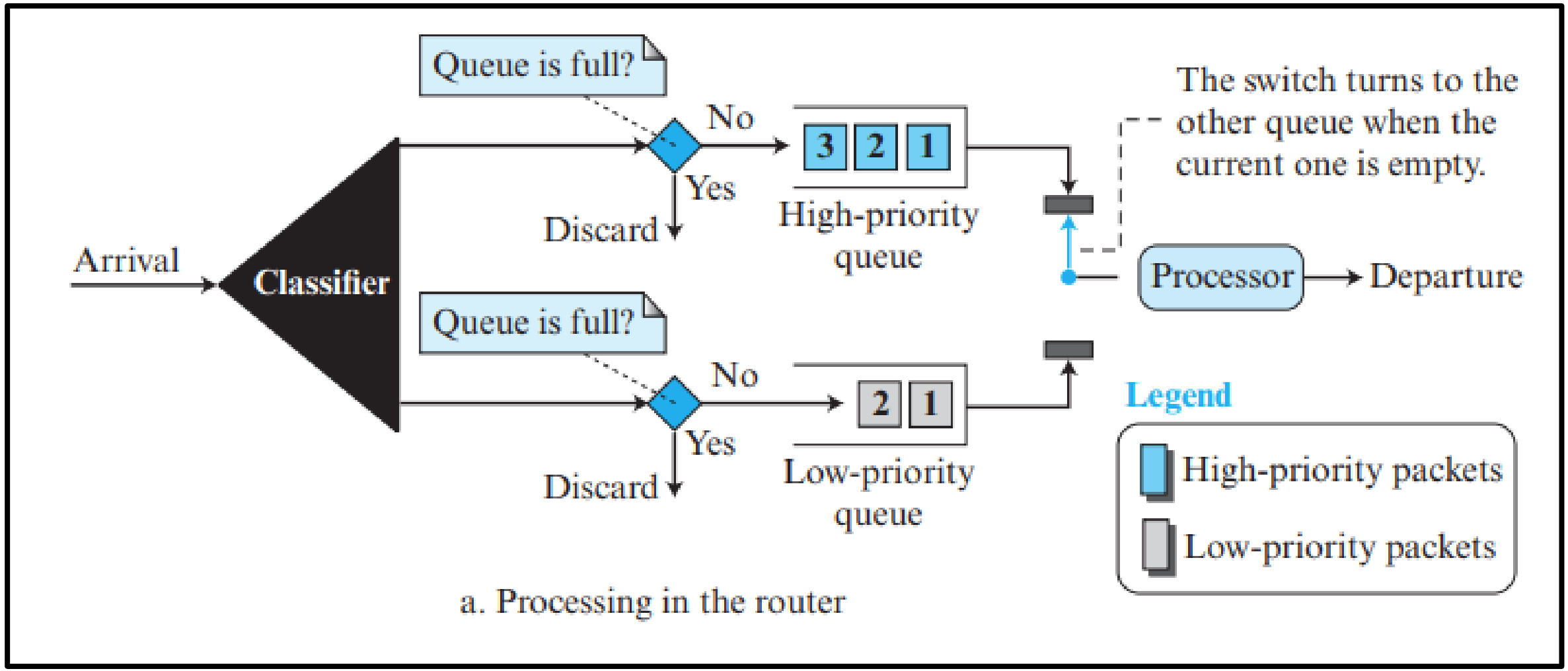
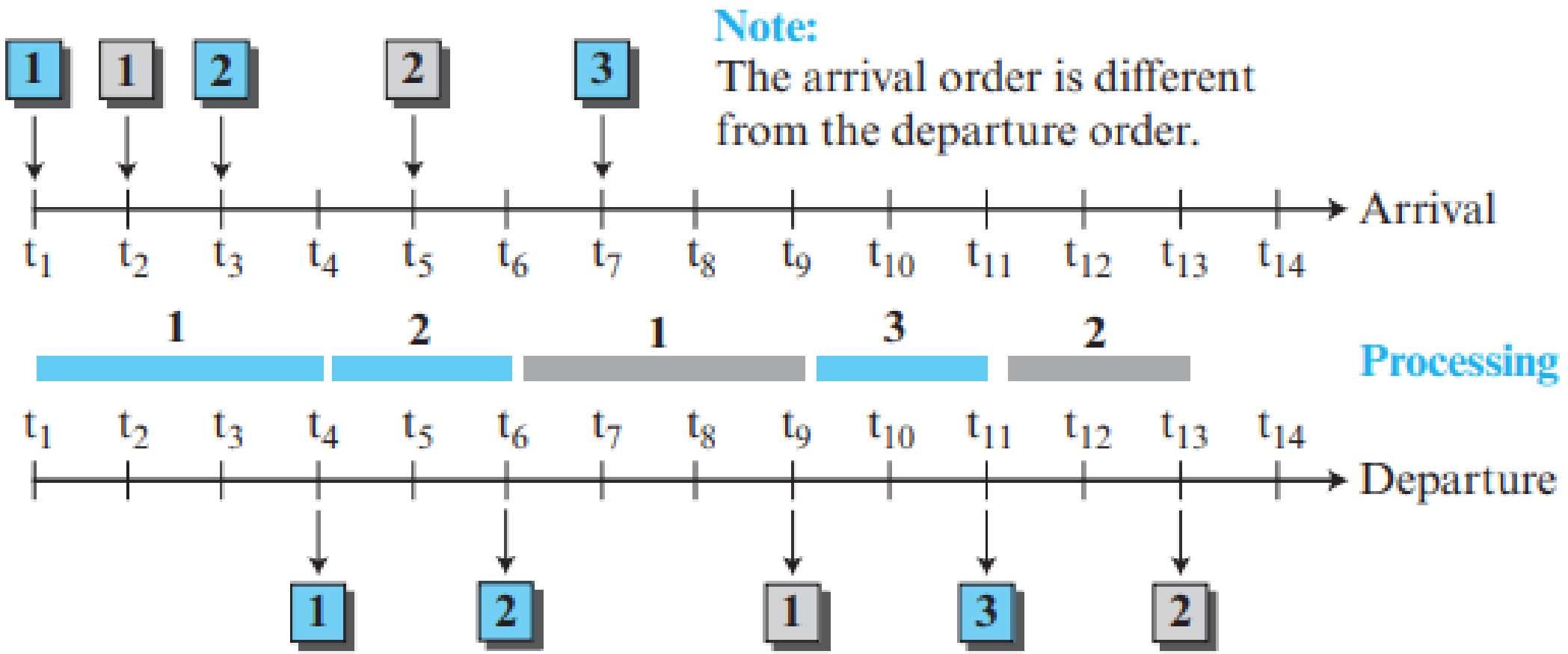

Packet 2
Packet 1
Packet 4
Packet 3
Packet 2
Packet 1
Packet 1
High Priority subqueue
Medium Priority subqueue
Low Priority queue

Figure shows priority queuing with two priority levels:



a. Processing in the router

Priority Queuing:



b. Arrival and departure time

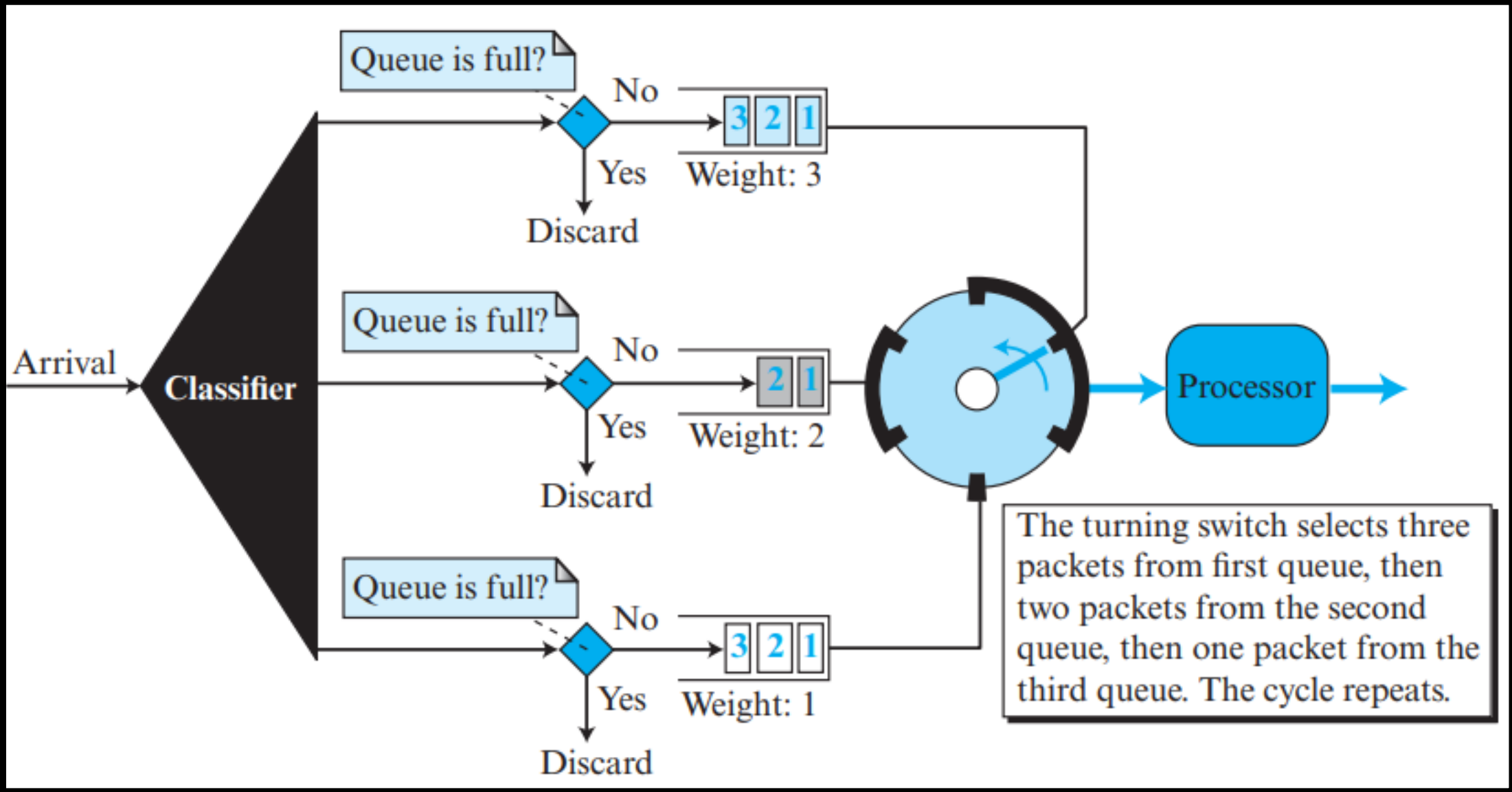
Weighted Fair Queuing:

- A better scheduling method is weighted fair queuing.
- In this technique, the packets are still assigned to different classes and admitted to different queues.
- The queues, however, are weighted based on the priority of the queues;
- higher priority → higher weight.
- The system processes packets in each queue in a round-robin fashion with the number of packets selected from each queue based on the corresponding weight.

Weighted Fair Queuing:

- For example, if the weights are 3, 2, and 1; then
  - Three packets are processed from the first queue;
  - Two from the second queue, and
  - One from the third queue.
- In this way, we have fair queuing with priority.
- In weighted fair queuing, each class may receive a small amount of time in each time period.

Weighted Fair Queuing



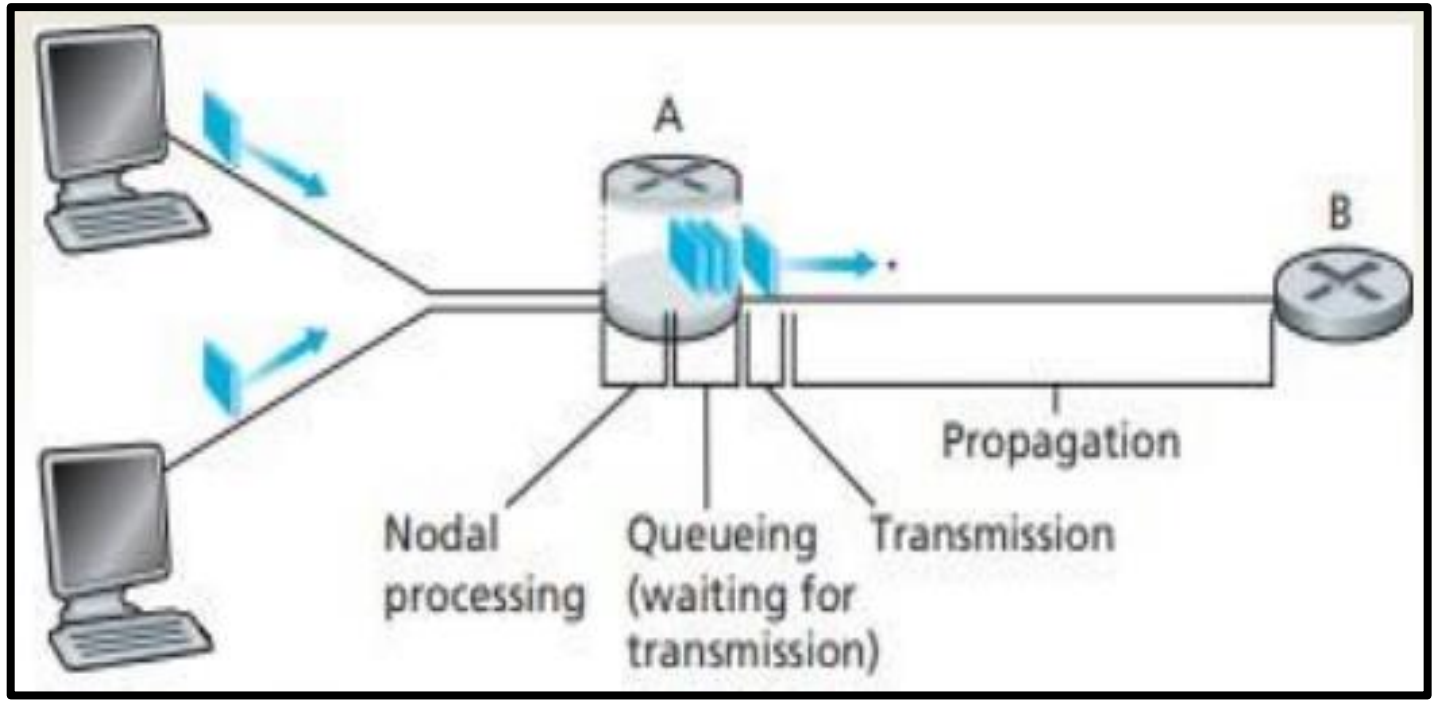
Weighted Fair Queuing:

- In otherwords, a fraction of time is devoted to serve each class of packets, but the fraction depends on the priority of the class.
- For example, in the figure, if the throughput for the router is R, the class with the highest priority may have the throughput of R/2, the middle class may have the throughput of R/3, and the class with the lowest priority may have the throughput of R/6.
- However, this situation is true if all three classes have the same packet size, which may not occur.
- Packets of different sizes may create many imbalances in dividing a decent share of time between different classes.

NETWORK DELAY

- Queueing delay is the time a job waits in a queue until it can be executed.
- The delay refers to the time required to transmit a packet or a group of packets from the transmit end to the receive end.
- To send a packet from A to B there are delays since this is a Store and Forward network.
- It specifies the latency for a bit of data to travel across the network from one communication endpoint to another.
- It is typically measured in multiples or fractions of a second.
- We have the following types of delays in computer network:
  a) Processing delay – time it takes a router to process the packet header
  b) Queuing delay – time the packet spends in routing queues
  c) Transmission delay – time it takes to push the packet's bits onto the link
  d) Propagation delay – time for a signal to propagate through the media

NETWORK DELAY



Nodal delay at router A

- Let d_{proc}, d_{queue}, d_{trans}, and d_{prop} denote the processing, queuing, transmission, and propagation delays;
- Total nodal delay, $d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$

NETWORK DELAY

- **Processing delay** is the **time taken** by **a switch to process the packet header.** The delay depends on the **processing speed** of the switch.
- **Queuing delay** refers to the **time** that a **packet waits** to be **processed in the buffer** of a switch. The delay is **dependent on** the **arrival rate** of the incoming packets, the **transmission capacity** of the outgoing link, and the **nature of the network's traffic.**

NETWORK DELAY

- **Transmission delay** refers to the time it takes to transmit a data packet onto the outgoing link.
- The delay is determined by the size of the packet and the capacity of the outgoing link:
  - Transmission Delay=L/R
  - L→Length of the packet
  - R→Transmission rate of the link from router A to router B(Rbits/sec)

NETWORK DELAY

- **Propagation delay** is the **time** that it takes **for a bit to reach from one end of a link to the other**.
- The delay **depends** on the **distance** between the sender and the receiver, and the **propagation speed** of the wave signal.

Throughput

- Consider transferring a large file (video clip) from host A to host B:

➢ **Instantaneous throughput:** The rate at which host B is receiving the file.

➢ **Average throughput:** If the file consist of F bits and the transfer take T seconds for the receiver to receive all F bits, then the average throughput is F/T Latency is the measure of throughput.

➢ **Latency:-** The time taken for the data to get at its destination across the network.

Quality of Service

P. 674

- Quality of service (QoS) is an internetworking issue that refers to a set of techniques and mechanisms that guarantees the performance of the network to deliver predictable service to an application program.
- Quality of service (QoS) is the measurement of the overall performance of a computer network, particularly the performance seen by the users of the network.
- To quantitatively measure quality of service, several related aspects of the network service are to be considered, such as packet loss, bit rate, throughput, transmission delay, availability, jitter, etc.

Quality of Service

- In computer networking and other packet- switched telecommunication networks, quality of service refers to traffic prioritization and resource reservation control mechanisms.
- QoS is exclusively applied to network traffic generated for video on demand, IPTV, VoIP, streaming media, videoconferencing and online gaming.

Quality of Service

Data-Flow Characteristics:

- If we want to provide quality of service for an Internet application, we first need to define what we need for each application.
- Four types of characteristics are attributed to a data flow: Reliability, Delay, Jitter, and Bandwidth.

Quality of Service

Data-Flow Characteristics:

i. Reliability:

- Reliability is a characteristic that a flow needs in order to deliver the packets safe and sound to the destination.
- Lack of reliability means losing a packet or acknowledgment, which causes retransmission.
- Sensitivity of different application programs to reliability varies.
- For example, reliable transmission is more important for electronic mail, file transfer, and Internet access than for telephony or audio conferencing.

Quality of Service

Data-Flow Characteristics:

Delay:

- **Source-to-destination delay** is another flow characteristic.
- Again, **applications** can **tolerate delay** in **different degrees.**
- In this case, **telephony, audio conferencing, video conferencing,** and remote login need **minimum delay**, while delay in file transfer or e-mail is less important.

Quality of Service

Data-Flow Characteristics:

Jitter:

- Jitter is the variation in delay for packets belonging to the same flow.

i. For example, if four packets depart at times 0, 1, 2, 3 and arrive at 20, 21, 22, 23, all have the same delay, 20 units of time.

ii. On the other hand, if the above four packets arrive at 21, 23, 24, and 28, they will have different delays.

- For applications such as audio and video, the first case is completely acceptable; the second case is not.
- These types of applications do not tolerate jitter.

Quality of Service

Data-Flow Characteristics:

Bandwidth:

- Different applications need different bandwidths.
- In video conferencing we need to send millions of bits per second to refresh a color screen, while the total number of bits in an e-mail may not reach even a million.

Data-Flow Characteristics:

Sensitivity of Applications:

- **Various applications are sensitive to some data flow characteristics.**

Table 8.9 *Sensitivity of applications to flow characteristics*

Application	*Reliability*	*Delay*	*Jitter*	*Bandwidth*
FTP	High	Low	Low	Medium
HTTP	High	Medium	Low	Medium
Audio-on-demand	Low	Low	High	Medium
Video-on-demand	Low	Low	High	High
Voice over IP	Low	High	High	Low
Video over IP	Low	High	High	High

Eg: Amazon Music
for a monthly fee

Eg:- Amazon Prime Vid
YouTube, etc

Quality of Service

Sensitivity of Applications(cntd..):

- For those applications with a high level of sensitivity to reliability, we need to do error checking and discard the packet if corrupted.
- For those applications with a high level of sensitivity to delay, we need to be sure that they are given priority in transmission.
- For those applications with a high level of sensitivity to jitter, we need to be sure that the packets belonging to the same application pass the network with the same delay.
- Finally, for those applications that require high bandwidth, we need to allocate enough bandwidth to be sure that the packets are not lost.

Quality of Service

Flow Classes:

- Based on the flow characteristics, we can classify flows into groups, with each group having the required level of each characteristic.
- The Internet community has not yet defined such a classification formally.
- However, we know, for example, that a protocol like FTP needs a high level of reliability and probably a medium level of bandwidth, but the level of delay and jitter is not important for this protocol.

As per ATM specifications, there are five classes of defined service:

a) Constant Bit Rate (CBR)

b) Variable Bit Rate-Non Real Time (VBR-NRT)

c) Variable Bit Rate-Real Time (VBR-RT)

d) Available Bit Rate (ABR)

e) Unspecified Bit Rate (UBR)

Quality of Service

a) **Constant Bit Rate (CBR):** This class is used for emulating circuit switching. CBR applications are quite sensitive to cell-delay variation. Examples of CBR are telephone traffic, video conferencing, and television.

b) **Variable Bit Rate-Non Real Time (VBR-NRT):** Users in this class can send traffic at a rate that varies with time depending on the availability of user information. An example is multimedia e-mail.

c) **Variable Bit Rate-Real Time (VBR-RT):** This class is similar to VBR–NRT but is designed for applications such as interactive compressed video that are sensitive to cell delay variation.

d) **Available Bit Rate (ABR):** This class of ATM services provides rate-based flow control and is aimed at data traffic such as file transfer and e-mail.

e) **Unspecified Bit Rate (UBR):** This class includes all other classes and is widely used today for TCP/IP.

Flow Control to Improve QoS

- *Several Mechanisms:*

✓**Scheduling:**

i. **FIFO Queuing**
ii. **Priority Queuing**
iii. **Weighted Fair Queuing**

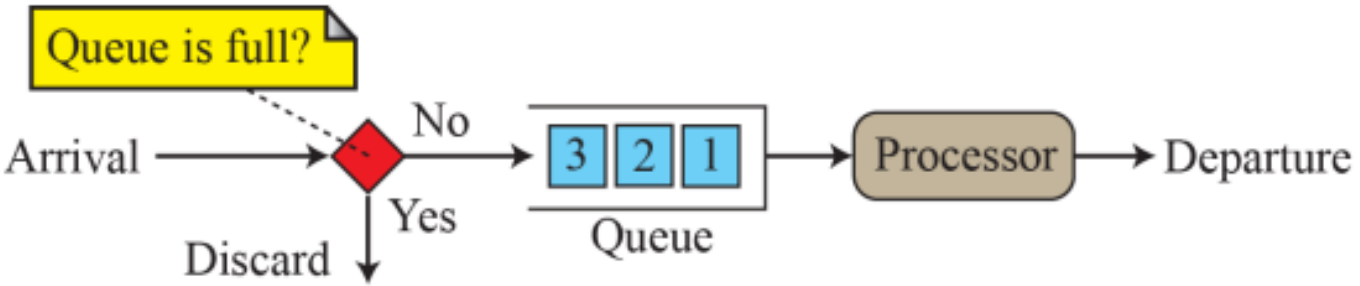
✓**Traffic Shaping or Policing**

i. **Leaky Bucket**
ii. **Token Bucket**

✓**Resource Reservation**

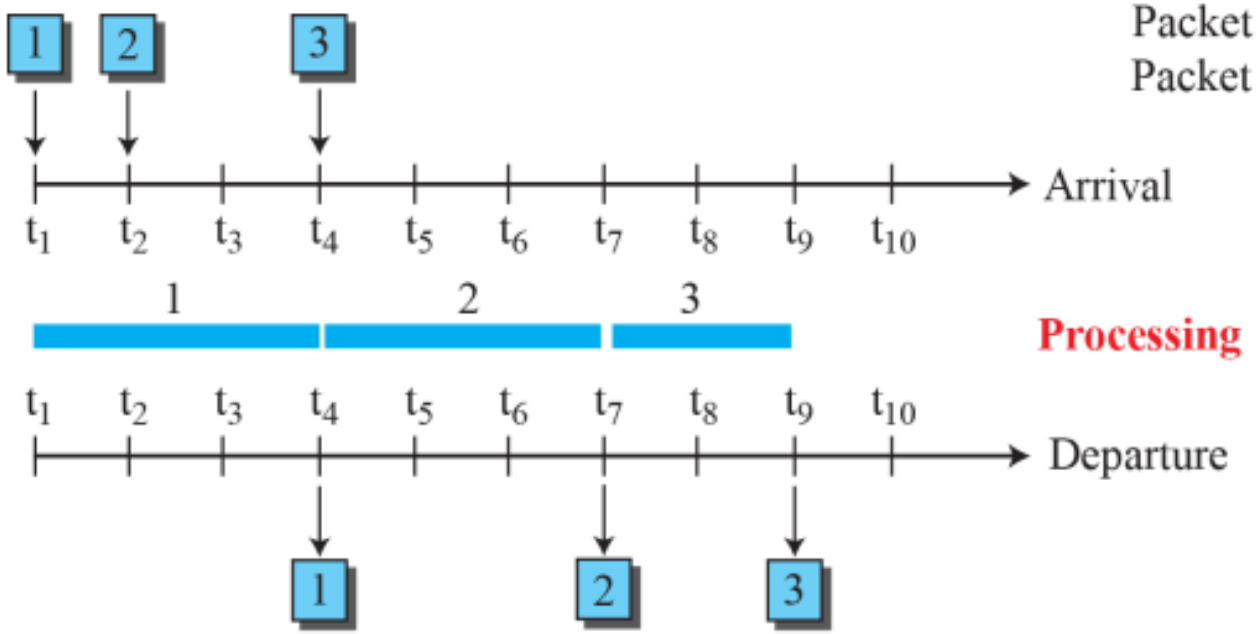
✓**Admission Control**

Figure 8.59 : FIFO queue



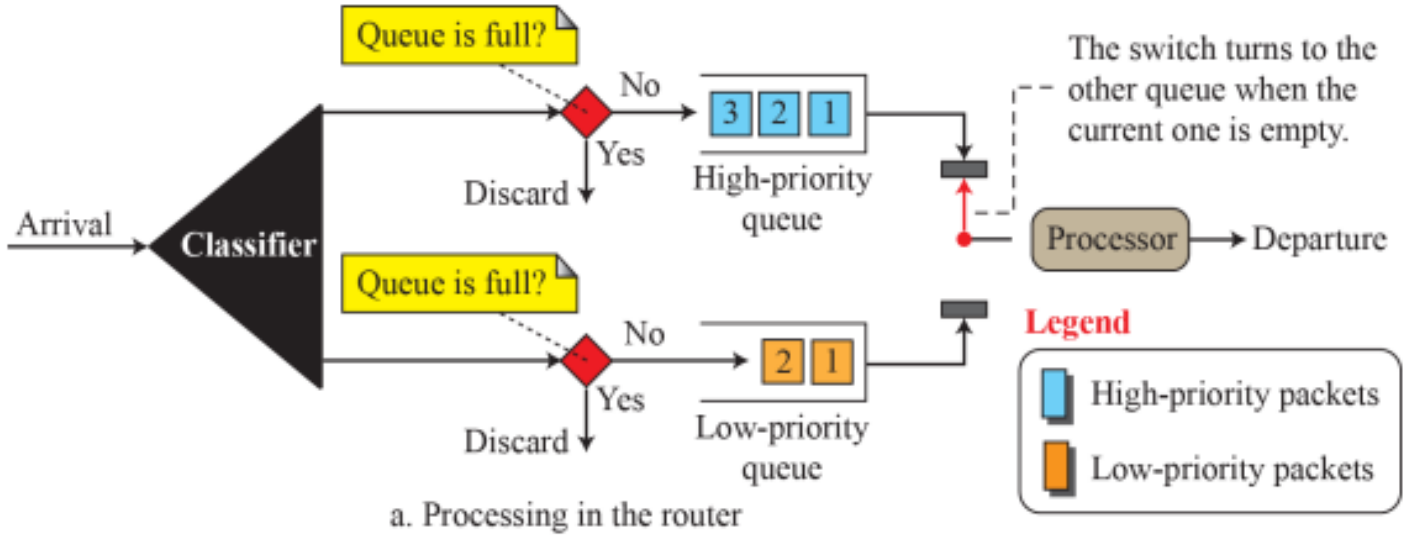
a. Processing in the router

Required processing time
Packet 1: three time units
Packet 2: three time units
Packet 3: two time units

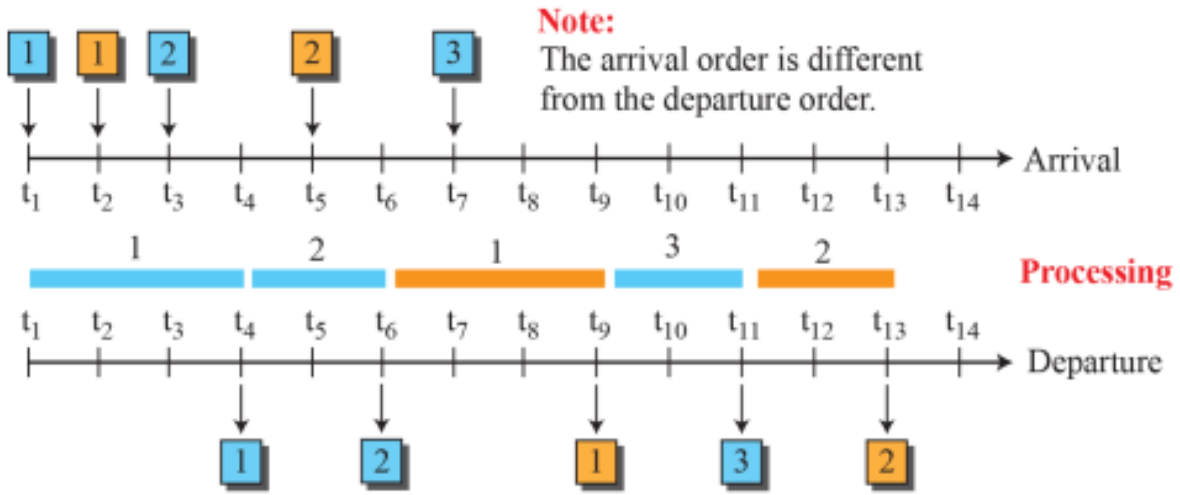


b. Arrival and departure time

Figure 8.60 : Priority queuing

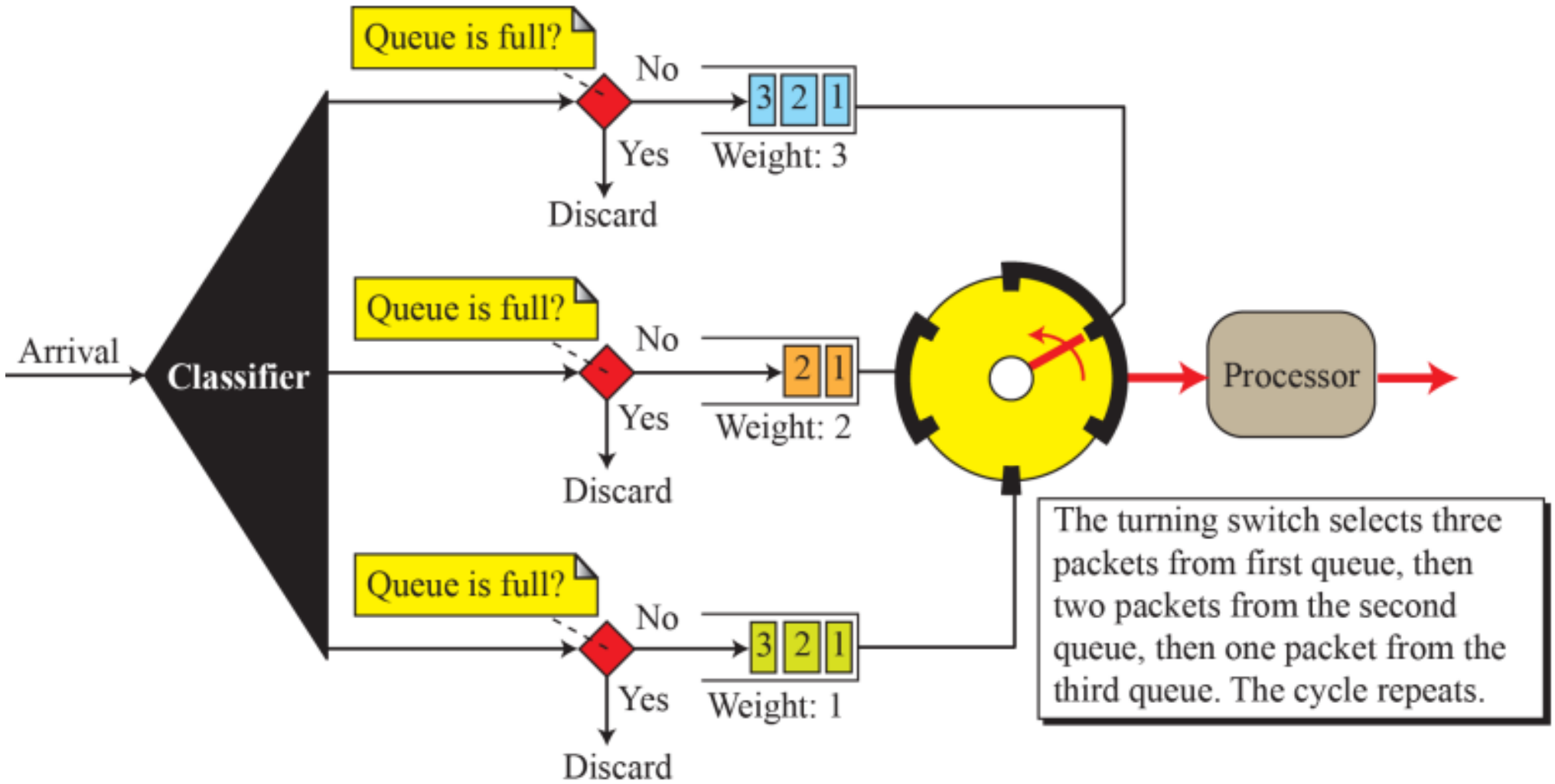


a. Processing in the router



b. Arrival and departure time

Weighted Fair Queuing:



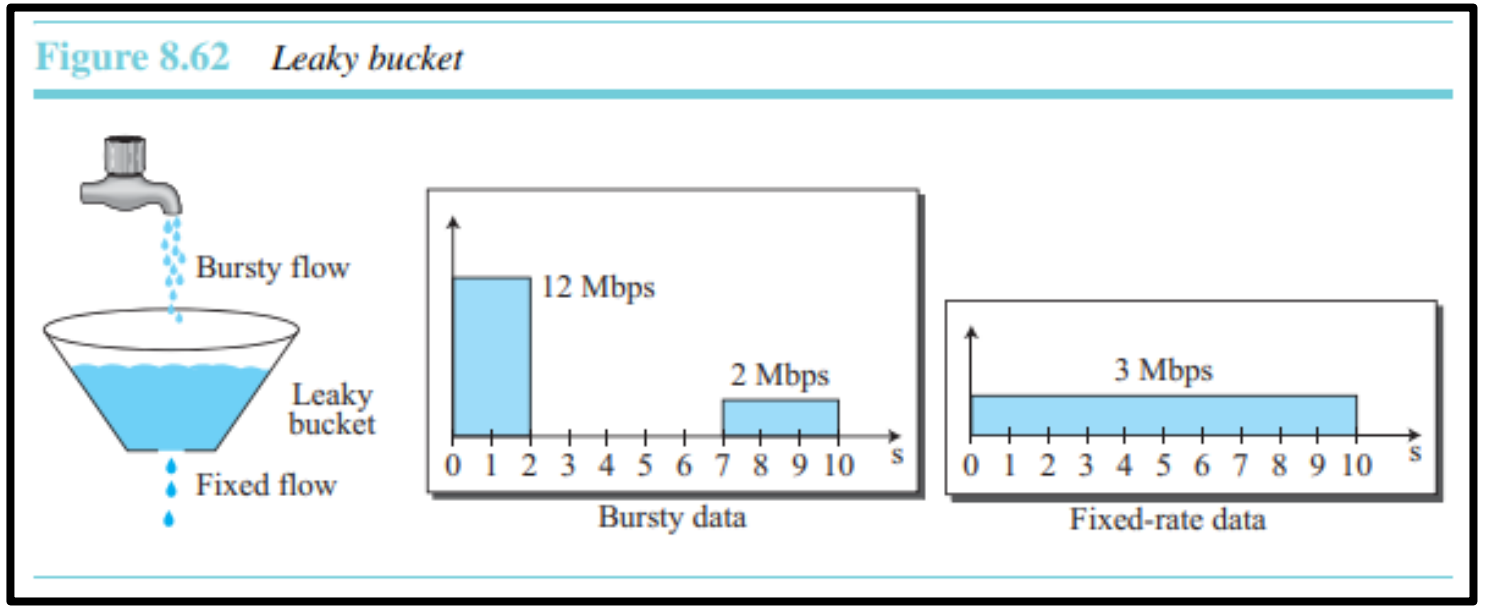
Quality of Service (cntd.)

Traffic Shaping or Policing:

- To control the amount and the rate of traffic is called traffic shaping or traffic policing.
- Traffic shaping is used → when the traffic leaves a network;
- Traffic policing is used → when the data enters the network.
- *Two techniques can shape or police the traffic:*
  i. Leaky bucket &
  ii. Token bucket

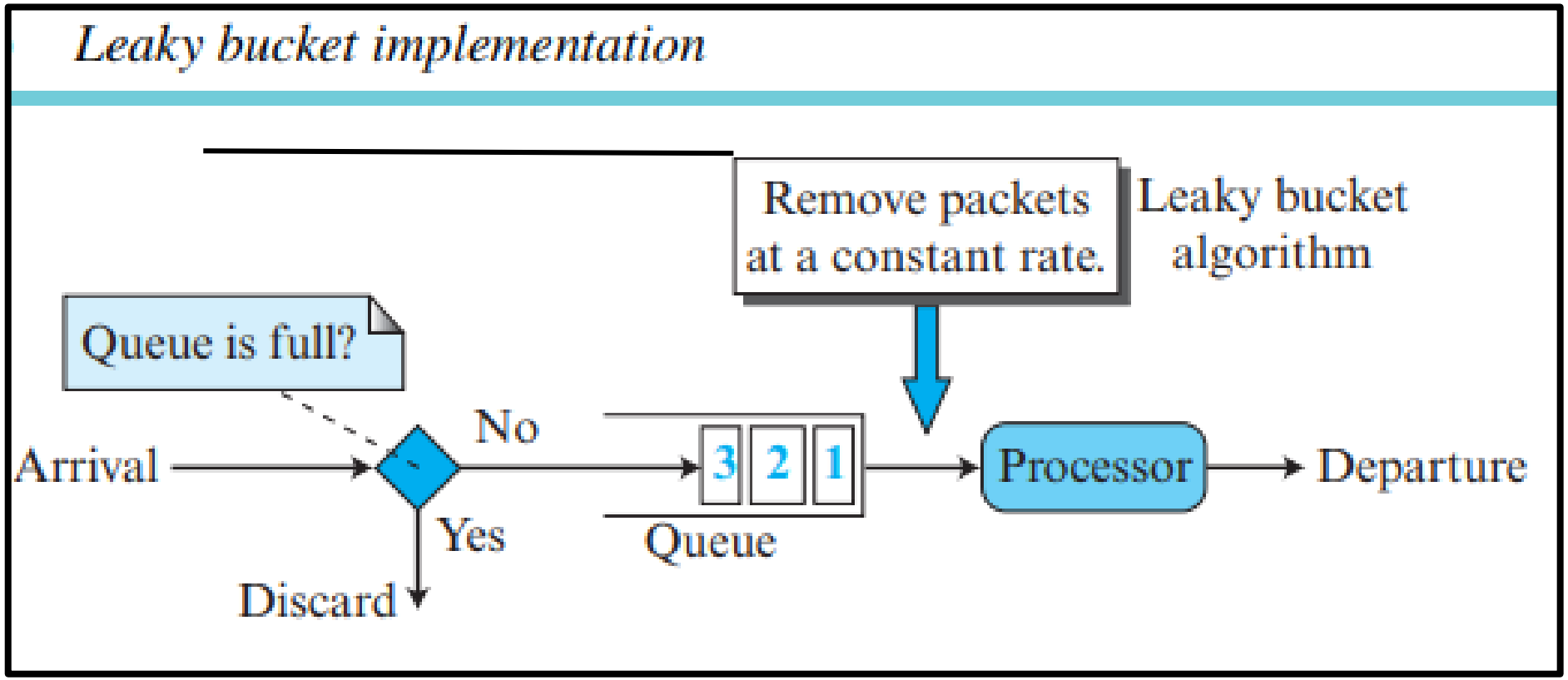
Leaky Bucket

- In networking, a technique called leaky bucket can smooth out bursty traffic.
- Bursty chunks are stored in the bucket and sent out at an average rate.
- Figure shows a leaky bucket and its effects.

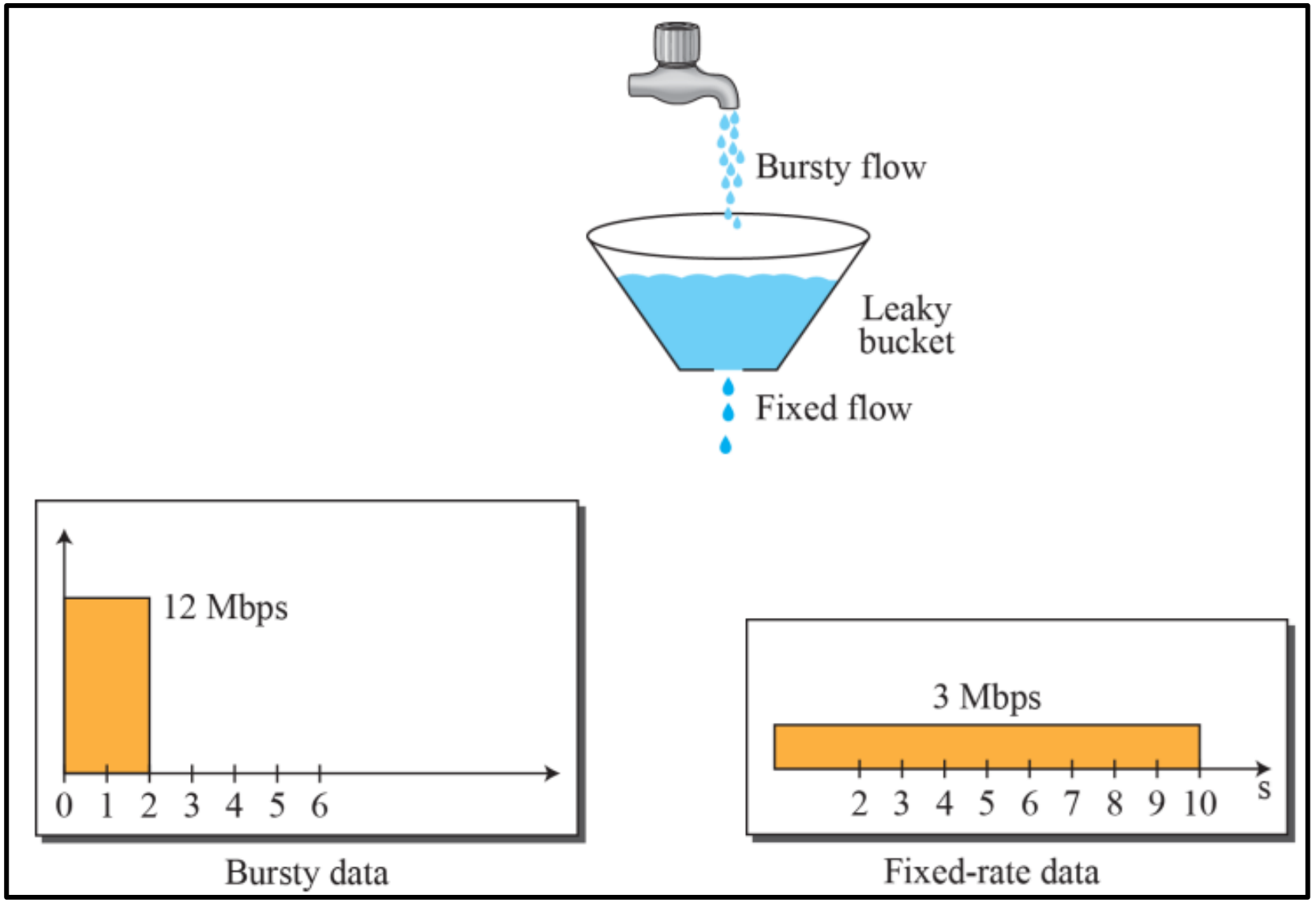


Quality of Service (cntd.)

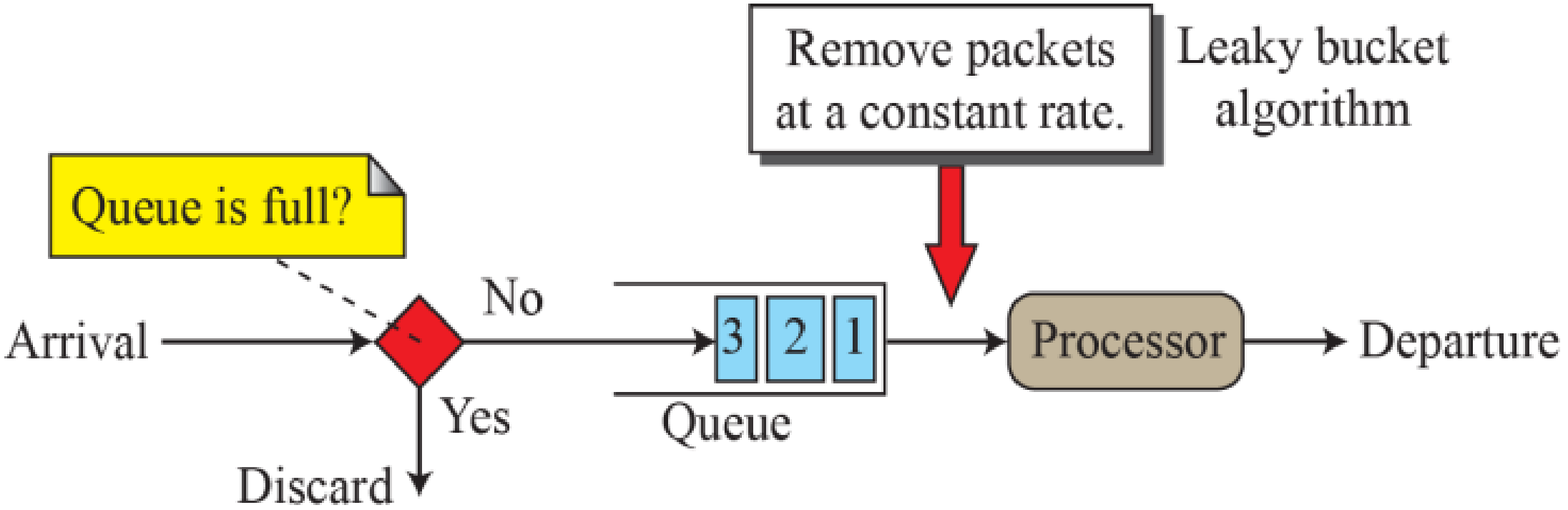
- A Leaky Bucket Algorithm shapes bursty traffic into fixed-rate traffic by averaging the data rate.
- It may drop the packets if the bucket is full.



Leaky bucket



Leaky Bucket Implementation



Quality of Service (cntd.)

Token Bucket:

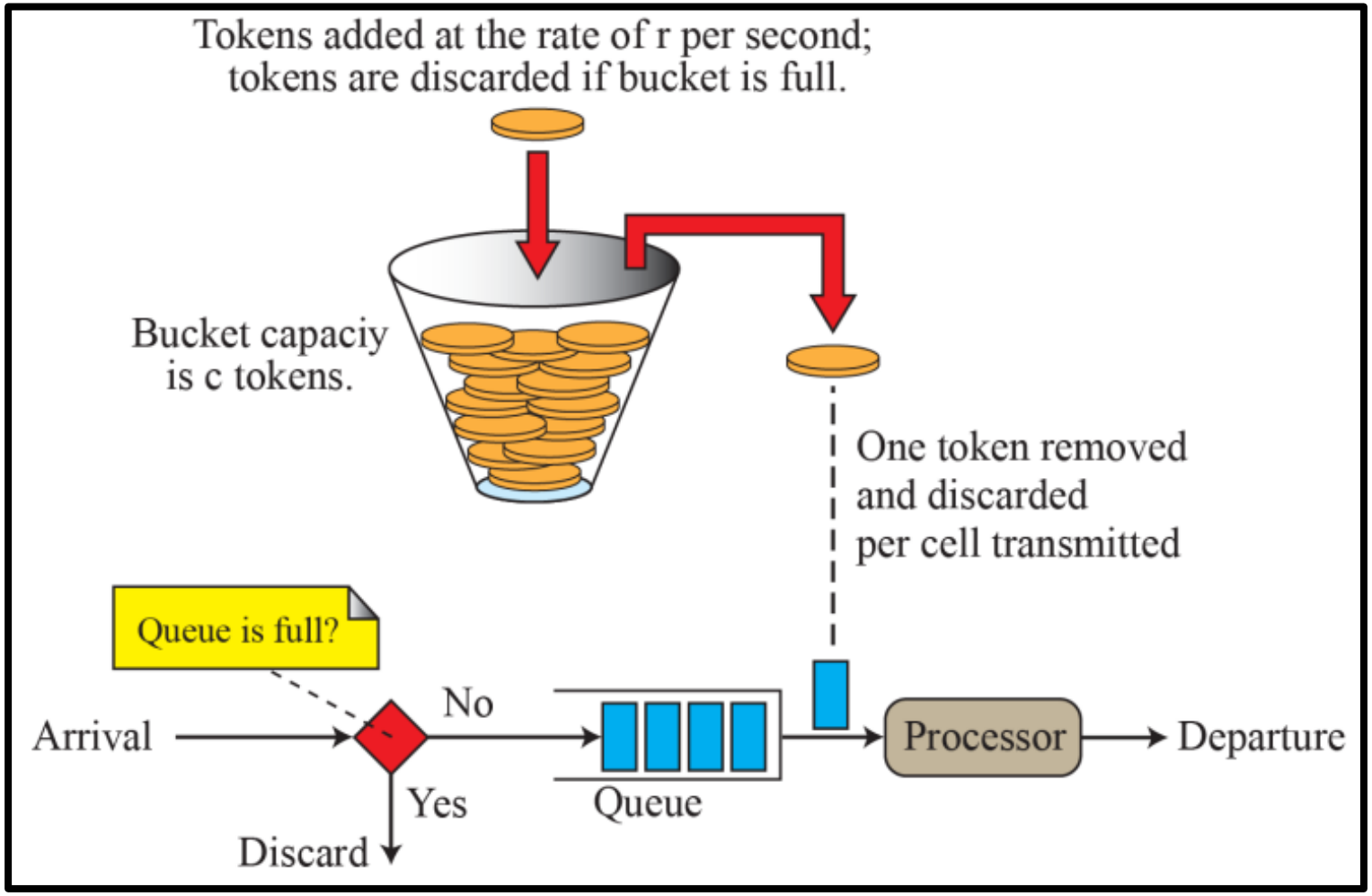
- The leaky bucket is very restrictive. It does not credit an idle host.
- Eg: if a host is not sending for a while, its bucket becomes empty.
- The token bucket algorithm allows idle hosts to accumulate credit for the future in the form of tokens.
- The maximum number of cells that can enter the network during any time interval of length t is shown below.
- The maximum average rate for the token bucket is shown below.

✓ Maximum number of packets = rt + c
✓ Maximum average rate = (rt + c)/t packets per second

➢ 'C' Tokens → capacity of the token bucket is c tokens
➢ 'r' → no.of of tokens entering the bucket per second.

Quality of Service (cntd.)

- The Token bucket allows bursty traffic at a regulated maximum rate.



QoS Service Models

- Administrators use three models to manage their network traffic:

i. Integrated Service(IntServ)

ii. Differentiated Service (DiffServ)

iii. Best Effort(least common)

Integrated Services (IntServ)

- To provide different QoS for different applications, IETF developed the integrated services (IntServ) model.
  - (IETF → Internet Engineering Task Force is a standards organization for the Internet and is responsible for the technical standards that make up the Internet protocol suite.)
- In this model, which is a flow-based architecture, resources such as bandwidth are explicitly reserved for a given data flow.
- In other words, the model is considered a specific requirement of an application in one particular case regardless of the application type (data transfer, or voice over IP, or video-on-demand).
- What is important are the resources the application needs, not what the application is doing.

Integrated Services (IntServ)

- *The model is based on three schemes:*

1. The packets are first classified according to the service they require.
2. The model uses scheduling to forward the packets according to their flow characteristics.
3. Devices like routers use admission control to determine if the device has the capability (available resources to handle the flow) before making a commitment.
   - *Eg:- if an application requires a very high data rate, but a router in the path cannot provide such a data rate, it denies the admission.*

- Integrated Services is a flow-based QoS model designed for IP.
- In this model packets are marked by routers according to flow characteristics.

Integrated Services (IntServ)

- **Resource Reservation Protocol (RSVP)**
- In the IntServ model, an application uses a signaling protocol (Resource Reservation Protocol (RSVP))to notify the network of its traffic parameters and apply for a specific level of QoS before sending packets.
- The RSVP protocol reserves resources such as bandwidth and priority on a known path, and each network element along the path must reserve required resources for data flows requiring QoS guarantee.

Integrated Services (IntServ)

Flow Specification:

- IntServ is flow-based.
- To define a specific flow, a source needs to define a flow specification, which is made of two parts:

1. Rspec (resource specification): Rspec defines the resource that the flow needs to reserve (buffer, bandwidth, etc.).
2. Tspec (traffic specification): Tspec defines the traffic characterization of the flow.
   - bustiness in the traffic → Delay, Jitter, etc.....
   - Traffic shaping & policing

Integrated Services (IntServ)

Admission:

- After a router receives the flow specification from an application, it decides to admit or deny the service.
- The decision is based on the previous commitments of the router and the current availability of the resource.

Integrated Services (IntServ)

Service Classes:

- **Two classes of services have been defined for Integrated Services:**
  - **i. Guaranteed service &**
  - **ii. Controlled-load service.**

Integrated Services (IntServ)

Guaranteed Service Class:

- This type of service is designed for real-time traffic that needs a guaranteed minimum end-to-end delay.
- This type of service guarantees that the packets will arrive within a certain delivery time and are not discarded if flow traffic stays within the boundary of Tspec.
- We can say that guaranteed services are Quantitative Services, in which the amount of end-to-end delay and the data rate must be defined by the application.
- Eg: - Normally guaranteed services are required for real-time applications (voice over IP).

Integrated Services (IntServ)

Controlled-Load Service Class:

- This type of service is designed for applications that can accept some delays but are sensitive to an overloaded network and to the danger of losing packets.
- Eg: file transfer, e-mail, and Internet access.
- The controlled load service is a Qualitative Service in that the application requests the possibility of low-loss or no-loss packets.

PROTOCOL LAYERING

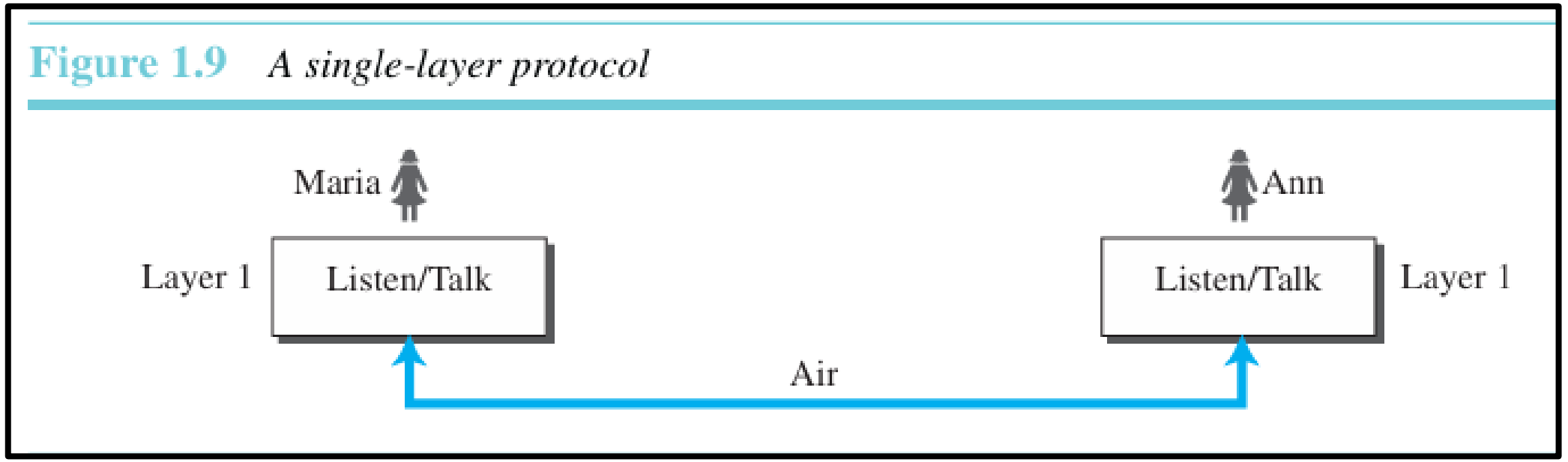
PROTOCOL LAYERING

Protocol

- A protocol defines the Rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively.
- When communication is simple, we may need only one simple protocol;
- when the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or protocol layering.

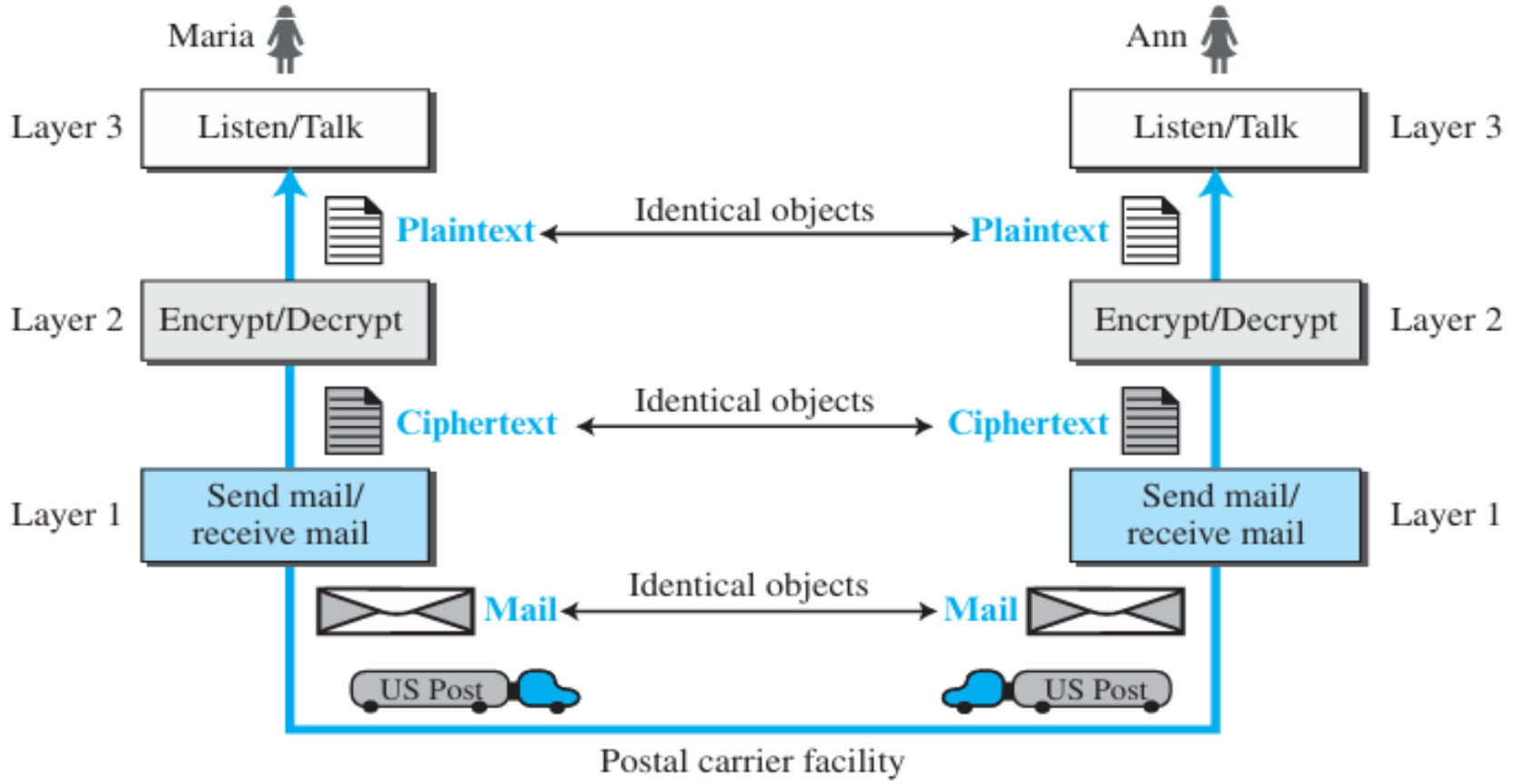
First Scenario :

- **In the first scenario, communication is so simple that it can occur in only one layer.**



Second Scenario

Figure 1.10 *A three-layer protocol*



- Protocol layering enables us to divide a complex task into several smaller and simpler tasks.

Advantages

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

ii. A layer needs to be able to receive a set of services from the lower layer and to give the services to the upper layer; we don't care about how the layer is implemented.

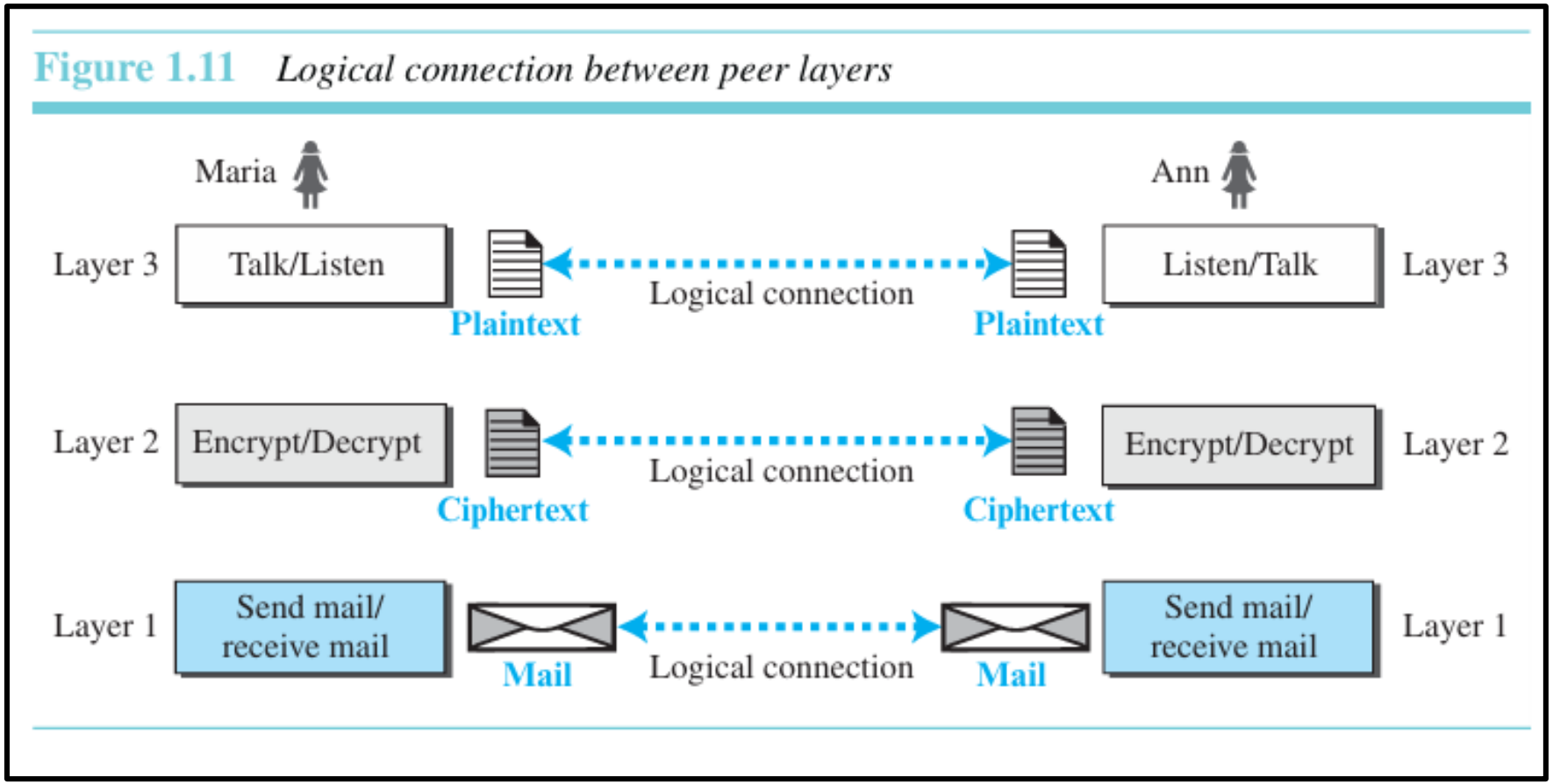
iii. Communication does not always use only two end systems; there are intermediate systems that need only some layers, but not all layers.

- If we did not use protocol layering, we would have to make each intermediate system as complex as the end systems, which makes the whole system more expensive.

Principles of Protocol Layering

1. if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction.
   - Eg:- third layer task is to listen (in one direction) and talk (in the other direction).
   - The second layer needs to be able to encrypt and decrypt.
   - The first layer needs to send and receive mail.
2. Two objects under each layer at both sites should be identical.
   - Eg:- the object under layer 3 at both sites should be a plaintext letter.
   - The object under layer 2 at both sites should be a ciphertext letter.
   - The object under layer 1 at both sites should be a piece of mail.

Logical Connection



After following the above two principles, we can think about logical connection between each layer as shown in Figure. This means that we have layer-to-layer communication.

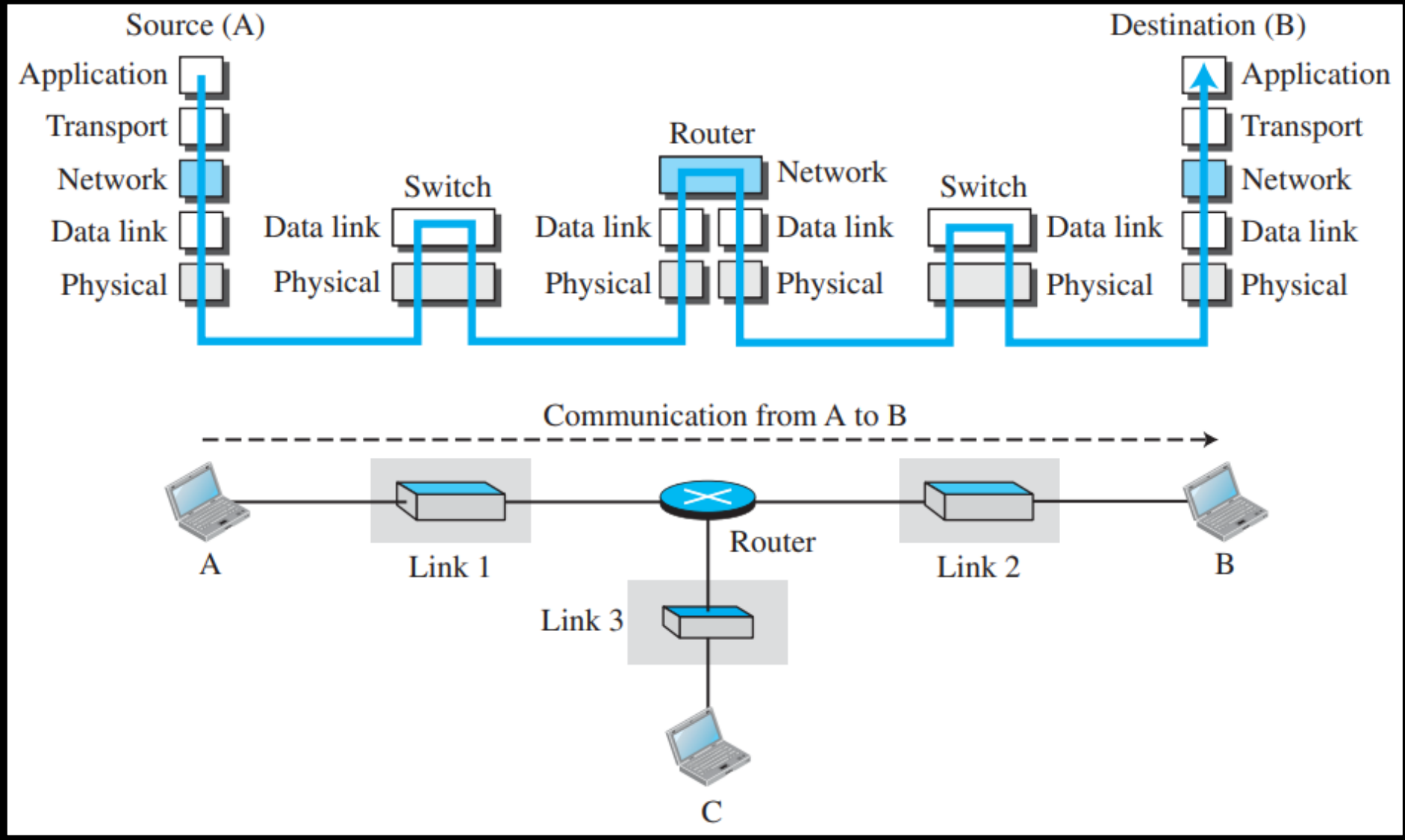
PROTOCOL LAYERING:

1. TCP/IP Protocol Suite
2. OSI Model

TCP/IP Protocol Suite

- TCP/IP is a protocol suite used in the Internet today.
  - 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.
- The original TCP/IP protocol suite was defined as four software layers built upon the hardware.
- Today, however, TCP/IP is thought of as a five-layer model.

Communication through an Internet



Communication through an Internet:

- Computer A communicates with computer B.
- As the figure shows, we have five communicating devices in this communication: source host (computer A), the link-layer switch in link 1, the router, the link-layer switch in link 2, and the destination host (computer B).
- 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;
- Source host needs to create a message in the application layer and send it down the layers so that it is physically sent to the destination host.
- The destination host needs to receive the communication at the physical layer and then deliver it through the other layers to the application layer.

- The router is involved only in three layers;
- there is no transport or application layer in a router as long as the router is used only for routing. Although a router is always involved in one network layer, it is involved in 'n' combinations of link and physical layers;
  - 'n' →number of links the router is connected to.
- The reason is that each link may use its own data-link or physical protocol.
- Eg:- in the above figure, the router is involved in three links, but the message sent from source A to destination B is involved in two links.
- Each link may be using different link-layer and physical-layer protocols;
- Router needs to receive a packet from link 1 based on one pair of protocols and deliver it to link 2 based on another pair of protocols.
- A link-layer switch in a link, however, is involved only in two layers, data-link and physical. Since the connections are in the same link, which uses only one set of protocols.

TCP/IP Protocol Suite

- TCP and IP are different protocols of Computer Networks.
- The basic difference between TCP (Transmission Control Protocol) and IP (Internet Protocol) is in the transmission of data.
- IP→ finds the destination of the mail and
- TCP → has the work to send and receive the mail.

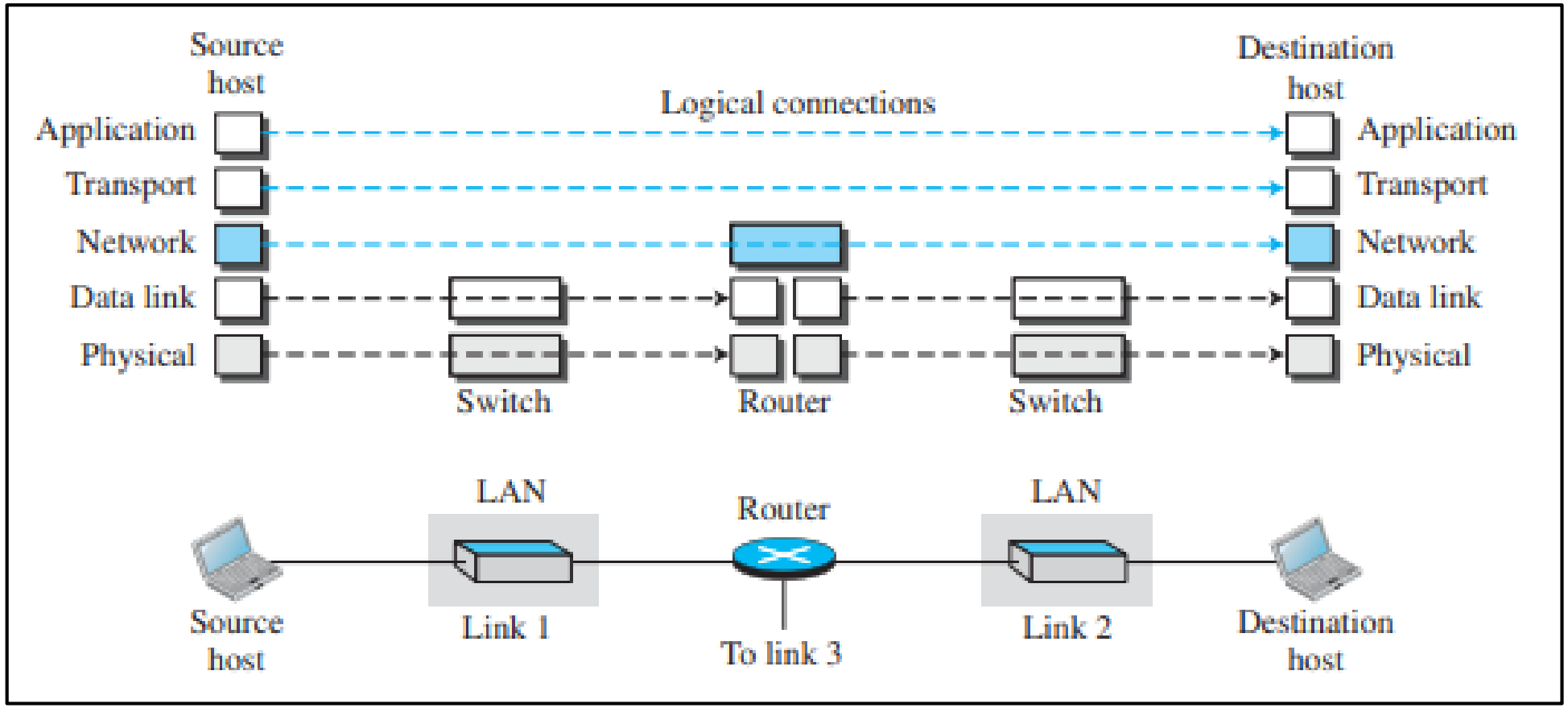
Layers of TCP/IP Model

- Application Layer
- Transport Layer(TCP/UDP)
- Network/Internet Layer(IP)
- Data Link Layer (MAC)
- Physical Layer

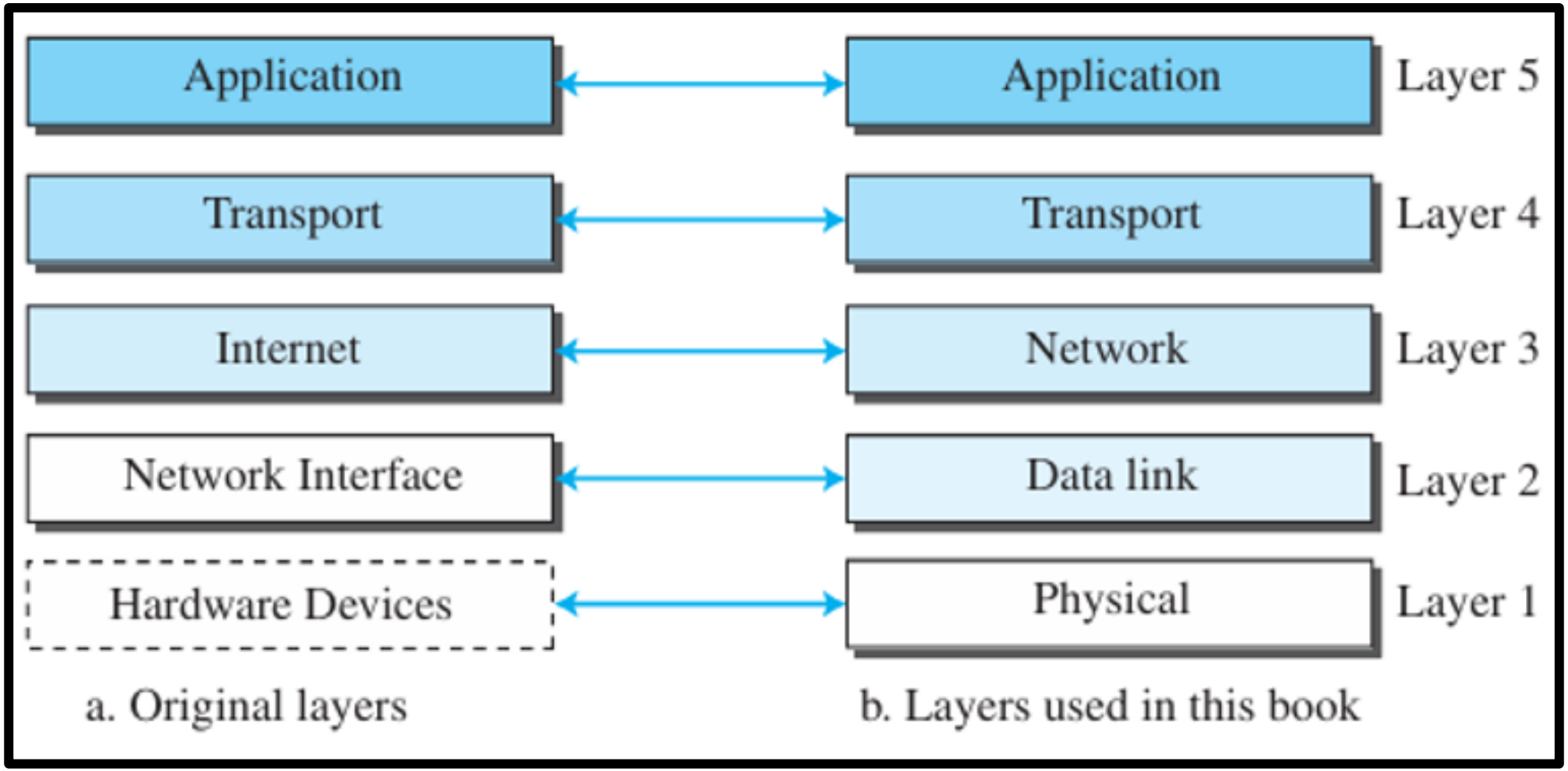
Layers in the TCP/IP Protocol Suite

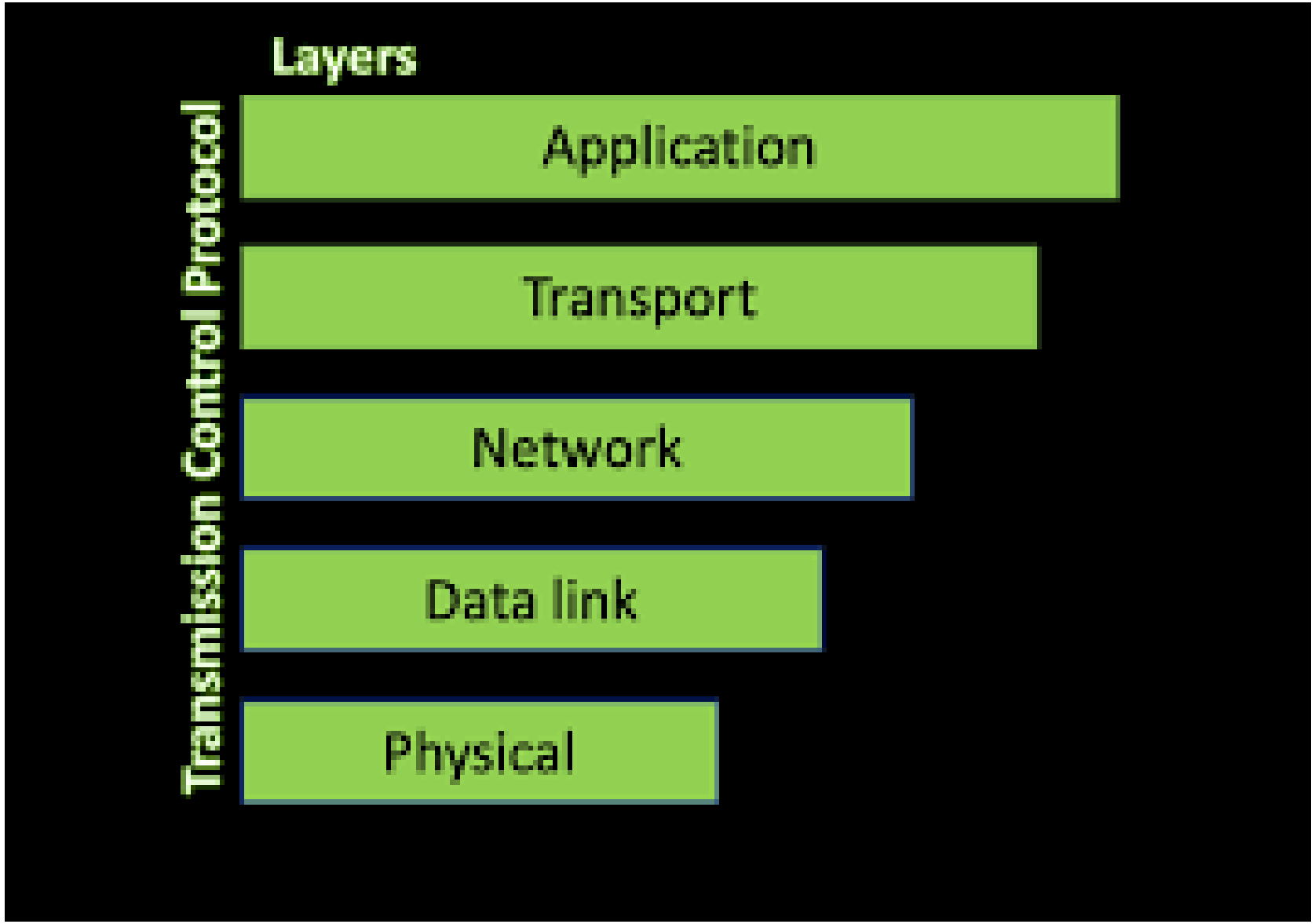
- Logical connections is between layers of the TCP/IP protocol suite.
- Using logical connections makes it easier for us to think about the duty of each layer.
- Duty of the application, transport, and network layers is end-to-end.
- Duty of the data-link and physical layers is hop-to-hop, in which a hop is a host or router.
- In other words, the domain of duty of the top three layers is the internet, and the domain of duty of the two lower layers is the link.
- In the top three layers, the data unit (packets) should not be changed by any router or link-layer switch.
- In the bottom two layers, the packet created by the host is changed only by the routers, not by the link-layer switches.

Logical connections between layers of the TCP/IP protocol suite

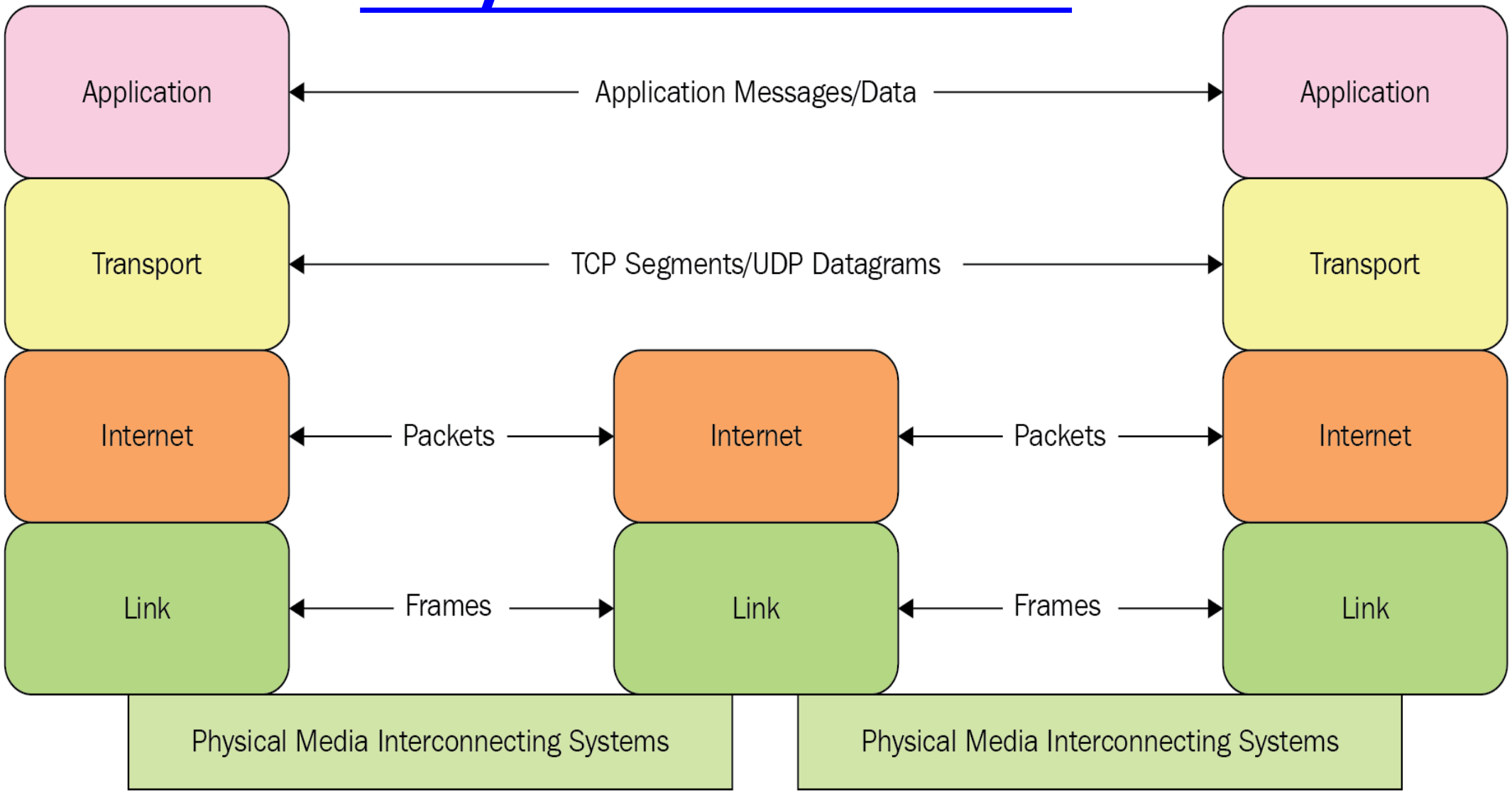


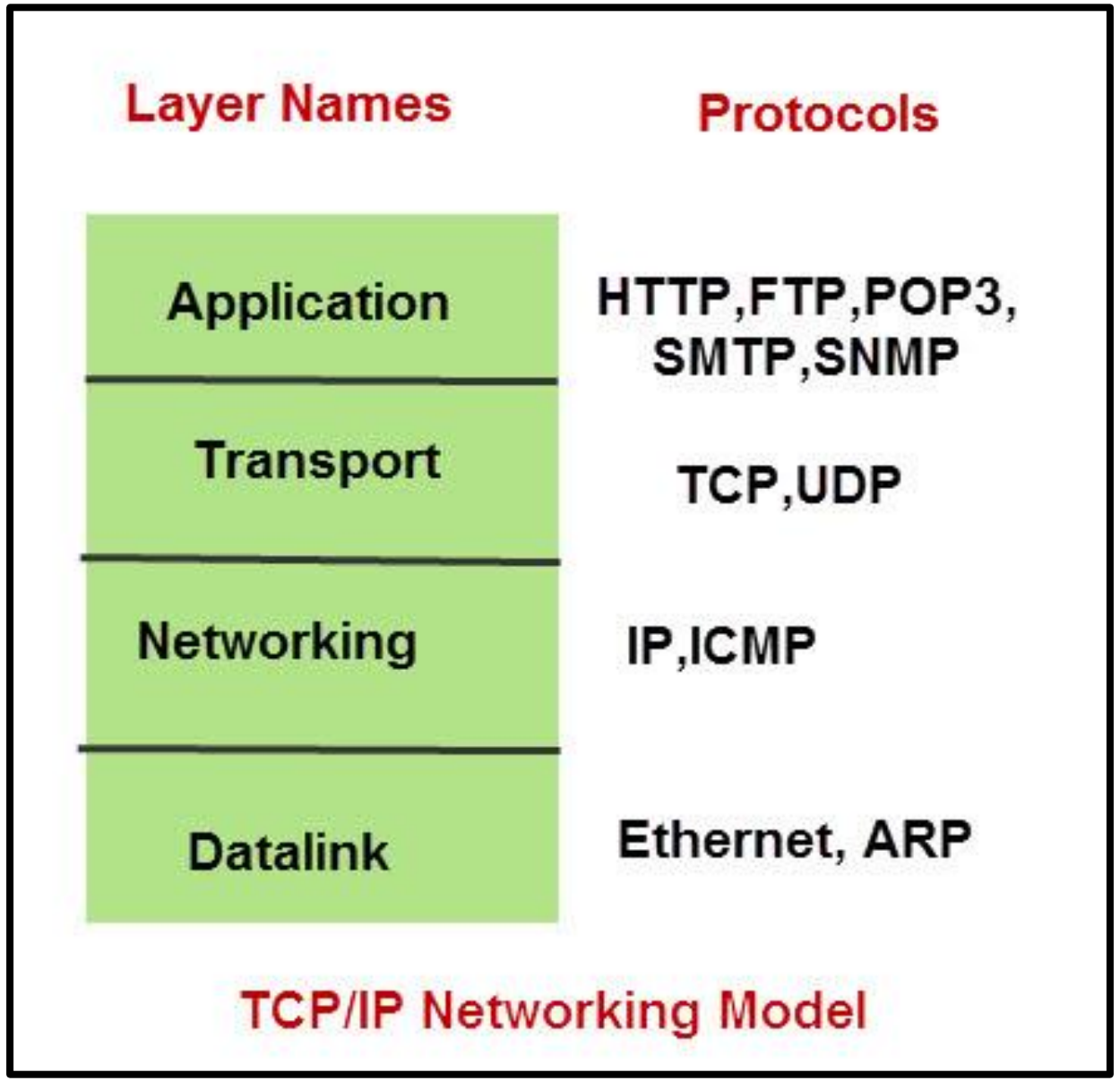
TCP/IP Protocol Suite




Layers
Transmission Control Protocol
Application
Transport
Network
Data link
Physical

TCP/IP Protocol Suite




Layer Names
Protocols
Application
HTTP,FTP,POP3,
SMTP,SNMP
Transport
TCP,UDP
Networking
IP,ICMP
Datalink
Ethernet, ARP
TCP/IP Networking Model

Application Layer

- The two application layers exchange messages between each other as though there were a bridge between the two layers.
- However, we should know that the communication is done through all the layers.
- 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.
- The application layer in the Internet includes many predefined protocols, but a user can also create a pair of processes to be run at the two hosts.

Application Layer

Application layer in the internet includes many predefined protocols:

i. Hypertext Transfer Protocol (HTTP) is a vehicle for accessing the World Wide Web(WWW).

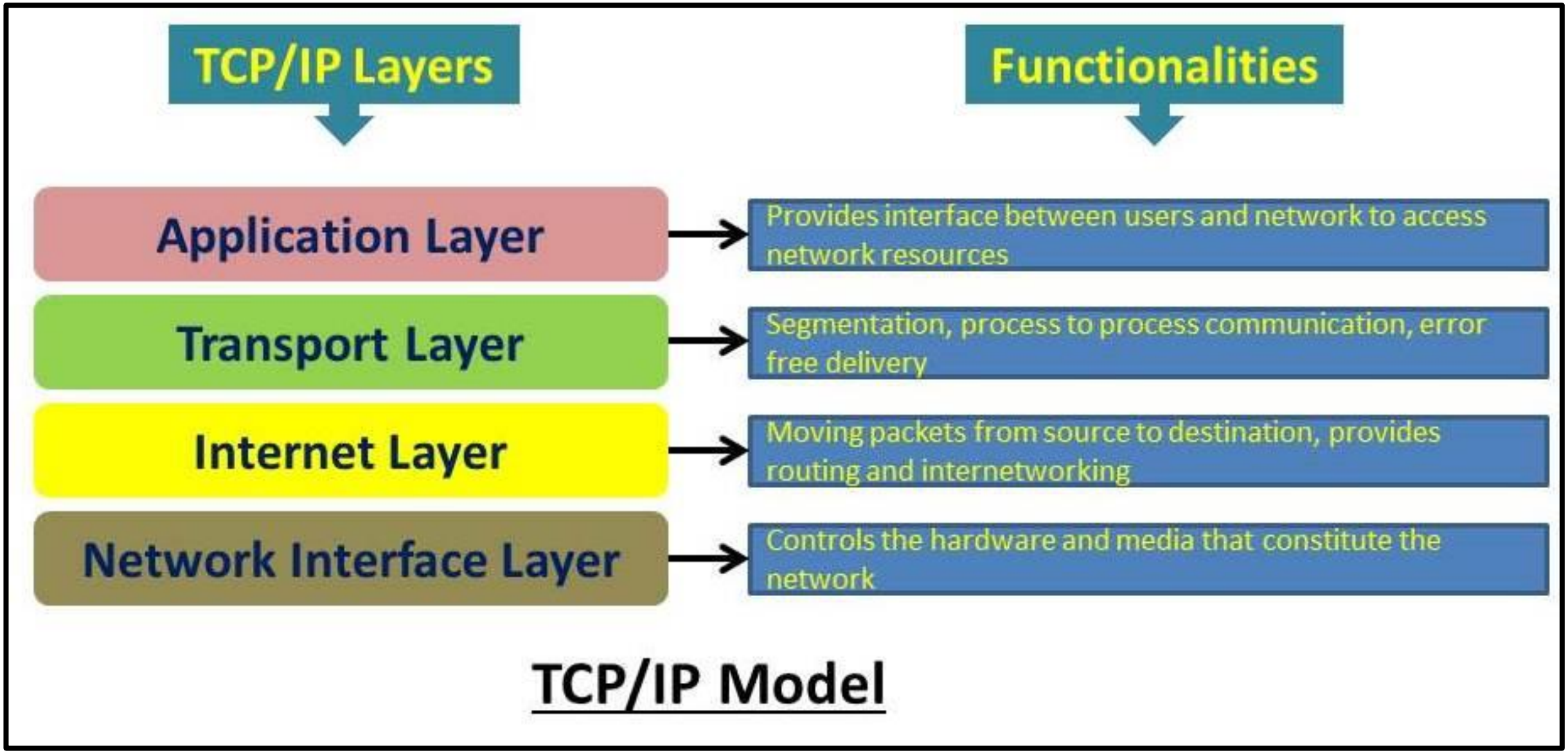
ii. Simple Mail Transfer Protocol (SMTP) is the main protocol used in electronic mail (e-mail) service.

iii. File Transfer Protocol (FTP) is used for transferring files from one host to another.

iv. Terminal Network (TELNET) and Secure Shell (SSH) are used for accessing a site remotely.

v. Simple Network Management Protocol (SNMP) is used by an administrator to manage the Internet at global and local levels.

vi. Domain Name System (DNS) is used by other protocols to find the network-layer address of a computer.


TCP/IP Layers
Functionalities
Application Layer
Provides interface between users and network to access network resources
Transport Layer
Segmentation, process to process communication, error free delivery
Internet Layer
Moving packets from source to destination, provides routing and internetworking
Network Interface Layer
Controls the hardware and media that constitute the network
TCP/IP Model

Transport Layer

- The logical connection at the transport layer is also end-to-end.
- The transport layer at the source host gets the message from the application layer, encapsulates it in a transport layer packet (called a segment or a user datagram in different protocols) and sends it, through the logical (imaginary) connection, to the transport layer at the destination host.
- In other words, the transport layer is responsible for giving services to the application layer: to get a message from an application program running on the source host and deliver it to the corresponding application program on the destination host.
- More than one protocol in the transport layer, which means that each application program can use the protocol that best matches its requirement.
- Transport Layer protocols are TCP,UDP and SCTP.

Transport Layer(cntd.)

TCP - -Transmission Control Protocol:

- TCP is a connection-oriented protocol - It first establishes a logical connection between transport layers at two hosts before transferring data.
- It creates a logical pipe between two TCPs for transferring a stream of bytes.
- TCP divides a stream of data into smaller units called segments. Each segments include sequence number for reordering after receipt. If an error occurs data is retransmitted.
- TCP is configured more for reliability than for speed.
- TCP provides flow control, error control and congestion control to reduce the loss of segments due to congestion in the network.
- Applications that use TCP are WWW,Email,File transfer

Transport Layer(cntd.)

- **UDP-User Datagram Protocol :**
  - Connectionless protocol
  - Transmits user datagrams without first creating a logical connection.
  - In UDP, each user datagram is an independent entity without being related to the previous or the next one
  - UDP is a simple protocol.
  - does not provide flow, error, or congestion control.
  - Unreliable
  - No retransmission of the packets involved in TCP, when a packet is corrupted or lost.
  - UDP is designed more for speed than reliability.
  - Common uses for UDP are Streaming media, VoIP(voice over internet),online games.

Transport Layer(cntd.)

SCTP → Stream Control Transmission Protocol:

- Designed to respond to new applications that are emerging in the multimedia.
- SCTP Provides features of both TCP and UDP protocols .
- SCTP is message or datagram orientated like UDP but it also ensures reliable sequential transport
- t of data with congestion control like TCP.

Network Layer

- The network layer is responsible for creating a connection between the source computer and the destination computer.
- The communication at the network layer is host-to-host.
- There can be several routers from the source to the destination, the routers in the path are responsible for choosing the best route for each packet.
- Responsible for host-to-host communication and routing the packet through possible routes.
- Protocols in the network layer are: IP, ICMP, IGMP, DHCP, ARP.

Network Layer(cntd.)

- **Internet Protocol (IP):**
- It defines the format of the packet, called a datagram at the network layer.
- IP also defines the format and the structure of addresses used in this layer.
- IP is also responsible for routing a packet from its source to its destination, which is achieved by each router forwarding the datagram to the next router in its path.
- IP is a connectionless protocol.
- Provides no flow control, no error control, and no congestion control services.

Network Layer(cntd.)

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

Data-link Layer

- The data-link layer takes a datagram and encapsulates it in a packet called a frame.
- Data Link Layer is divided into two :
  i. Medium access control layer
  ii. Logic Link Control Layer
- Medium access control layer performs two functions:

a) **Encapsulation:** Receives IP packet, add header and trailer. Header contains MAC address of the sender and receiver. Trailer contains error checking data used to detect errors in the received Ethernet frame. (MAC address is a unique 6 byte address embedded in the NIC of a device by its manufacturer)

b) **Medium Access:** For accessing the media Ethernet uses Carrier Sense Multiple access / Collision Detection or CSMA/CD. In this method each computer listen to the medium before sending data through the network.

Data-link Layer(cntd.)

- **Logic Link Control Layer performs the following functions:**
  - **LLC controls flow control and error control .**
  - **Flow control restricts the amount of data that a sender can send without overwhelming the receiver.**
  - **Error detection and retransmission is done by using the error checking bytes added in the header of the Frame.**
  - **Some link-layer protocols provide complete error detection and correction, some provide only error correction.**

Physical Layer

- Physical layer is responsible for carrying individual bits in a frame across the link.
- Physical layer is the lowest level in the TCP/IP protocol suite, the communication between two devices at the physical layer is still a logical communication because there is another, hidden layer, the transmission media, under the physical layer.
- Two devices are connected by a transmission medium (cable or air), the transmission medium does not carry bits; it carries electrical or optical signals.
- So the bits received in a frame from the data-link layer are transformed and sent through the transmission media, but we can think that the logical unit between two physical layers in two devices is a bit.
- There are several protocols that transform a bit to a signal.

Physical Layer

- *The functions of this layer are:*
  - ➢ It defines how bits are to be encoded into optical or electrical signals.
  - ➢ It states the transmission mode, i.e. simplex, half duplex or full duplex
  - ➢ It states the topology of the network, i.e. bus, star, ring etc.
  - ➢ The protocol in this layer are Ethernet, Token ring, Frame relay and ATM.
- Copper cable passes electrical signals.
- Optical fiber cable passes light signals.
- Radio signals travel in the air/vaccum.
- The most common protocol used at physical layer is Ethernet.