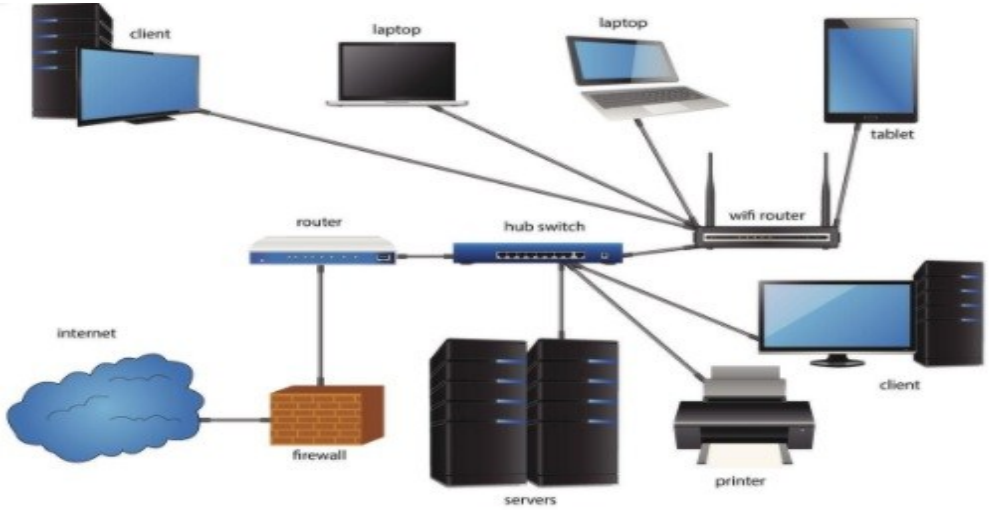
COMPUTER NETWORKS



Instructor: Mr. B. V. Sathish Kumar, Assistant Professor

Department of Electronics and Communication Engineering

Syllabus

UNIT – I

Introduction: Network Topologies WAN, LAN, MAN. Reference models- The OSI Reference Model- the TCP/IP Reference Model - A Comparison of the OSI and TCP/IP Reference Models

UNIT – II

Physical Layer – Fourier Analysis – Bandwidth Limited Signals – The Maximum Data Rate of a Channel – Guided Transmission Media, Digital Modulation and Multiplexing: Frequency Division Multiplexing, Time Division Multiplexing, Code Division Multiplexing Data Link Layer Design Issues, Error Detection and Correction, Elementary Data Link Protocols, Sliding Window Protocols

UNIT – III

The Data Link Layer - Services Provided to the Network Layer – Framing – Error Control – Flow Control, Error Detection and Correction – Error-Correcting Codes – Error Detecting Codes, Elementary Data Link Protocols- A Utopian Simplex Protocol-A Simplex Stop and Wait Protocol for an Error free channel-A Simplex Stop and Wait Protocol for a Noisy Channel, Sliding Window Protocols-A One Bit Sliding Window Protocol-A Protocol Using Go-Back-N- A Protocol Using Selective Repeat

UNIT – IV

The Medium Access Control Sublayer-The Channel Allocation Problem-Static Channel Allocation-Assumptions for Dynamic Channel Allocation, Multiple Access Protocols-Aloha-Carrier Sense Multiple Multiple Access Protocols-Collision-Free Protocols-Limited Contention Protocols-Wireless LAN Protocols, Ethernet-Classic Ethernet Physical Layer-Classic Ethernet MAC Sublayer Protocol-Ethernet Performance-Fast Ethernet Gigabit Ethernet-10-Gigabit Ethernet-Retrospective on Ethernet, Wireless Lans-The 802.11 Architecture and Protocol Stack-The 802.11 Physical Layer-The802.11 MAC Sublayer Protocol-The 805.11 Frame Structure-Services

UNIT – V

Design Issues-The Network Layer Design Issues – Store and Forward Packet Switching-Services Provided to the Transport layer- Implementation of Connectionless Service-Implementation of Connection Oriented Service-Comparison of Virtual Circuit and Datagram Networks, Routing Algorithms-The Optimality principle-Shortest

path Algorithm, Congestion Control Algorithms-Approaches to Congestion Control-Traffic Aware Routing-Admission Control-Traffic Throttling-Load Shedding.

UNIT – VI

Transport Layer – The Internet Transport Protocols: UDP, the Internet Transport Protocols: TCP Application Layer –The Domain Name System: The DNS Name Space, Resource Records, Name Servers,

Electronic Mail: Architecture and Services, The User Agent, Message Formats, Message Transfer, Final Delivery

TEXT BOOKS:

1. Computer Networks, Tanenbaum and David J Wetherall, 5th Edition, Pearson Edu, 2010

2. Computer Networks: A Top Down Approach, Behrouz A. Forouzan, Firouz Mosharraf, McGraw Hill Education

UNIT-I

INTRODUCTION TO COMPUTER NETWORKS

What is a computer Network ?

- A network is group of systems interconnected with each other to exchange information.
- A computer network is collection of autonomous computers interconnected in a single technology.
- Two computers are said to interconnected with each other if they share some information between them.

History

- 18th century was the era of the great mechanical systems accompanying the Industrial Revolution.
- The 19th century was the age of the steam engine.
- During the 20th century, the key technology was information gathering, processing, and distribution.
- Among other developments, we saw the installation of worldwide telephone networks, the invention of radio and television, the birth and unprecedented growth of the computer industry, the launching of communication satellites, and, of course, the Internet.
- As a result of rapid technological progress, these areas are rapidly converging In the 21st century and the differences between collecting, transporting, storing, and processing information are quickly disappearing.

- During the first two decades of their existence, computer systems were highly centralized, usually within a single large room.
- A medium-sized company or university might have had one or two computers, while very large institutions had at most a few dozen.
- The old model of a single computer serving all of the organization's computational needs has been replaced by one in which a large number of separate but interconnected computers do the job.
- These systems are called **computer networks**

Advantages

1. Increased communication capabilities.

2. **File sharing:** Network offer quick and easy way to share files directly at a rapid speed thus saving time and integrity of files.

3. **Resouce sharing** : All computers in a network can share resources like printer, scanner, modem, fax machines, hard disk.

4. **Security:** Specific directories can be password protected to limit access to authorized users. Also, files and programs on a network can be designated as "copy inhibit" so you don't have to worry about the illegal copying of programs.

5. It is also possible to share data files across the network by creating a share on the hard drive and allowing other people access to that information.

6. **Internet connection sharing** - Using a home network, multiple family members can access the Internet simultaneously without having to pay an ISP for multiple accounts.

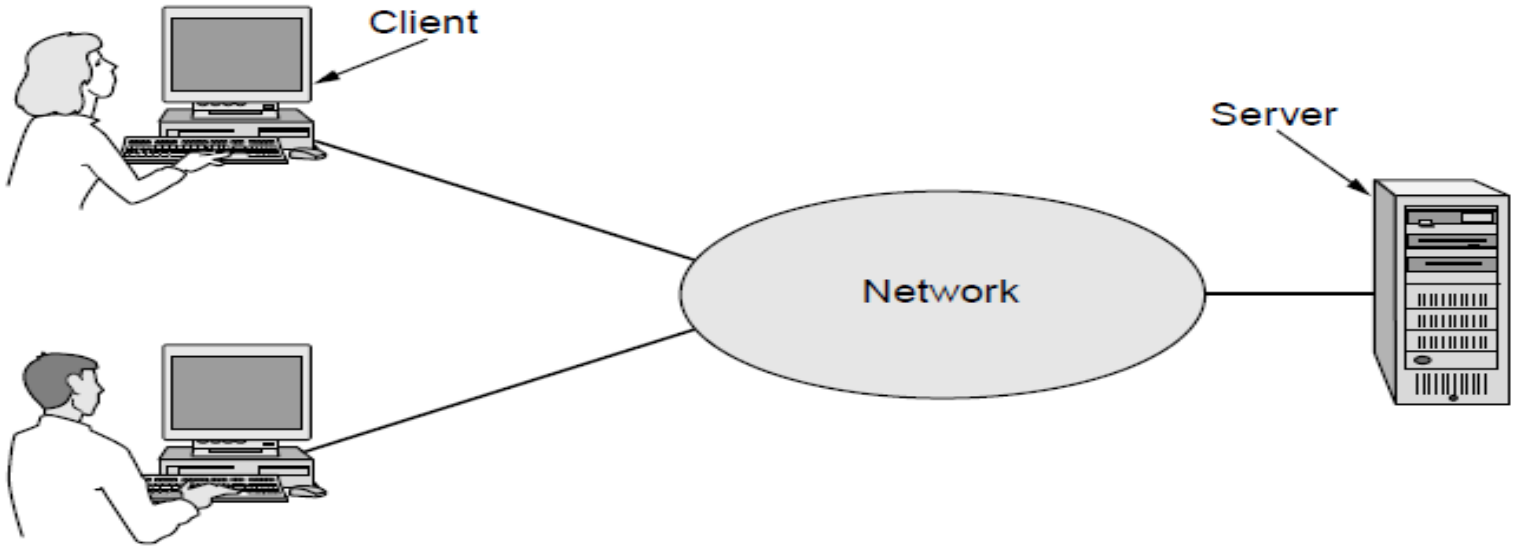
Limitations of Computer Networks

1. Network faults can cause loss of data.
2. Network faults could lead to loss of resources.
3. Systems open to hackers.

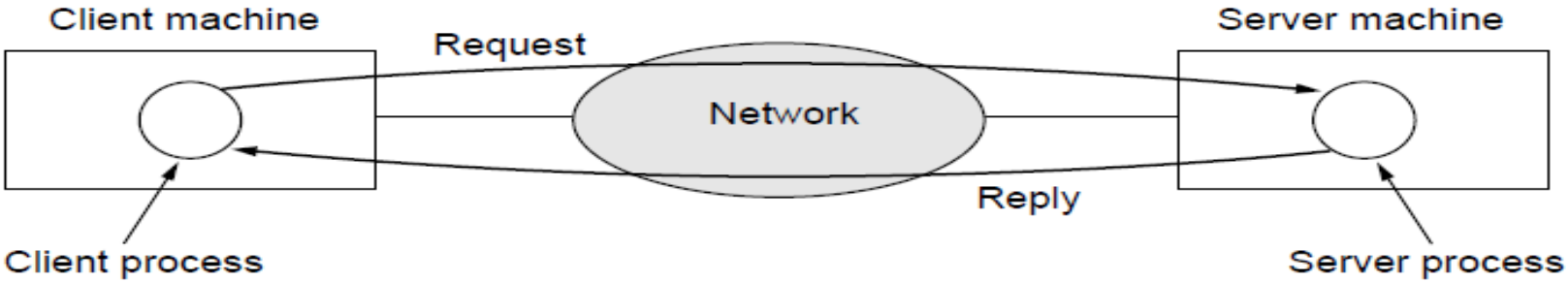
Applications

- Business Applications
- Home Applications
- Mobile Users

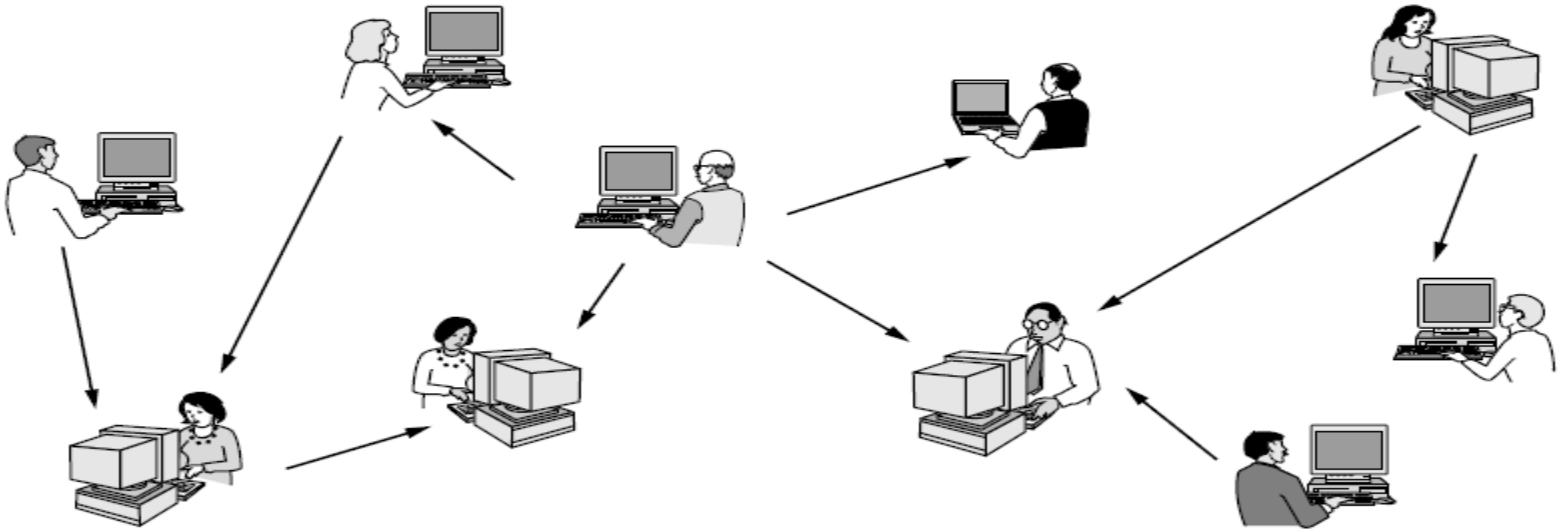
Business Applications



The client-server model involves requests and replies



Home Applications



In a peer-to-peer system there are no fixed clients and servers.

Contd..

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books online
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products online
P2P	Peer-to-peer	Music sharing

Some forms of e-commerce

Mobile Users

Wireless	Mobile	Typical applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in unwired buildings
Yes	Yes	Store inventory with a handheld computer

Combinations of wireless networks and mobile computing

What are the different types of network hardware?

- NIC (Network Interface Card)
- Repeater
- Switch
- Router
- Hub
- Modem
- Server
- Gateways
- Bridges
- Firewall

NIC (Network Interface Card)

- It is also known as LAN card ,Ethernet card, Network/Ethernet adaptor.
- It is an interface between computer and network cables.
- Network Interface Card (NIC) is a hardware unit, which is inbuilt inside a computer provided with a slot, it connects the computer to a computer network for communication with other devices via buses.
- It contains MAC address also called hardware **addresses** or physical **addresses**

FUNCTION OF REPEATERS

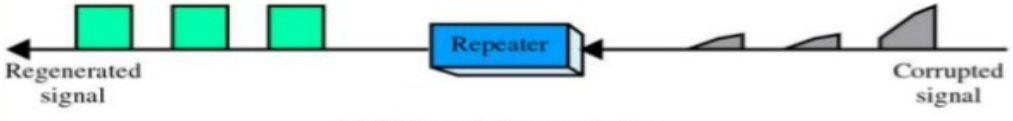
- Repeaters receive signals from one network segment and it regenerates, and retransmit those signals to another network segment.
- When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.
- A repeater can extend only the physical length of network.
- A repeater forwards every frame; it has no filtering capability.

Repeater

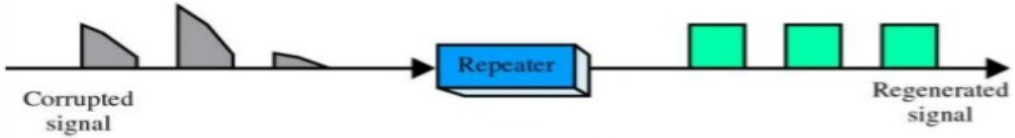
Repeater

Hub

Function of a Repeater



(a) Right-to-left transmission.

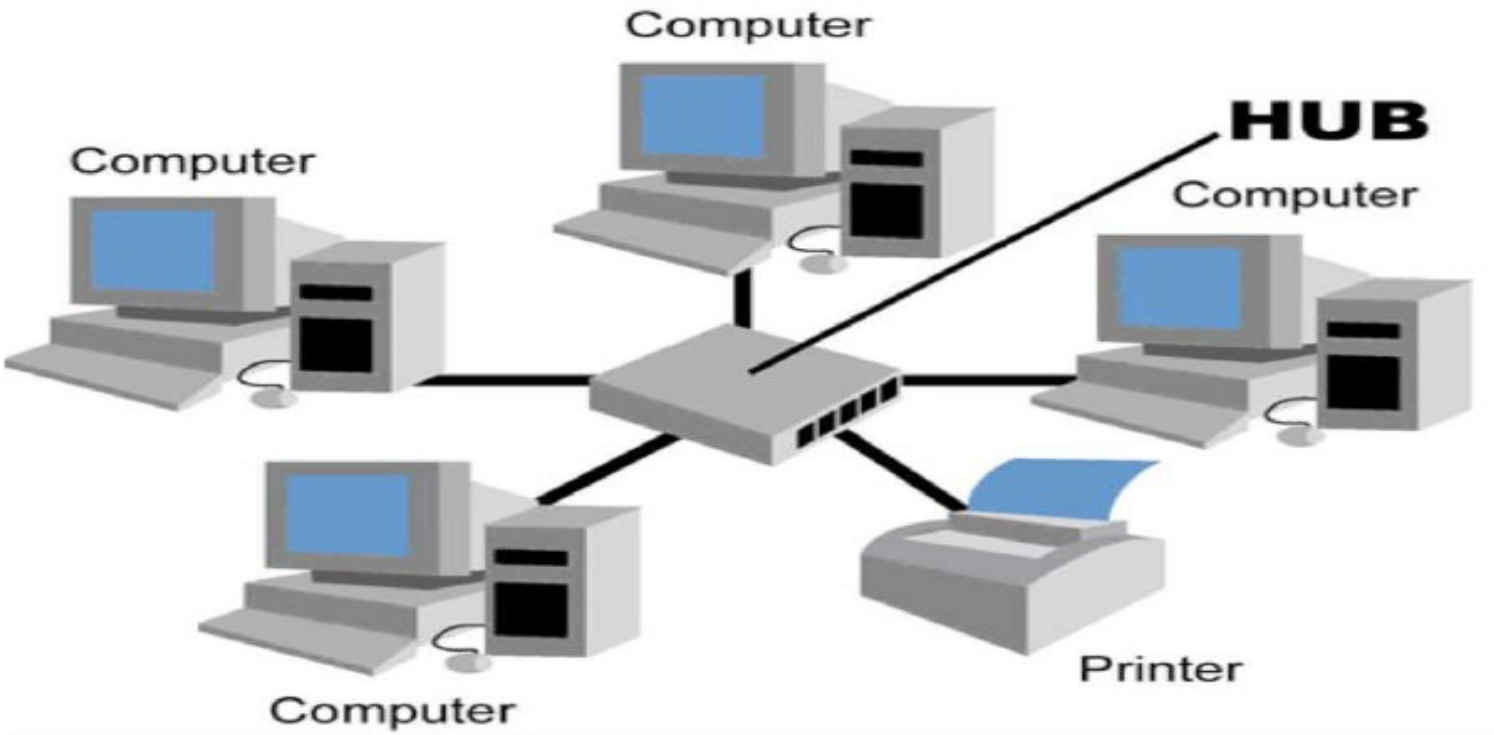


(b) Left-to-right transmission.

HUB

A hub is basically a multiport repeater .

- Hubs are a common connection point for devices in a network and are commonly used to connect segments of a LAN and have multiple ports.
- A hub takes the incoming data packet that comes into a port and copies it out to all the other ports in the hub.
- It doesn't perform any filtering or redirection of data.
- It operates on physical layer of OSI model.
- Hub is “Half-duplex“(can receive or forward only)

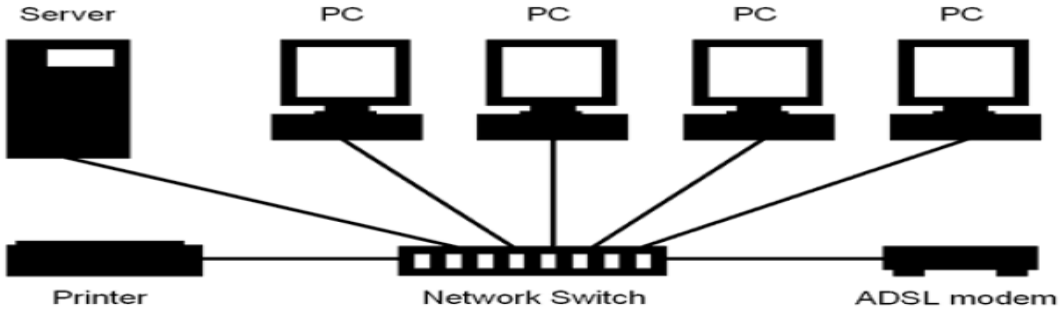

Computer
HUB
Computer
Computer
Computer
Computer
Printer

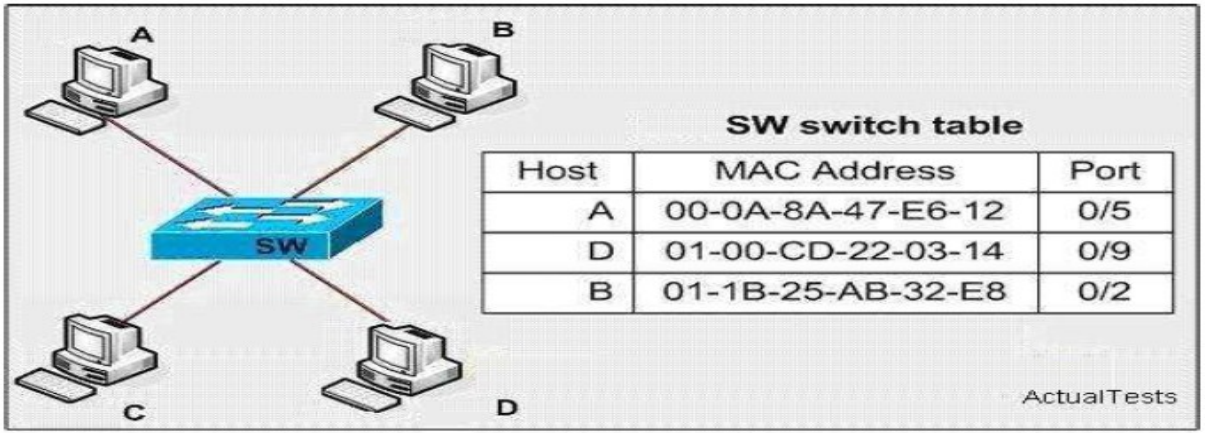
Switches

A network switch is a networking device that connects devices together on a computer networks, by using packet switching to receive, process and forward data to the destination device.

- **A switch is a device which connects various systems in a network.**
- **Switch maintains MAC address table.**
- **Packets are directly transferred to the destination without broadcasting.**
- **Switch is considered as an intelligent device.**
- **Can operates in Full-duplex mode(can send and receive frames at the same time)**

SWITCHES


Server
PC
PC
PC
PC
Printer
Network Switch
ADSL modem

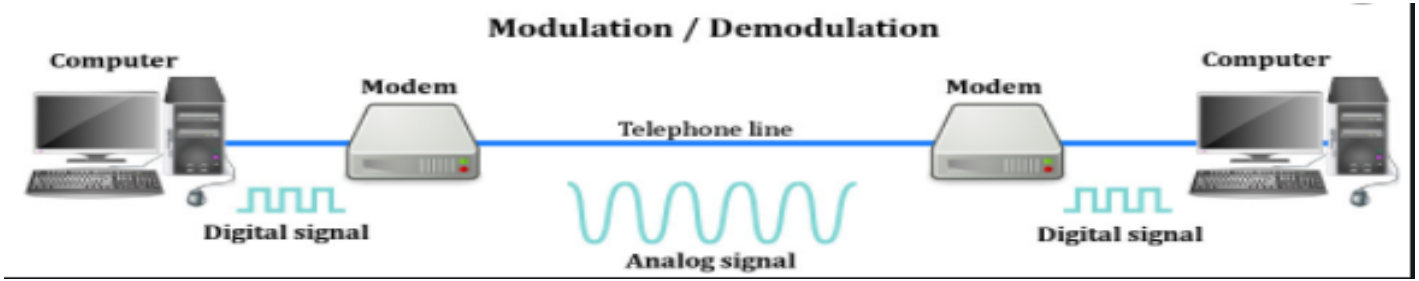

A
B
SW
C
D
SW switch table
Host
MAC Address
Port
A
00-0A-8A-47-E6-12
0/5
D
01-00-CD-22-03-14
0/9
B
01-1B-25-AB-32-E8
0/2
ActualTests

Router

- A router is a device, which enables communication between two different networks or enables communication between two different series/classes of network.
- A router is a internetworking device.
- A router is responsible for routing the data packets towards their destination.

MODEM

- **Modem** is a device that enables a **computer** to send or receive data over telephone or cable lines.
- The data stored on the **computer** is digital whereas a telephone line or cable wire can transmit only analog data.
- The main function of the **modem** is to convert digital signal into analog and vice versa.



NETWORK CATEGORIES

The computer networks are classified based on two factors

(i) Transmission Technology

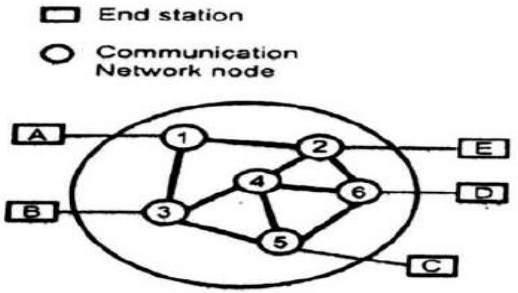
(ii) Scale(Size of the Network)

Based on the transmission technology

- Point to Point networks
- Broadcast networks(Multipoint Networks)

Point –to- Point Networks

- Point-to-point links connect individual pairs of machines. To go from the source to the destination on a network made up of point-to-point links, short messages, called **packets** in certain contexts, may have to first visit one or more intermediate machines.
- Often multiple routes, of different lengths, are possible, so finding good ones is important in point-to-point networks.
- Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called **unicasting**.



Communication network based on Point-to-Point Communication

Broadcast Networks

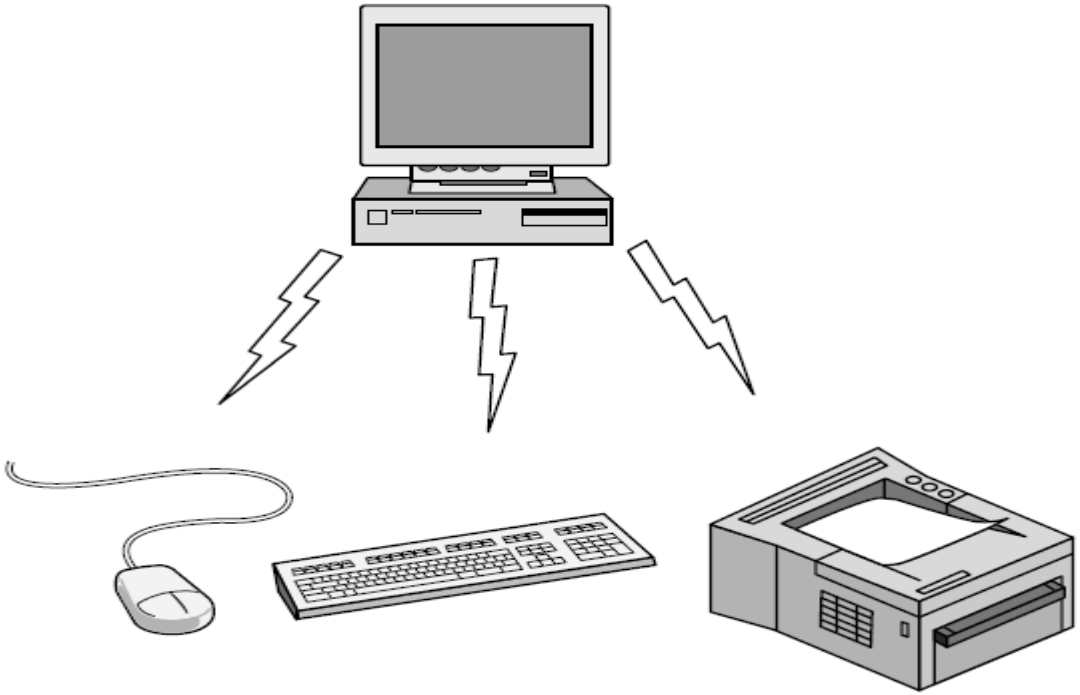
- On a broadcast network, the communication channel is shared by all the machines on the network; packets sent by any machine are received by all the others.
- An address field within each packet specifies the intended recipient.
- Upon receiving a packet, a machine checks the address field.
- If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.

Fig 1.1 Broadcast network based on shared bus

Classification of Computer Networks by scale.

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Personal Area Network



Bluetooth PAN configuration

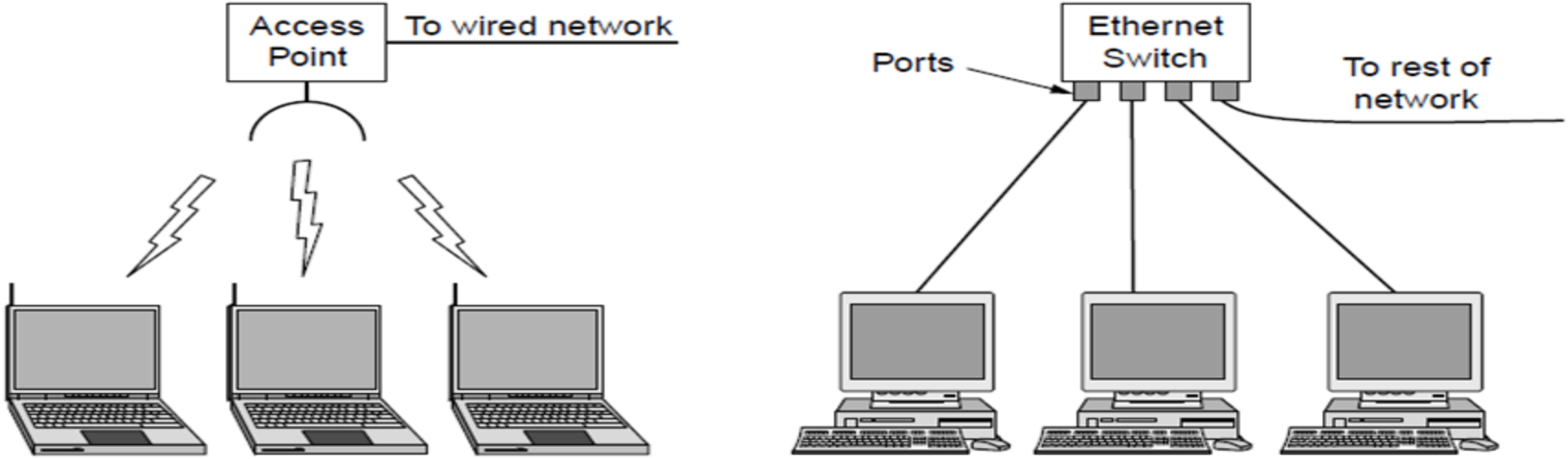
LAN (Local Area Network)

- Privately owned and links the devices in a single office, building or campus
- LANs designed to allow resources to be shared between PCs or workstations. The resources may be H.W (e.g. printer) or S.W (applications program) or data.
- In LANs one of the computers has a large capacity drive and becomes a server to other clients.

Contd..

- S/W stored on server and used as needed by the whole group.
- LAN size determined by licensing restrictions (no of users per copy of S/W)
- LAN use only one type of transmission medium.
- The most common LAN topologies are bus, ring and star.
- Traditionally LAN have data rates in the 4 to 16 Mbps. Today Speed can reach to 100Mbps or 1000MBps(1G).

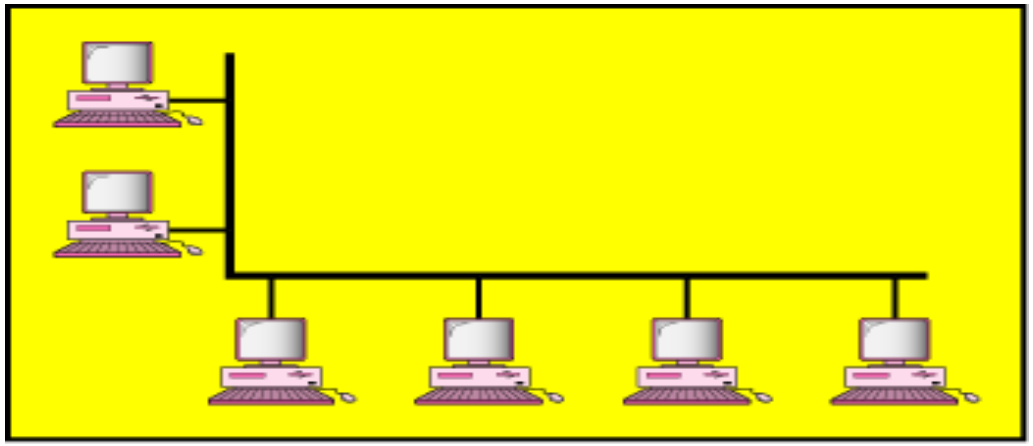
Local Area Networks



Wireless and wired LANs. (a) 802.11. (b) Switched Ethernet.

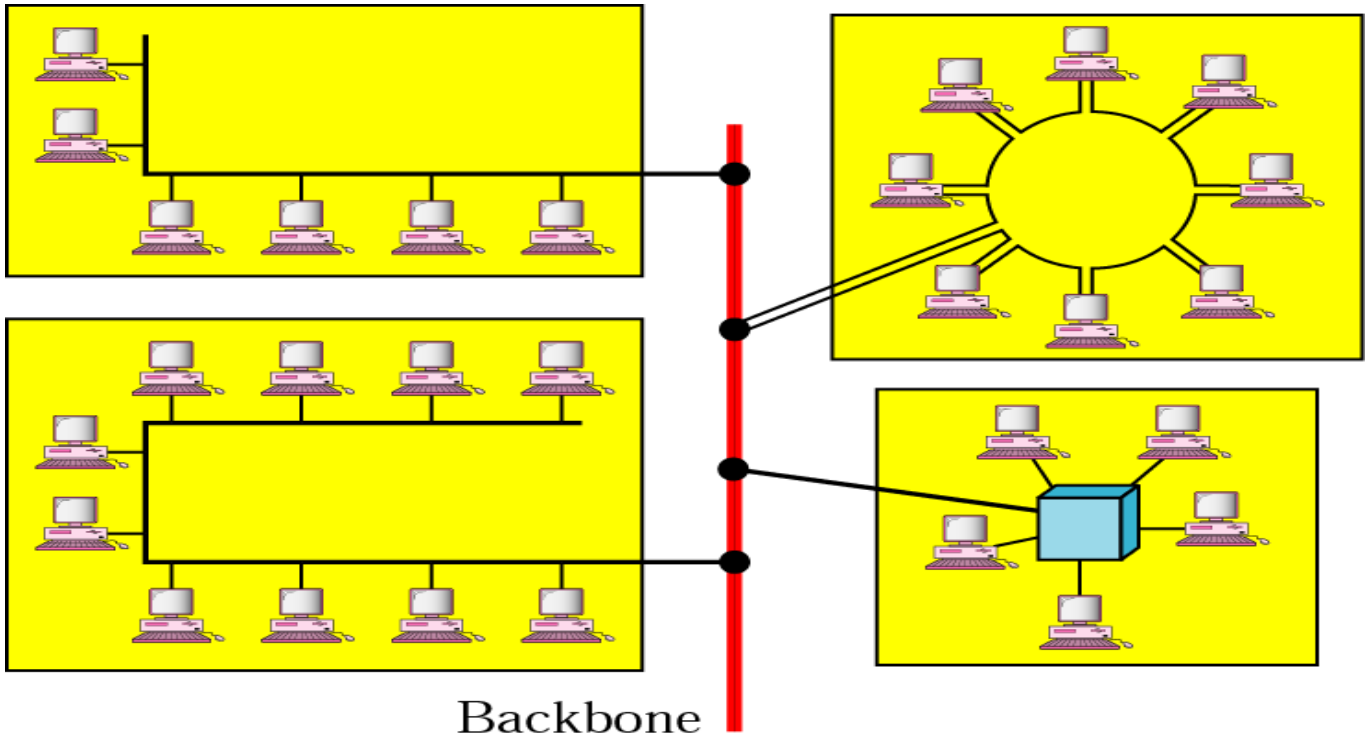
Single-Building LAN

Used in business environments, links a workgroup of task-related computer.



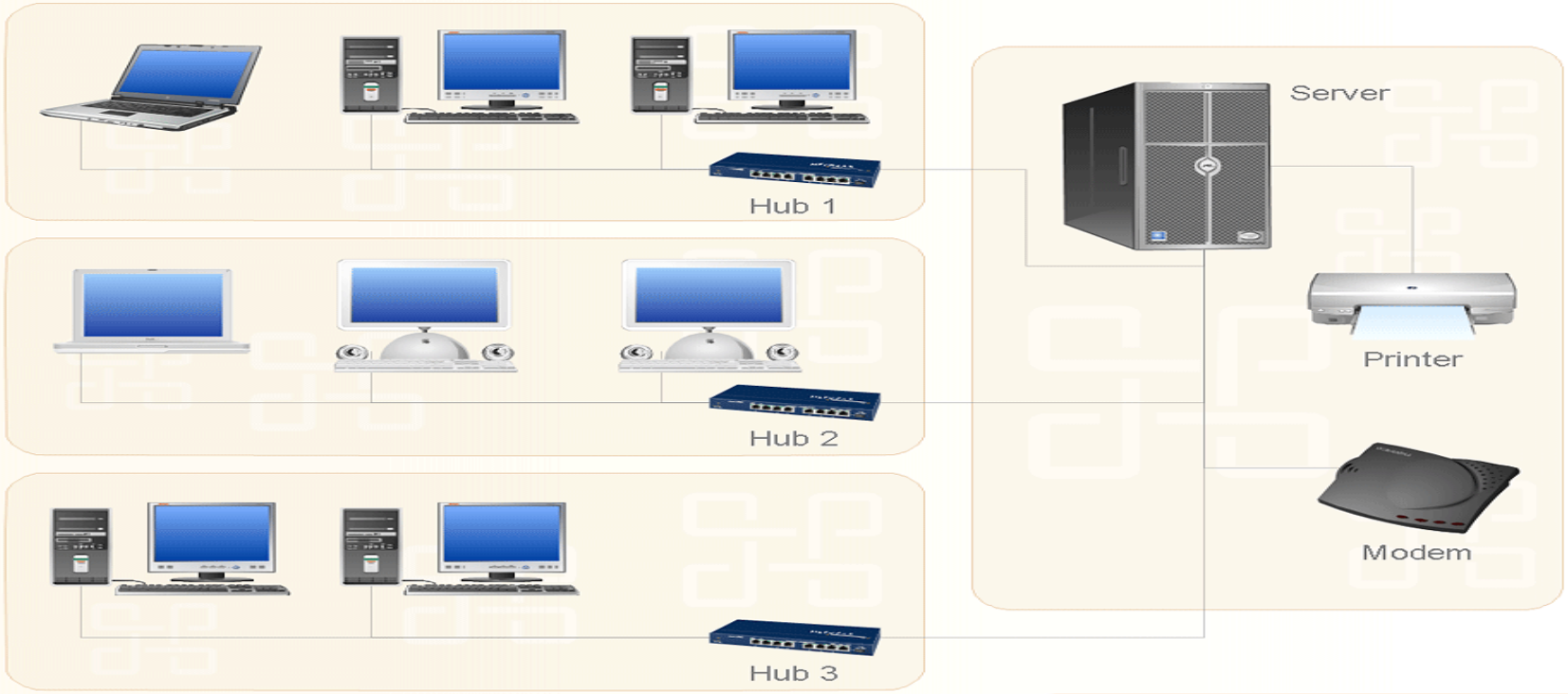
a. Single-building LAN

Multiple-building LAN



b. Multiple-building LAN

Local Area Network Example 2

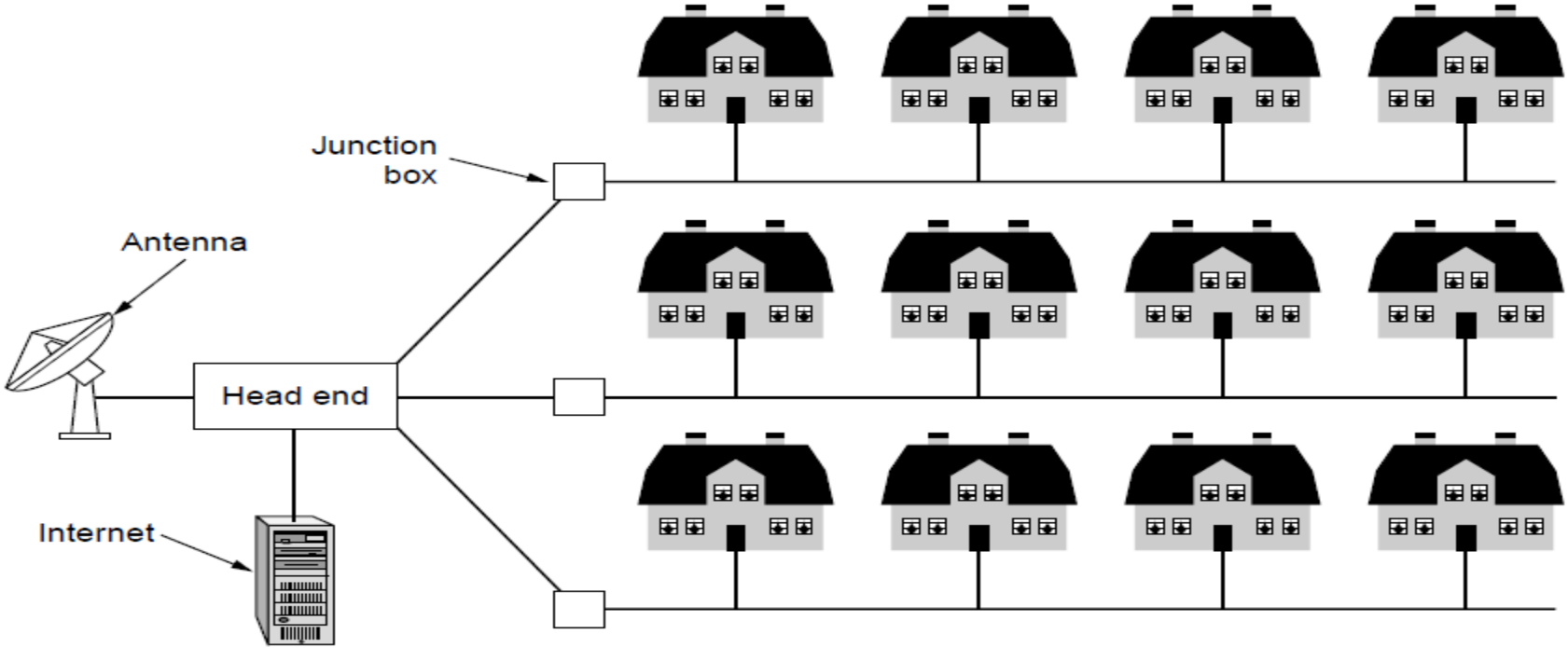


Simple LAN

MAN (Metropolitan Area Network)

- Owned by private company or it may be a service provided by public company (such as local tel.-company)
- Extended over an entire city.
- May be single network such as a cable television network, or it may be connected number of LANs into a large network so that resources may be shared LAN-TO- LAN.

Metropolitan Area Networks

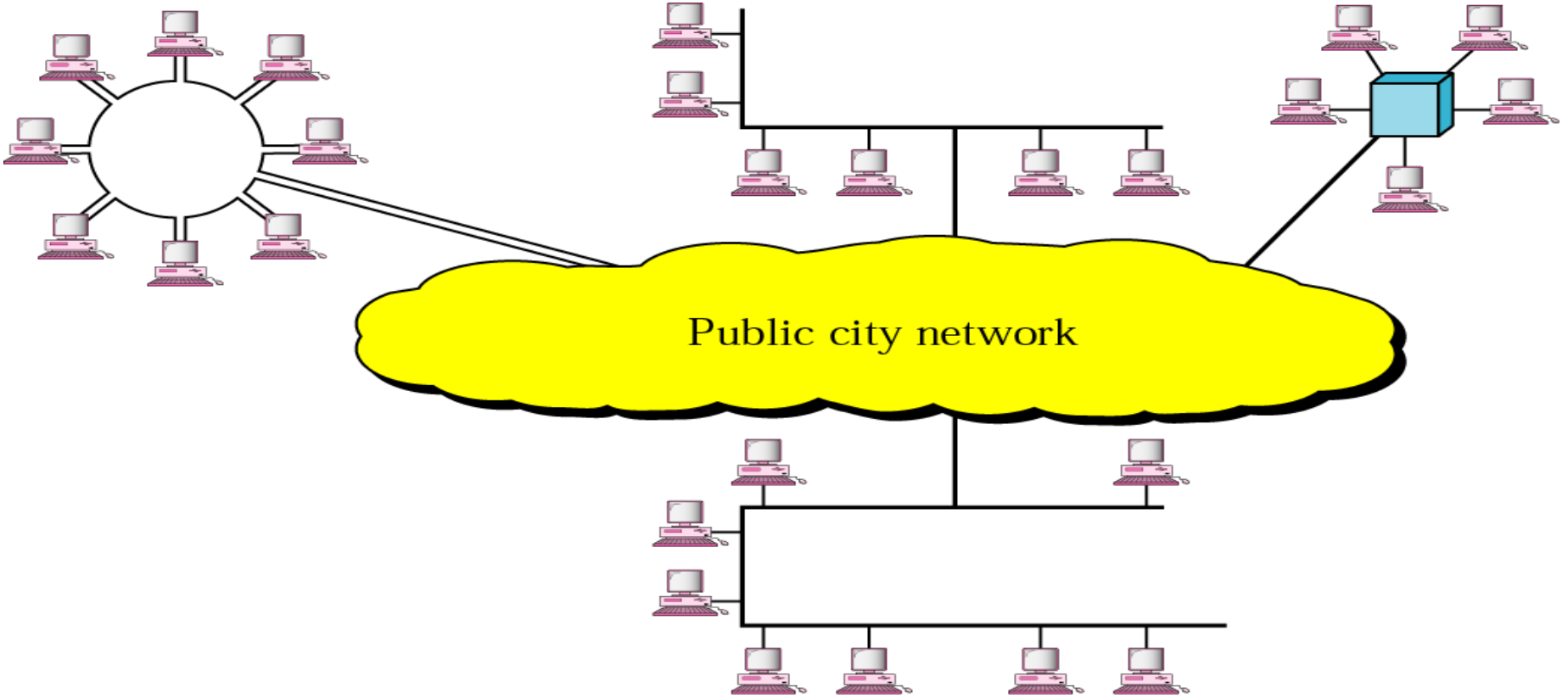


A metropolitan area network based on cable TV.

MAN (Metropolitan Area Network)

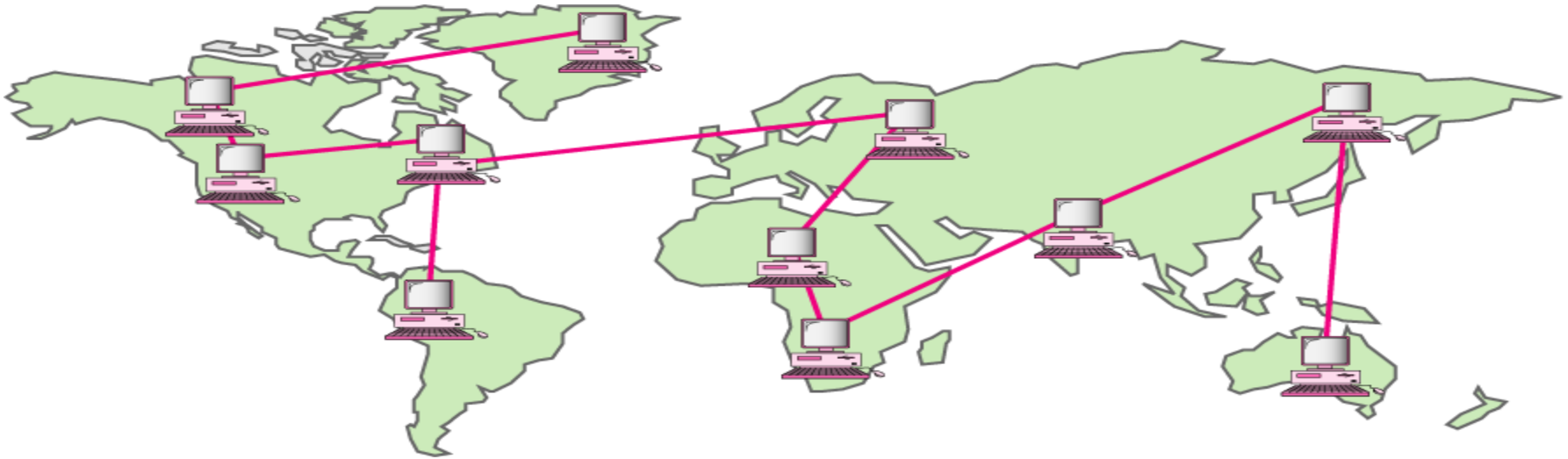
- **Examples:**
  - ✓ Company can use MAN to connect the LANs in all its offices throughout the city.
  - ✓ A part of the telephone line network that can provide DSL line to the customer

MAN



WAN (Wide Area Network)

- **Provides long distance transmission of data, voice , image and video information over large areas (country or whole world)**
- **In contrast to LAN, WAN may utilize public or private communication equipments or combination.**



Differences between LAN, MAN, WAN

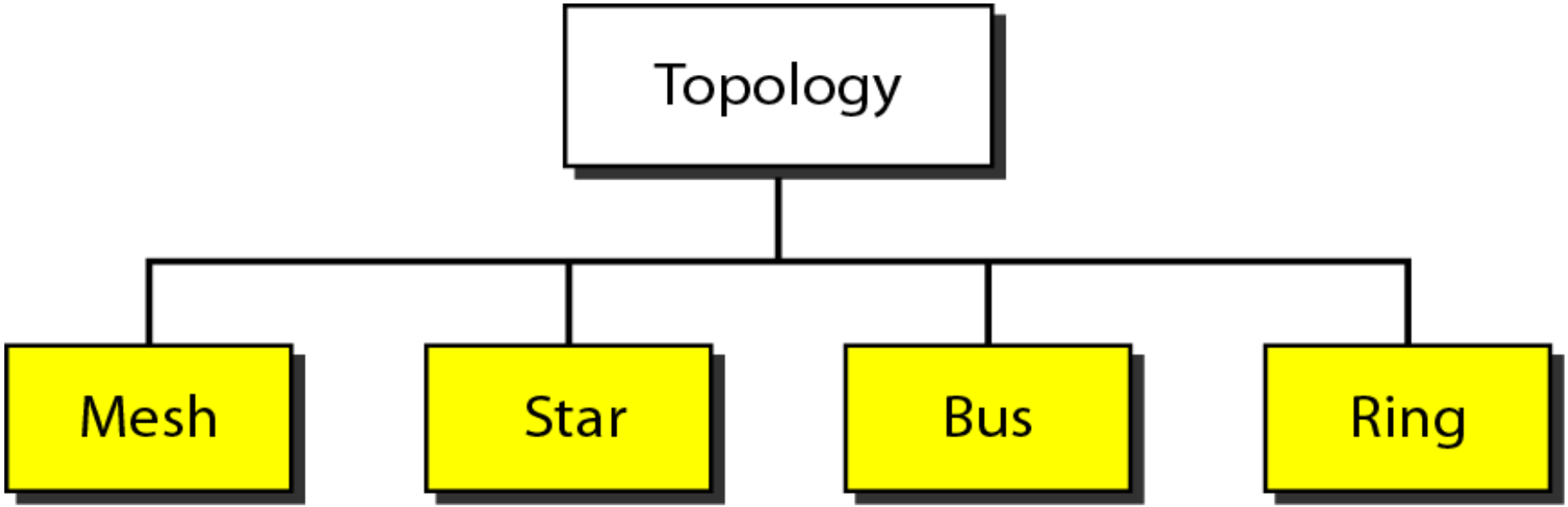
BASIS	LAN	MAN	WAN
Range	A communication network linking a number of stations in same local area. Range is 1 to 10 km	This network shares the characteristics of packet broadcasting networks. Range is100 km	A communication network distinguished from a Local Area Network. Range is Beyond 100 km
Media Used	Uses guided media	Uses guided as well as unguided media	Uses unguided media
Speed	A high speed i.e. 100kbps to 100mbps	Optimized for a large geographical area than LAN.	Long distance communications, which may or may not be provided by public packet network.
Cost	cheaper	costly	expensive
Equipment needed	NIC, switch and hub	Modem and router	Microwave, radio, infra-red laser

Physical Topology

- Two or more links for a **topology**.
  - The *topology* of a network refers to the geometric representation of the relationship of all the links and linking devices (nodes) to one another.
- The term *physical topology* refers to the way in which a network is laid out physically.

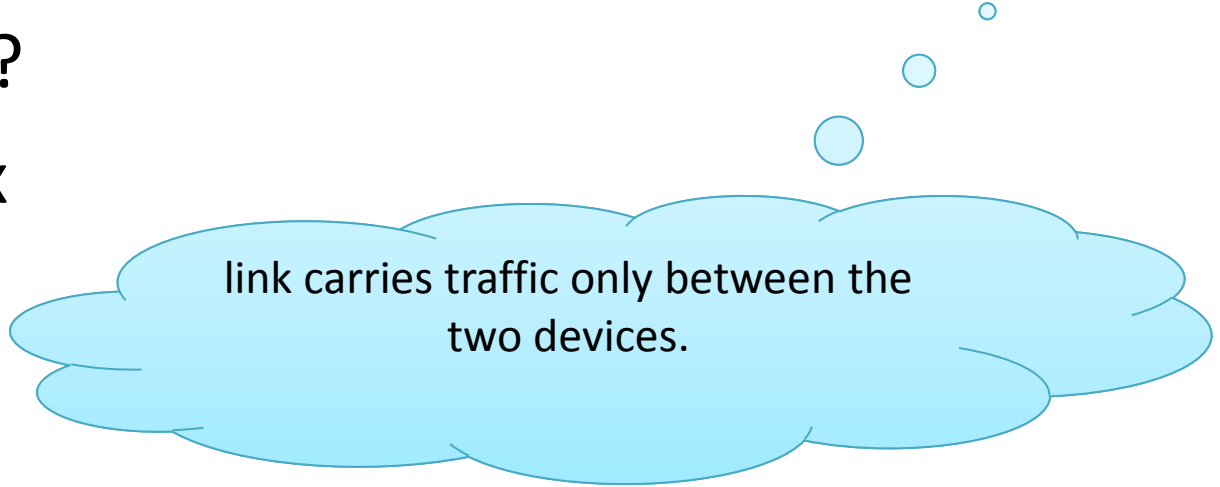
Physical Topology

- The way in which a network is laid out physically.



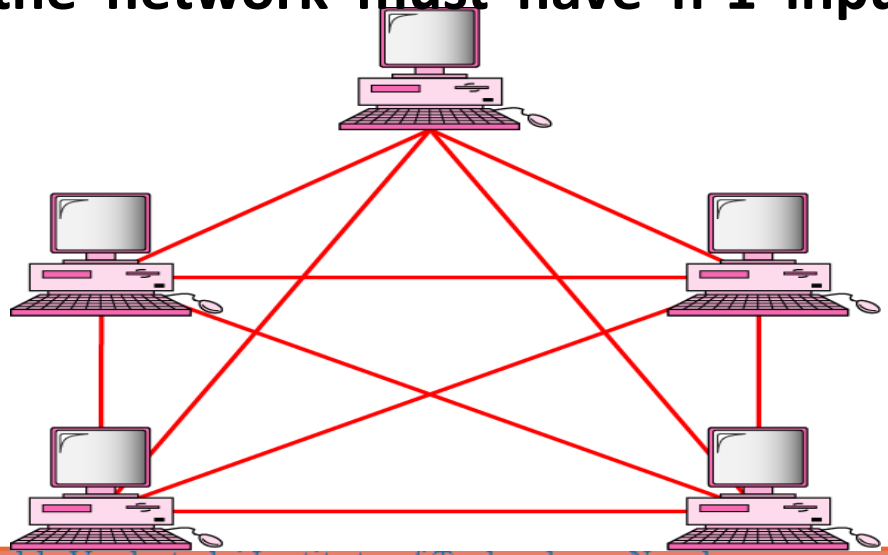
Mesh Topology

- Every device has a *dedicated* **point-to-point** link with every other device on the network.
- How many links do we need in a network with N nodes?
  - – Half duplex
  - - Full duplex



Fully connected mesh topology (for five devices)

- Every device has a dedicated point-to-point link to every other devices
- Fully connected mesh network has 2n(n-1) physical connection to link n devices.
- Every device on the network must have n-1 input/output (I/O) ports



Advantages of a Mesh topology

- Privacy or security (every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevents other user from gaining access the message
- eliminating the traffic problems The use of dedicated links guarantees that each connection can carry its own data load; that can occur when links must be shared by multiple devices.

Advantages of a Mesh topology

- A mesh is robust. If one link becomes unusable, it does not incapacitate the entire system.
- Fault identification and fault isolation easy. This enables the network manager to discover the precise location of fault and aids in finding its cause and solution.

Disadvantages of a Mesh topology

Related to the amount of cabling devices and the amount of I/O ports required:

- Every device must be connected to every other device, **installation and reconnection are difficult**
- The sheer bulk of the wiring can be greater than the available space can accommodate.
- The H.W required to connect each link (I/O ports and cable) expensive.

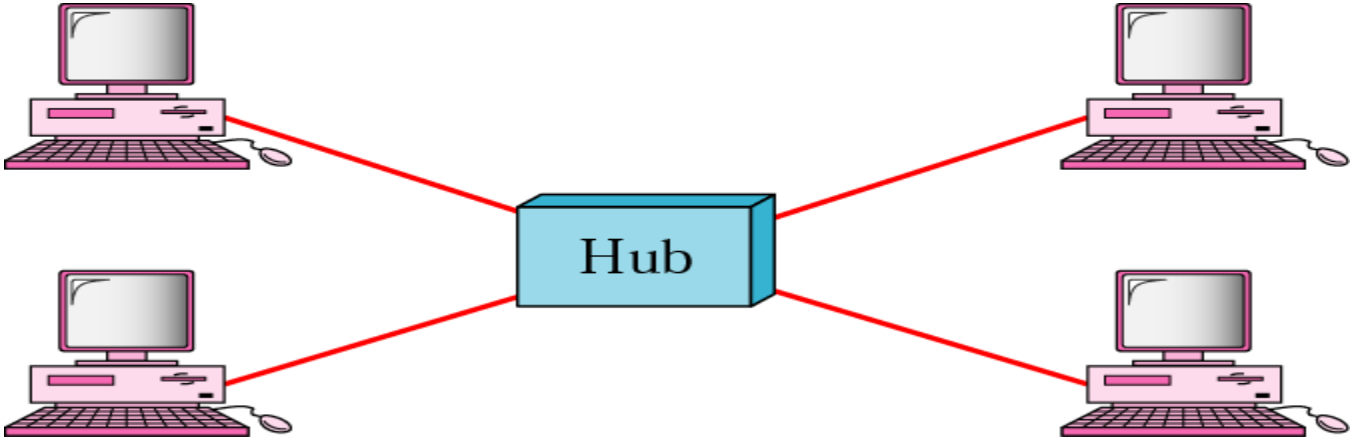
Disadvantages of a Mesh topology

So a mesh topology is usually implemented in a limited fashion(as a backbone connecting the main computers of a hybrid network that can include several other topology

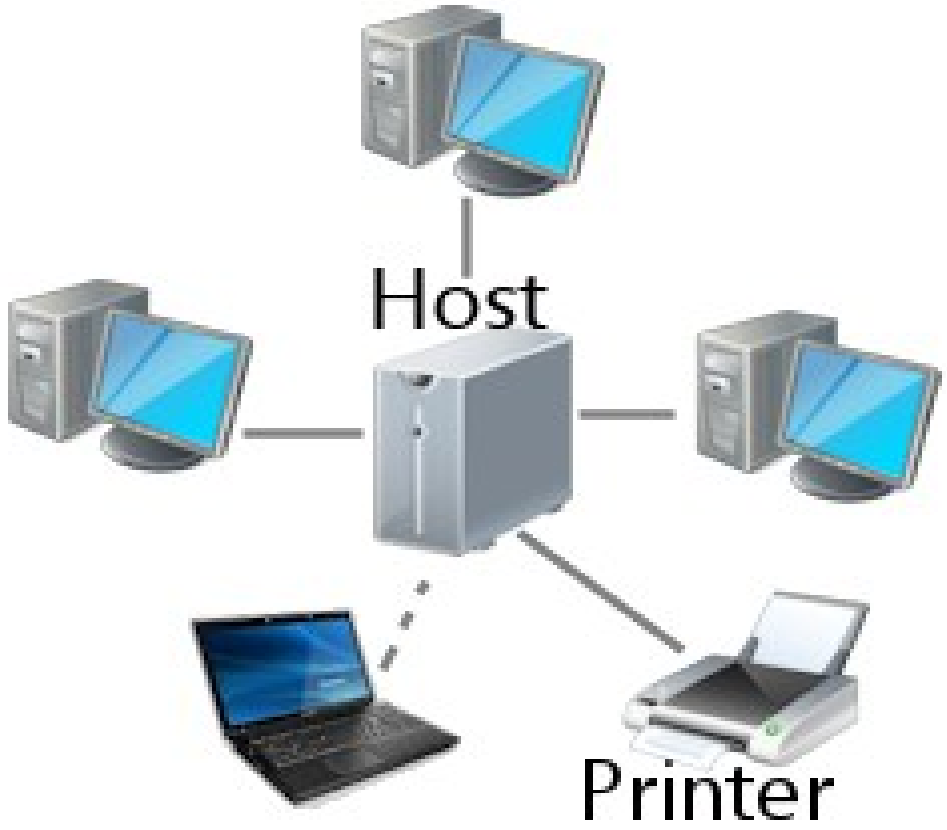
Star topology

Each device has a dedicated point-to-point link only to a central controller (hub)

Unlike a mesh , a star topology does not allow direct traffic between devices, if one device want to send data to another , it send it to the hub, which send it to other device



- The **star** pattern connects everything to a **host c** a **network switch,** or a **hub**, which handles the tasks.
- All communications between computers go through the host/switch/hub.



Advantages of a Star topology

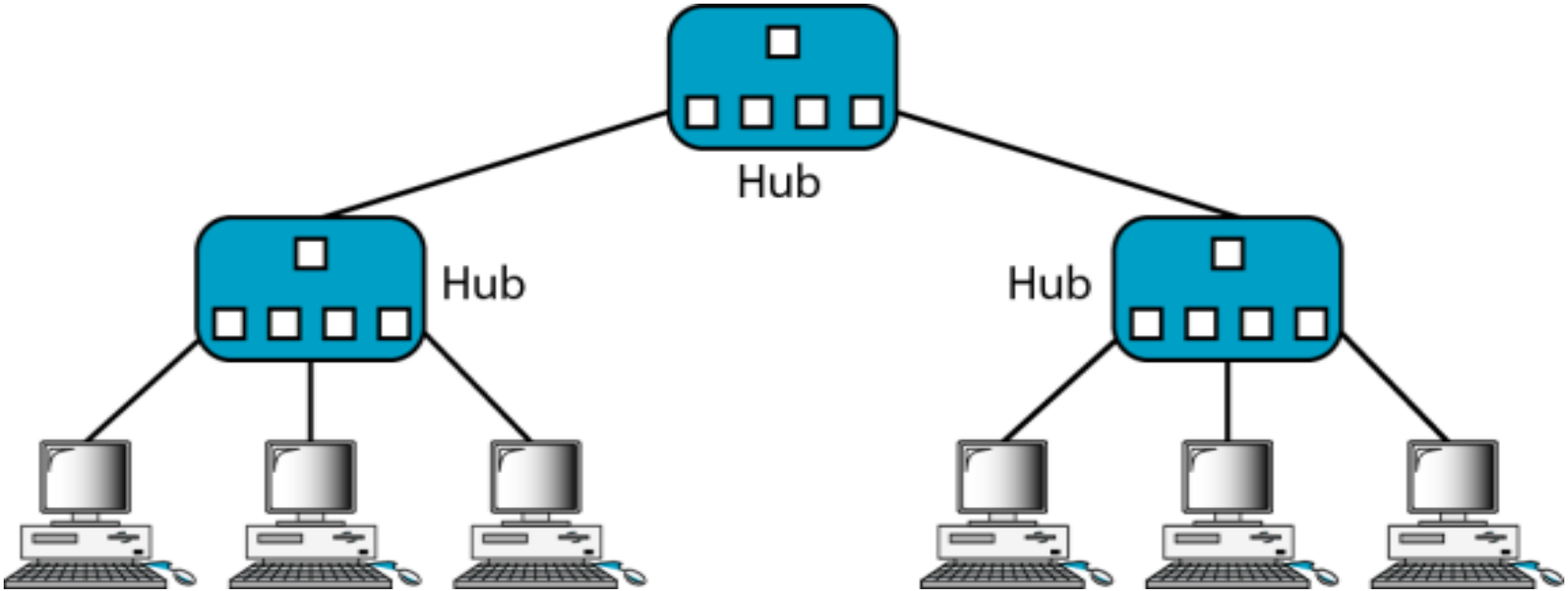
1. **Easy to install and reconfigure and less expensive**
   - each device need only one link and I/O port to connect it to any other devices.)
2. **Robustness:**
   - if one link fails, only that link affected and other links remain active.
3. **identification and fault isolation**

Disadvantages of a Star topology

- The dependency of the whole topology on one single point, the hub. **If the hub goes down, the whole system is dead.**

Tree topology : Is a variation of star

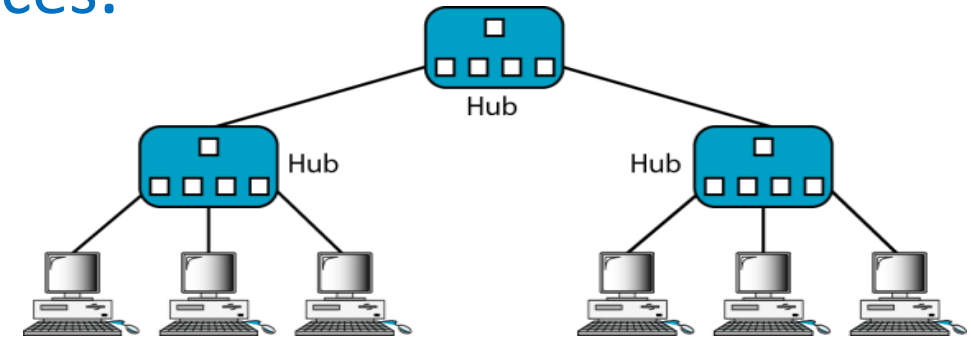
- Not every device plugs directly into the central hub. The majority of devices connect to secondary hub that in turn is connected to the central hub.



Tree topology : Is a variation of star

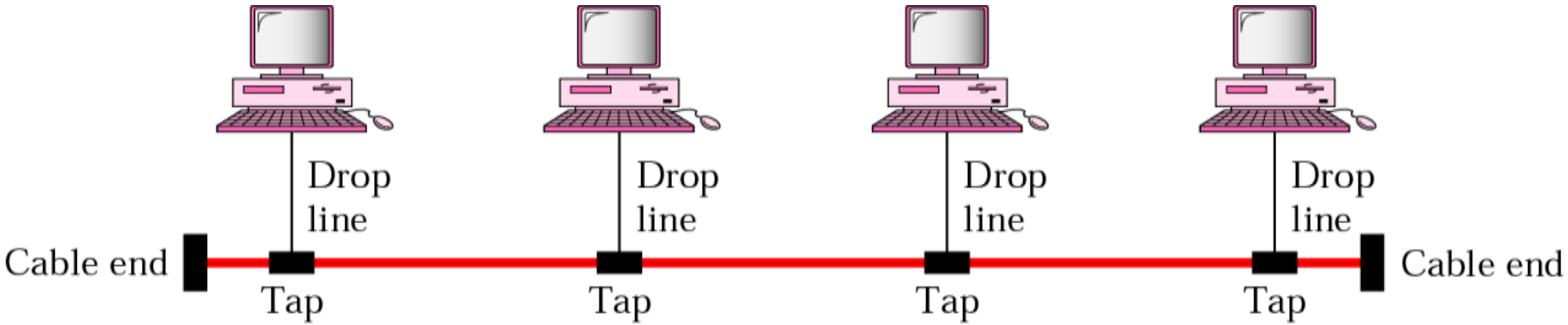
The advantages and disadvantages of tree topology are generally the same as those of star .

- The addition of secondary hubs bring more advantage: allows for more devices to be attached to a single central hub, therefore increase the distance a signal can travel between devices.

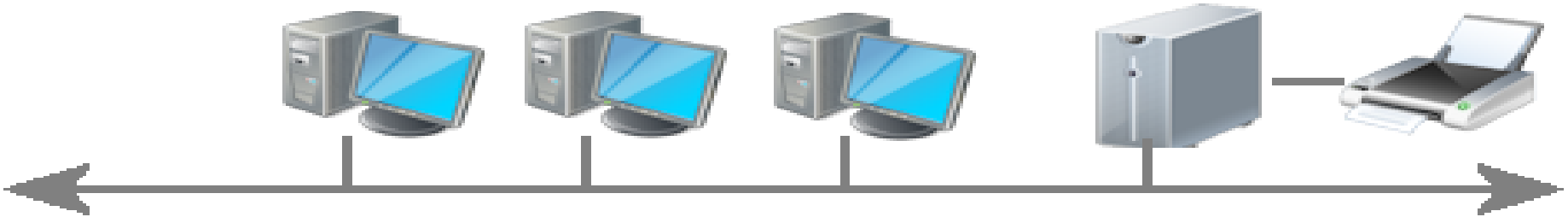


Bus topology

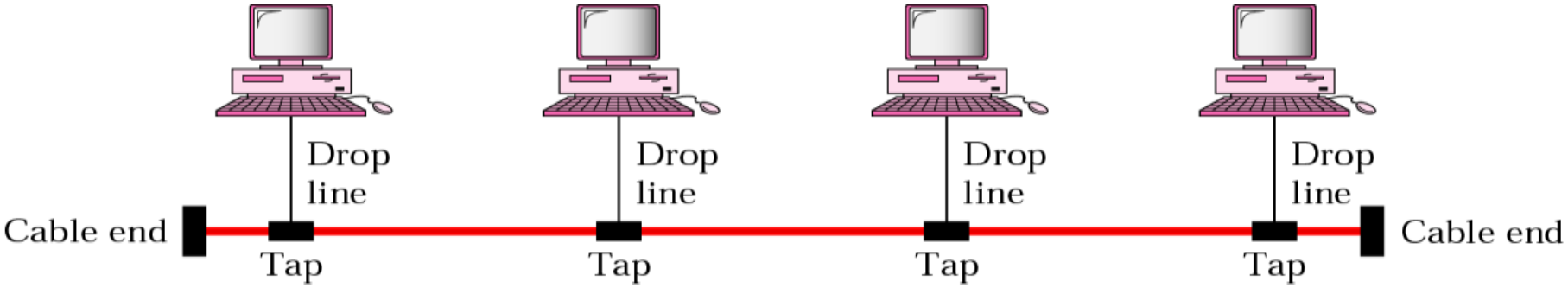
- Multipoint connection. Acts as a backbone to link all the devices in a network.



- The **bus** pattern connects the computer to the same communications line. Communications goes both directions along the line. All the computers can communicate with each other without having to go through the server.



Bus topology



There is a limit on the number of taps a bus can support and on the distance between those taps

- *As a signal travels along the backbone, it becomes weaker*

Advantages of a Bus topology

Ease of installation, use less cabling than mesh or star.

Disadvantages of a Bus topology

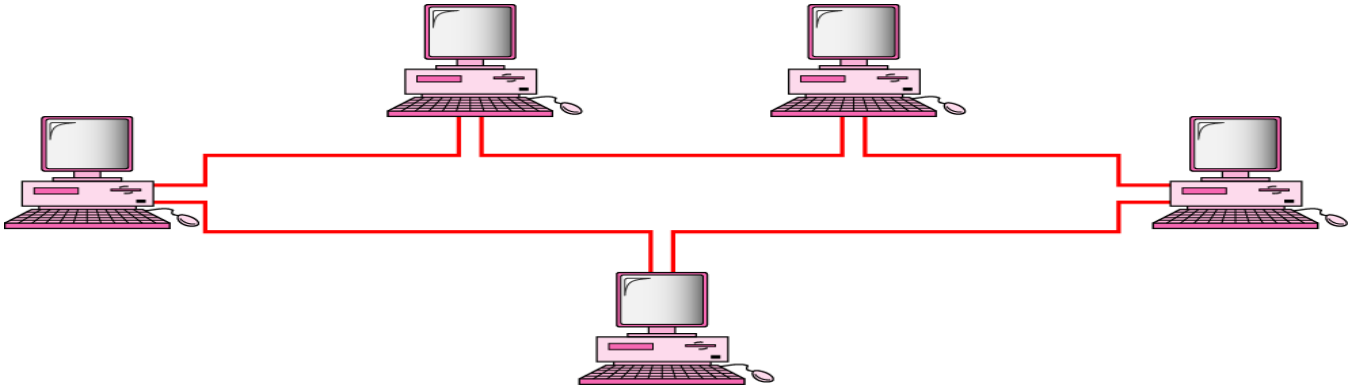
1. A fault in bus cable (break) stops all transmissions even between devices on the same side of the problem. The damaged area reflects signals back the direction of origin, creating noise in both directions

2. Reconnection

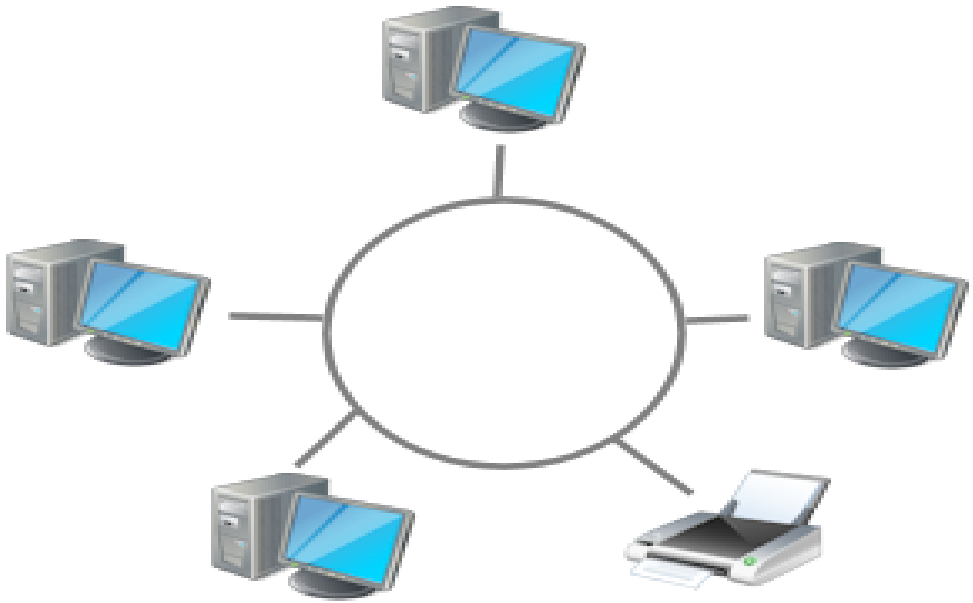
It can difficult to add new devices (adding more require modification or replacement of the backbone).

Ring Topology

- Each device has a *dedicated* point-to-point connection only with the two devices on either side of it
- A signal is passed along the ring in one direction from device until it reaches its destination.

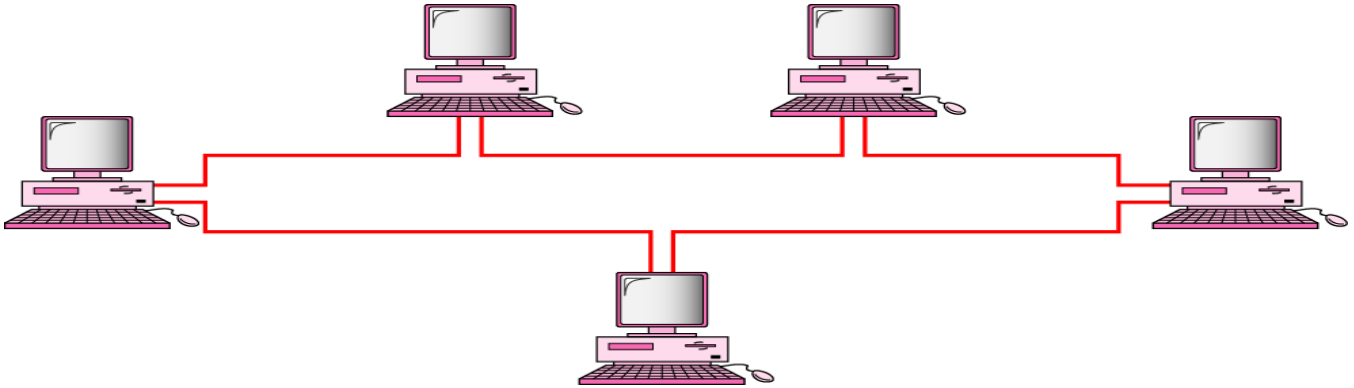


- The **ring** pattern connects the computers and other devices one to the other in a circle.
- There is no central host computer that holds all the data.
- Communication flows in one direction around the ring.



Ring Topology

- Each device in the ring incorporate as repeater
- **Repeater :regenerates the signal**
- **it receives a weakened signal, creates a copy, bit for bit, at the original strength**



Advantages of a Ring Topology

- **Easy to install and reconfigure.**

Each device is linked only to its immediate neighbors. To add or delete a device requires hanging only 2 connections

- **Fault isolation is simplified :**

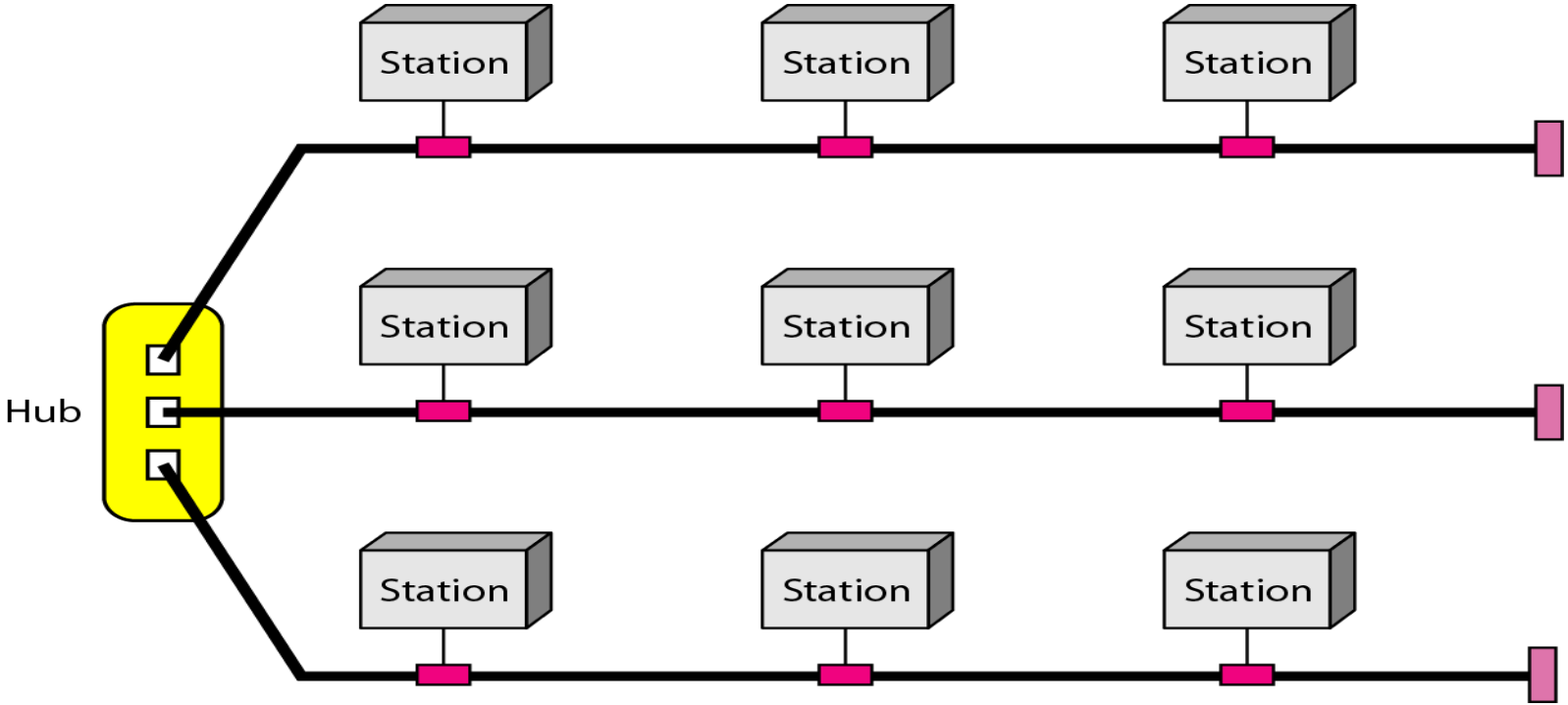
A signal is circulating at all times (token) if one device does not receive a signal within specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location

Disadvantages of a Ring Topology

- **Unidirectional traffic.**

  A break in the ring (such as disabled station) can disable the entire network. This can be solved by use dual ring

A hybrid topology: a star backbone with three bus networks

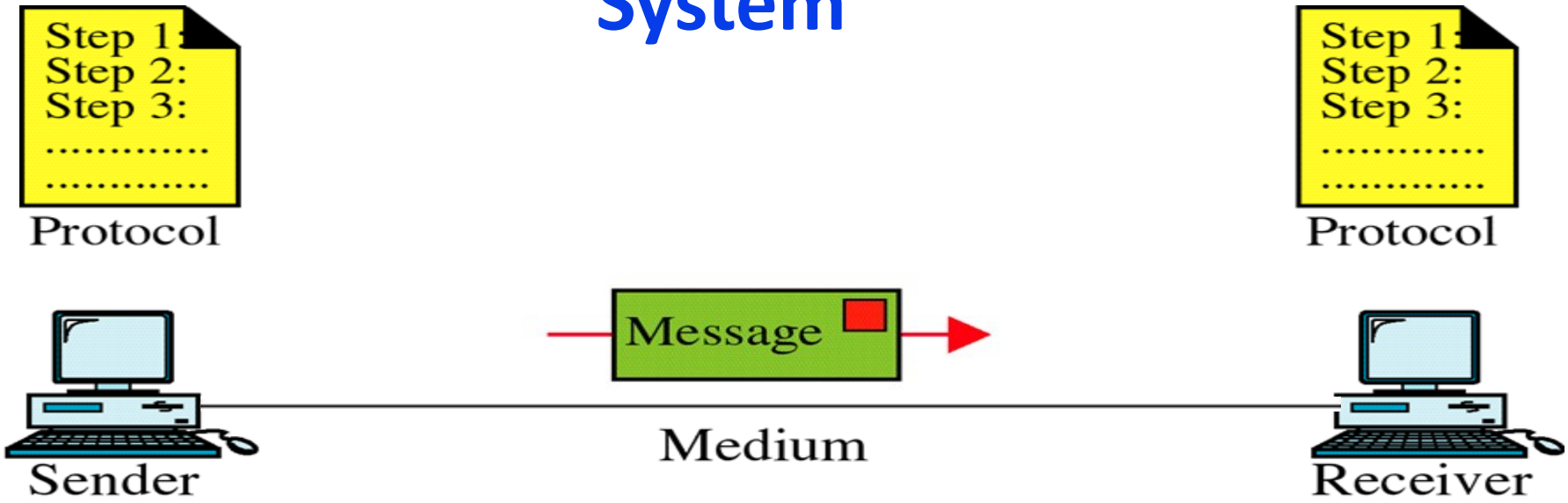


Definitions

- **Data:** information presented in whatever form

  text,image,audio,video
- **Data Communication:** exchange of data between two devices via transmission medium (wire cable / link).
- **Data Communication System:** Made up of a combination of hardware (physical equipment) and software (programs) to facilitate for effective communication of data.

Components of a Data Communication System



***Protocol*: is a set of rules that governs data communications. It represents an agreement between the communicating devices. Without a protocol two devices may be connected but not communicating.**

Characteristics of a Data Communication System

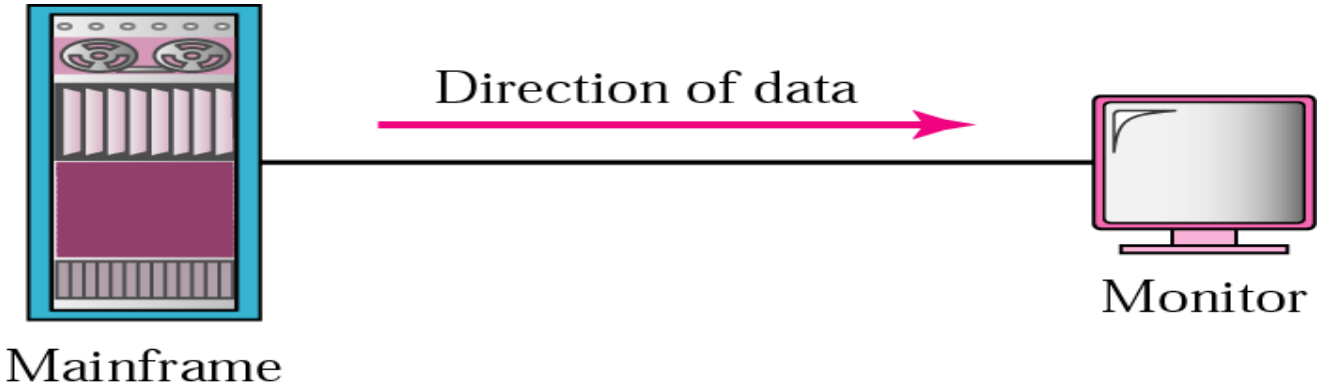
- ***Delivery*** : System must deliver data to correct destination. Data must be received by only intended device or user.
- ***Accuracy:*** The system must deliver data accurately
- ***Timeliness:*** the system must deliver data in a timely manner. Data delivered later are useless.
- ***Jitter:*** Variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

Data Flow

- Path taken by data within a device, network, or organization, as it moves from its source to its destination (a data repository or a data user).
- Categorized by direction of flow:
  - ❖ Simplex
  - ❖ Half-duplex
  - ❖ Full-duplex

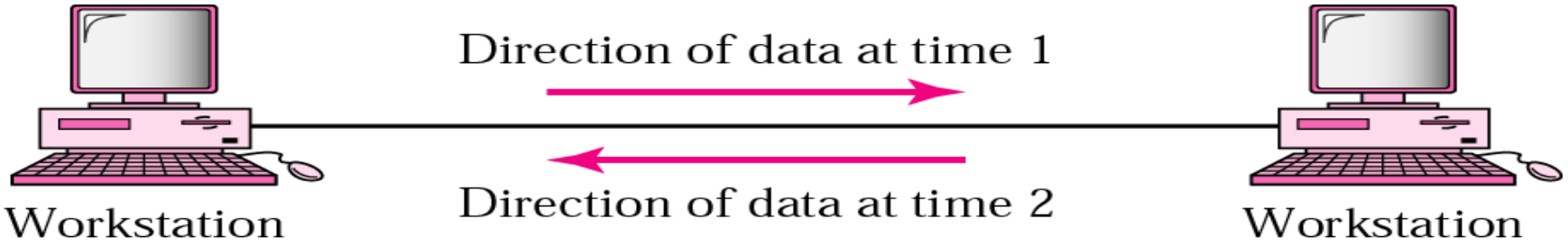
Simplex

- Communication is unidirectional, one of the two devices on a link can transmit; the other can only receive (one-way street).
- Ex: keyboard (input), monitors (output)



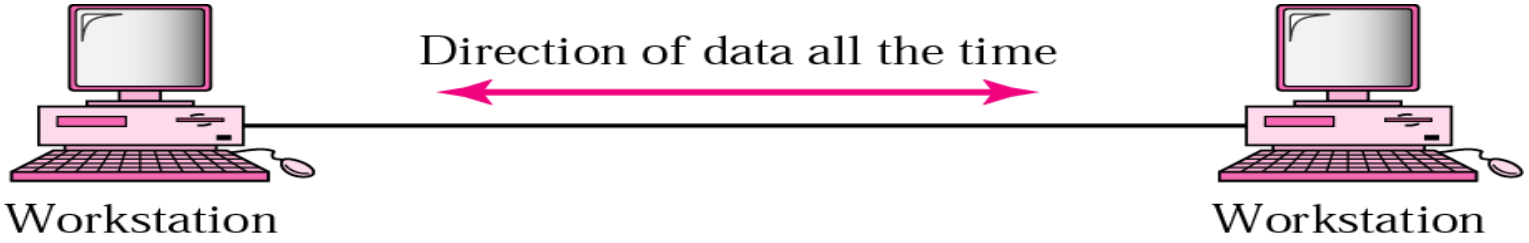
Half-duplex

Each station can both transmit and receive , ***but not at the same time***. When one device is sending the other can receive and vice versa. (one-lane road with two direction).



Full-duplex

- Both stations can transmit and receive simultaneously. (two way street with traffic flowing in both directions at the same time).
- Ex: telephone network.



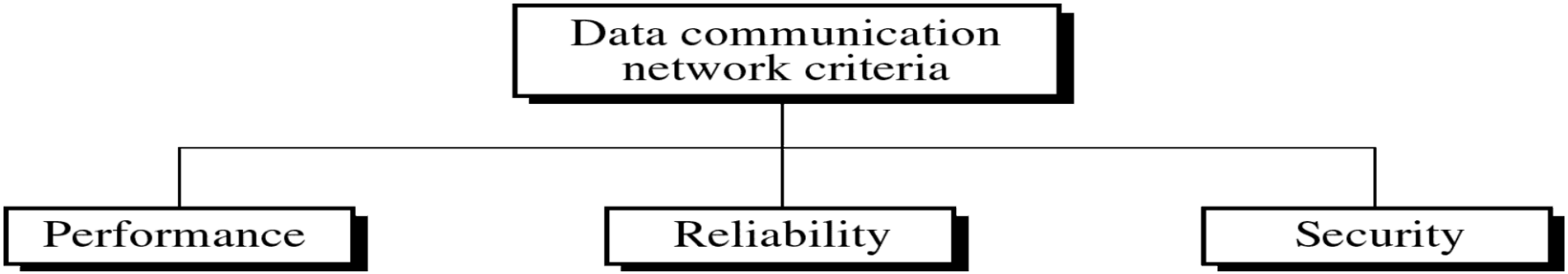
Signals going in either direction share the capacity of the link in two ways:

➢Either the link must contain two physically separate transmission paths one for sending and other for receiving.

➢Capacity of the channel is divided between signals traveling in both direction

Network Criteria

- A network must be able to meet a certain number of criteria.



Performance

- Can be measured in many ways!
  - Transmit time: the amount of time required for a message to travel from one device to another.
  - Response time: the elapsed time between an inquiry and a response.
- Often evaluated by two networking metrics: **throughput** and **delay**.

Throughput

- Throughput is an important network metric which is also known as bandwidth.
- The bandwidth of a network is given by the number of bits that can be transmitted over the network in a certain period of time.
- Depends on the network technology (hardware capabilities) and therefore is constant.

Throughput Example

- A network might have a bandwidth of 10 million bits/second (Mbps), meaning that it is able to deliver 10 million bits every second.

Delay

- Also known as latency.
- corresponds to how long it takes a message to travel from one end of a network to the other.
- Latency is measured strictly in terms of time.
- Effected by number of users and hence may change from time to time.

Delay Example

- A transcontinental network might have a latency of 24 milliseconds (ms); that is, it takes a message 24 ms to travel from one end of North America to the other.

Factors Affecting Performance

- Type of transmission media,
- Capabilities of connected H.W and the efficiency of software.
- Number of user

Network Criteria

- A network must be able to meet a certain number of criteria.
  - ✓ Performance
  - ❖ Reliability
  - ❖ Security

Reliability

- Accuracy of delivery.
- Measured by:
  - Frequency of failures
  - Time it takes to recover from a failure
  - The network's robustness in a catastrophe.

Network Criteria

- A network must be able to meet a certain number of criteria.
  - ✓ Performance
  - ✓ Reliability
  - ❖ Security

Security

- Many issues at the different layers!
- Examples:
  - Protecting data from unauthorized access.
  - Protecting data from damage.
  - Implementing policies and procedures for recovery from breaches and data losses.

LAYERED TASKS

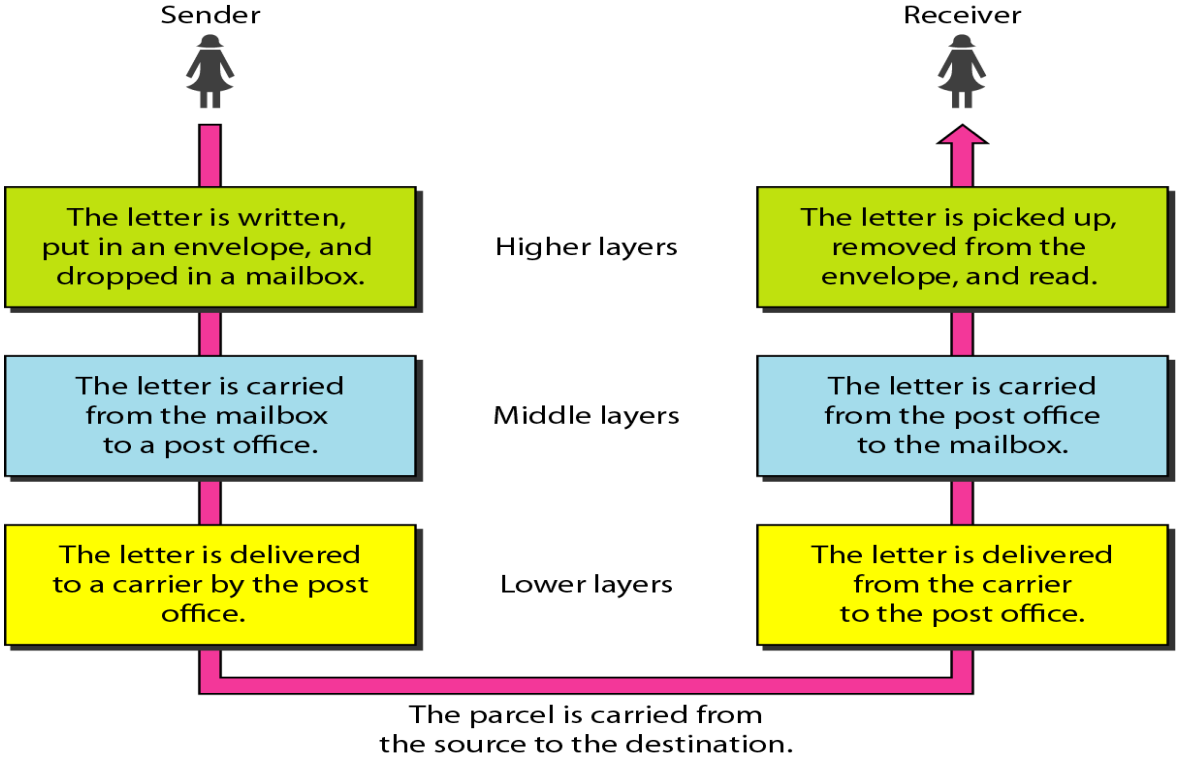
We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail. The process of sending a letter to a friend would be complex if there were no services available from the post office.

Topics discussed in this section:

Sender, Receiver, and Carrier

Hierarchy

Figure *Tasks involved in sending a letter*



Why layered architecture ?

To reduce the design complexity most of the networks are designed as series of layers.

A layer is an abstraction of protocols

Advantages :

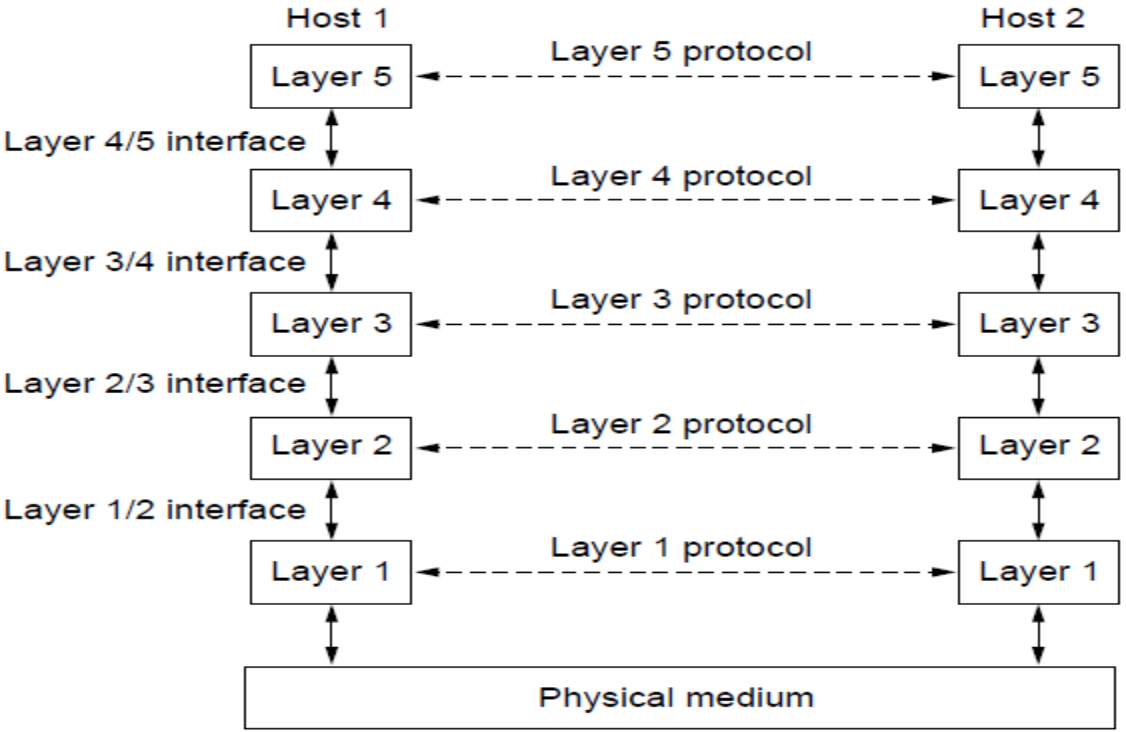
- Modularity-> breaking up into small pieces
- Clear Interfaces -> Open architecture and compatibility between components provided between different vendors

Network Software

Different Parts of the network software are :

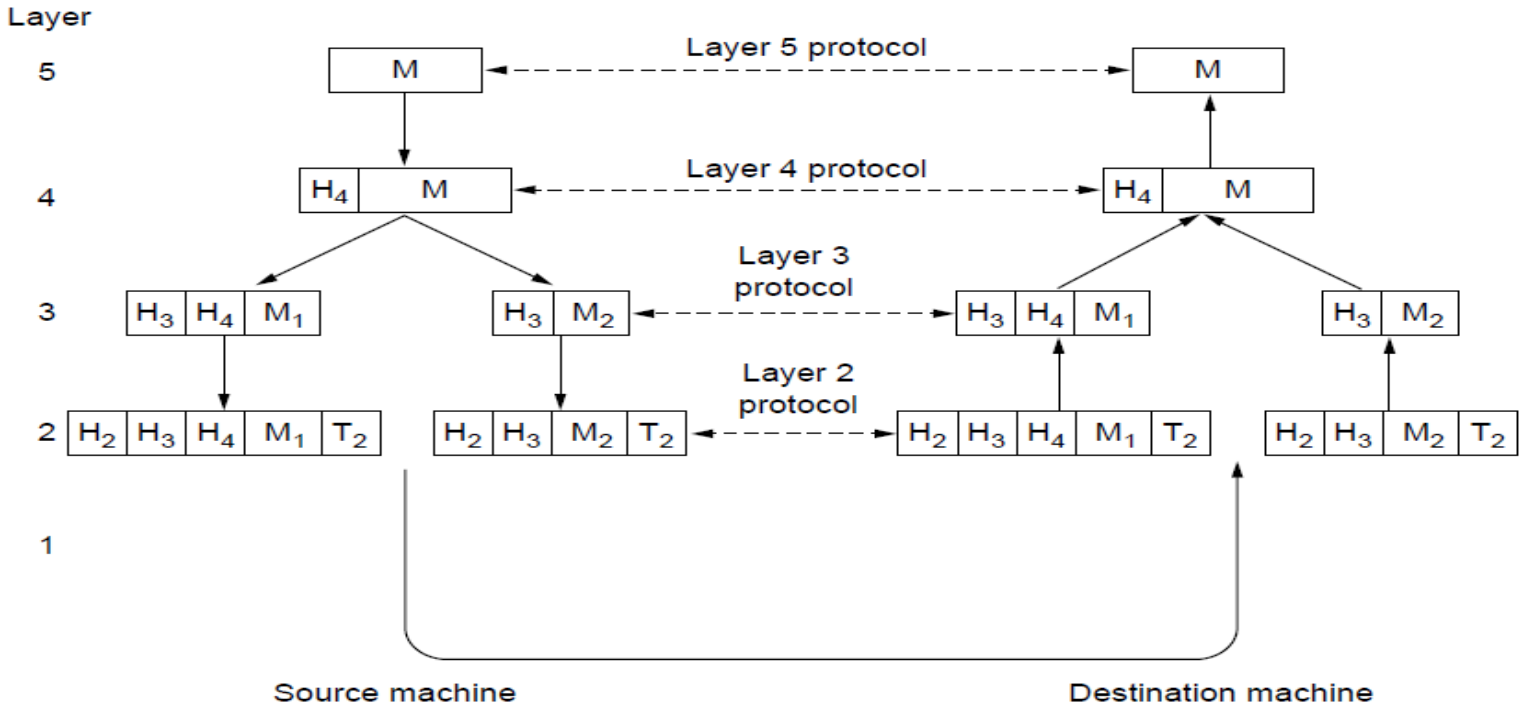
- Protocol hierarchies
- Design issues for the layers
- Connection-oriented versus connectionless service
- Service primitives
- Relationship of services to protocols

Protocol Hierarchies



Layers, protocols, and interfaces.

Protocol Hierarchies



Example information flow supporting virtual communication in layer 5.

Design issues for the layers

- Addressing
- Error control
- Flow control
- Multiplexing
- Routing

Addressing

- Since there are many computers on the network, every layer needs a mechanism for identifying the senders and receivers that are involved in a particular message.

- This mechanism is called **addressing** or **naming**, in the low and high layers, respectively.

Error Control

- There is a chance that some of these bits will be received damaged (inverted) due to fluke electrical noise, random wireless signals, hardware flaws, software bugs and so on.
- One mechanism for finding errors in received information uses codes for **error detection**.

Flow Control

- An allocation problem that occurs at every level is how to keep a fast sender from swamping a slow receiver with data.
- Feedback from the receiver to the sender is often used.
- This subject is called **flow control**.

Multiplexing

- Another important design issue is resource allocation.
- Multiplexing is needed in the physical layer where all the traffic for all the connections has to be sent over at most a few physical circuits

Routing

- Another reliability issue is finding a working path through a network. Often there are multiple paths between a source and destination, and in a large network, there may be some links or routers that are broken.
- Finding the shortest path

Connection-Oriented Versus Connectionless Service

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Movie download
	Unreliable connection	Voice over IP
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Text messaging
	Request-reply	Database query

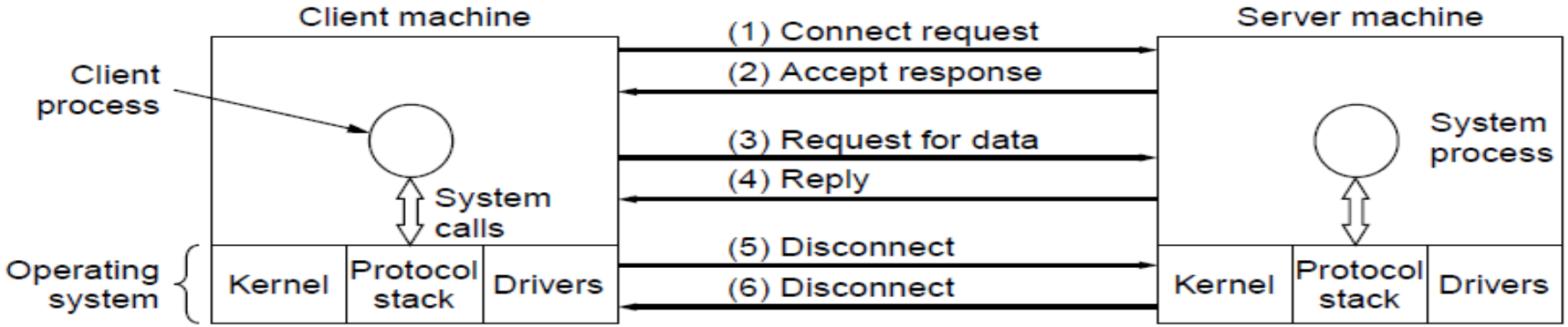
Six different types of service.

Service Primitives

Six service primitives that provide a simple connection-oriented service

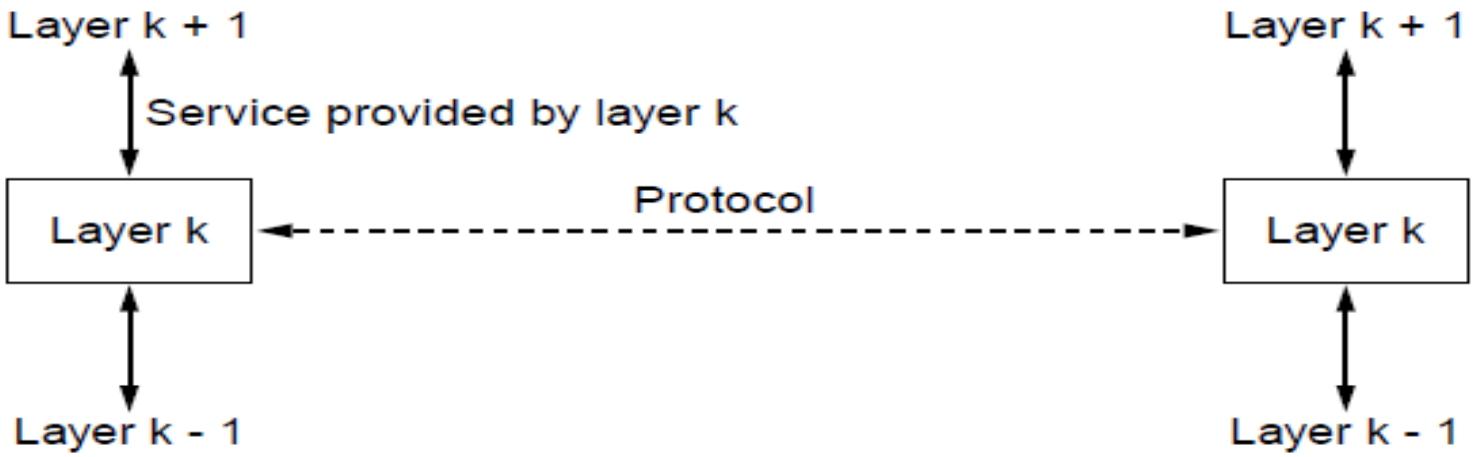
Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
ACCEPT	Accept an incoming connection from a peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Service Primitives



A simple client-server interaction using acknowledged datagrams.

The Relationship of Services to Protocols



The relationship between a service and a protocol.

THE OSI MODEL

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

Topics discussed in this section:

Layered Architecture
Peer-to-Peer Processes
Encapsulation

Note

ISO is the organization.
OSI is the model.

Figure *Seven layers of the OSI model*

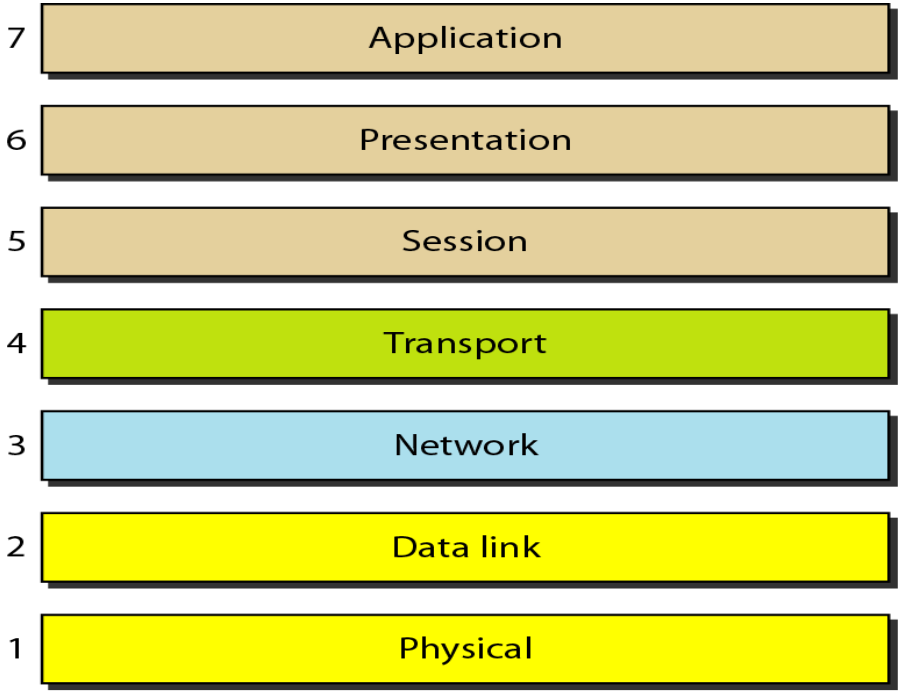


Figure *The interaction between layers in the OSI model*

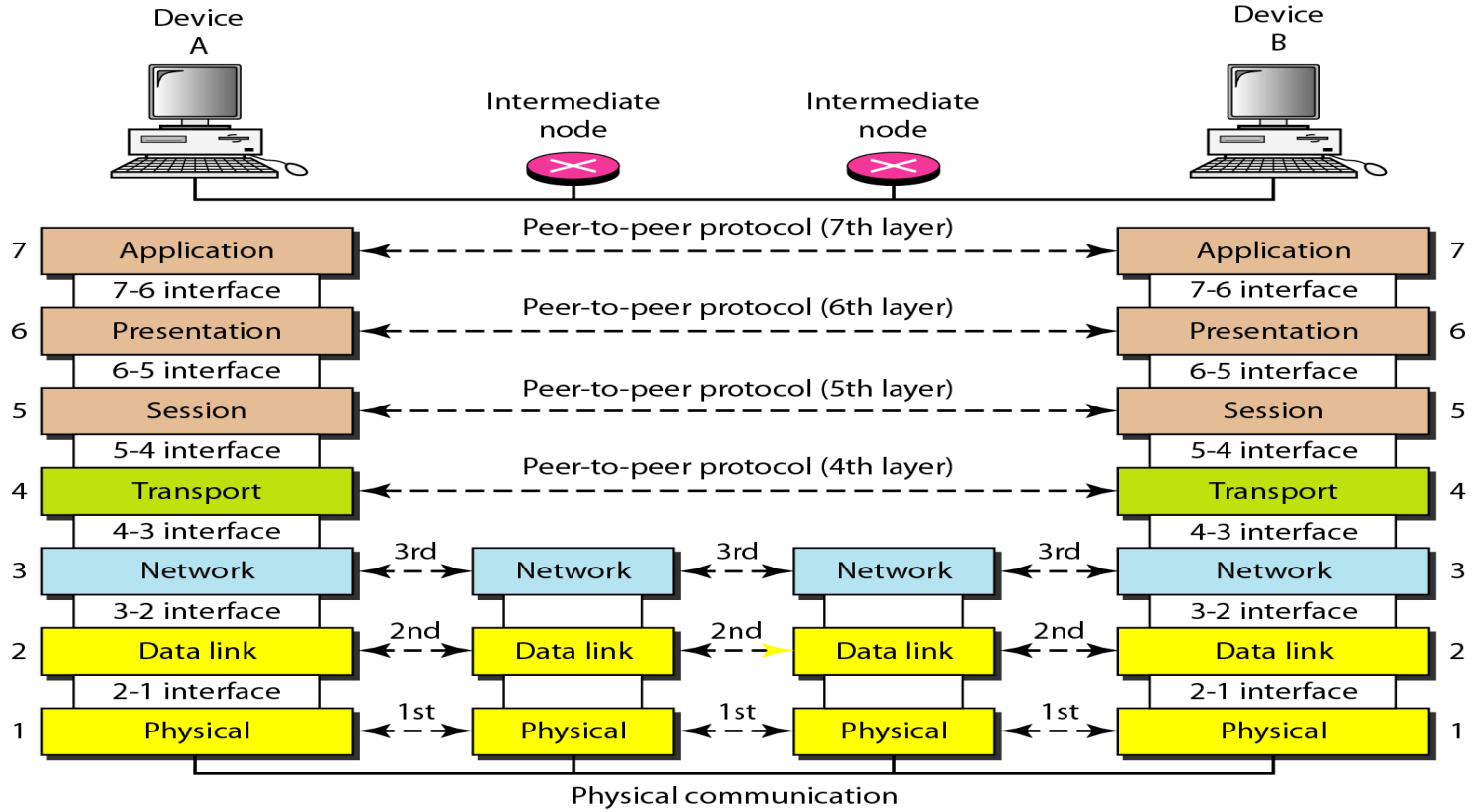
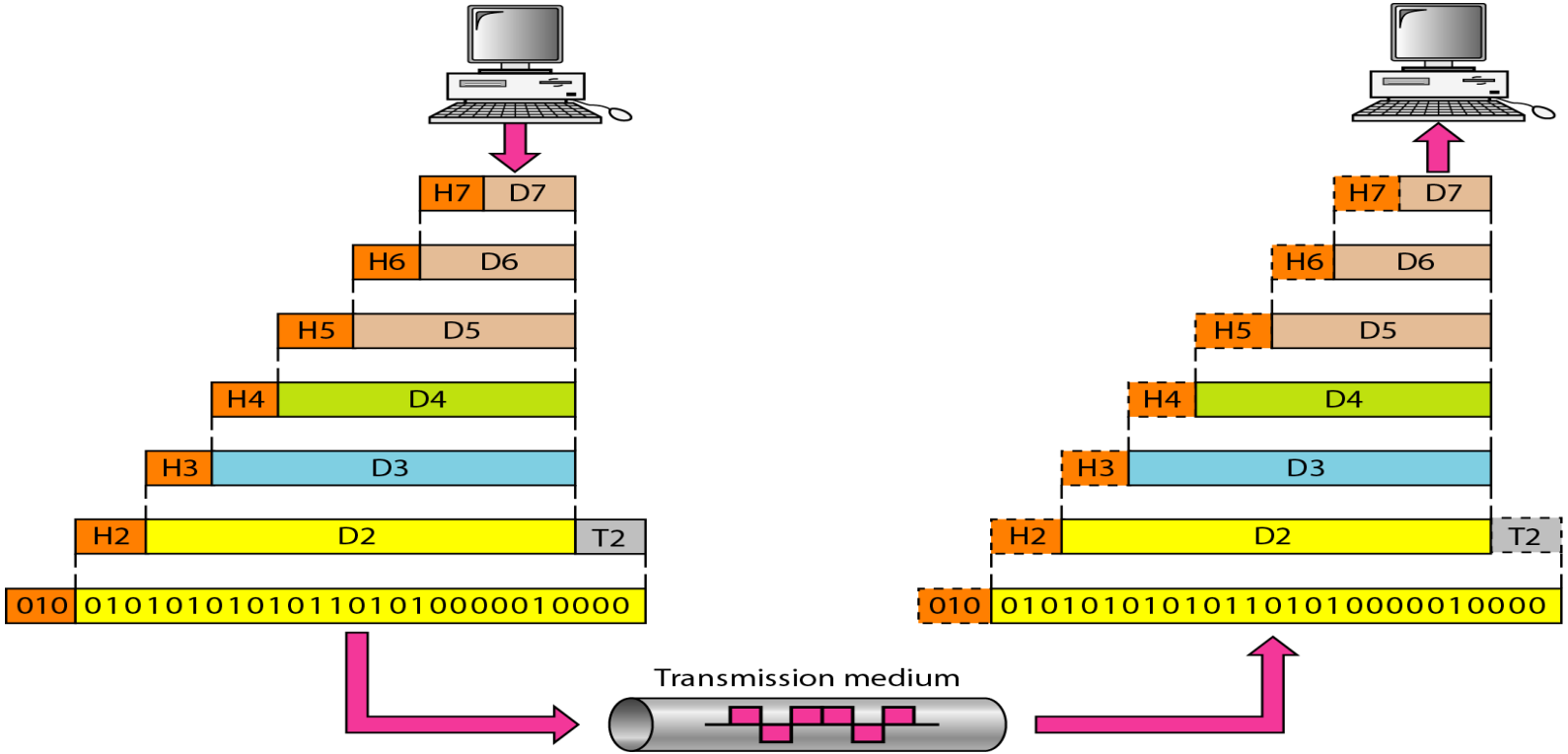


Figure *An exchange using the OSI model*



LAYERS IN THE OSI MODEL

In this section we briefly describe the functions of each layer in the OSI model.

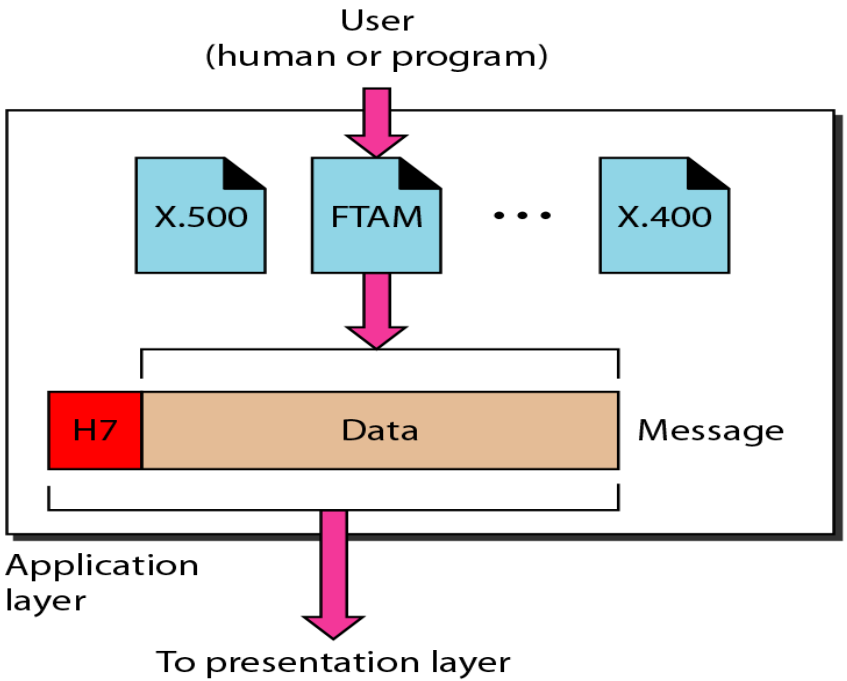
Topics discussed in this section:

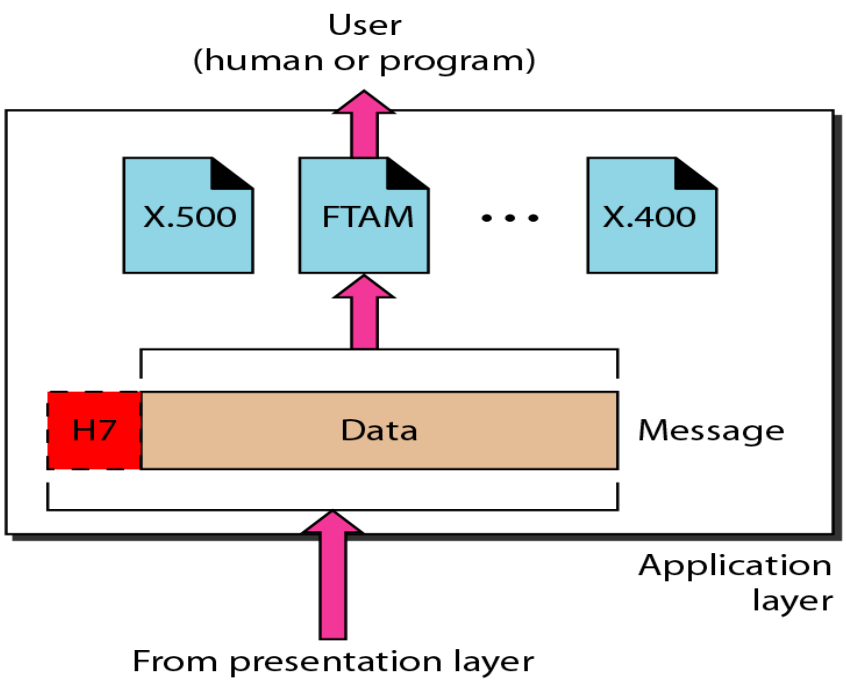
Physical Layer
Data Link Layer
Network Layer
Transport Layer
Session Layer
Presentation Layer
Application Layer

Note

The application layer is responsible for providing services to the user.

Figure *Application layer*

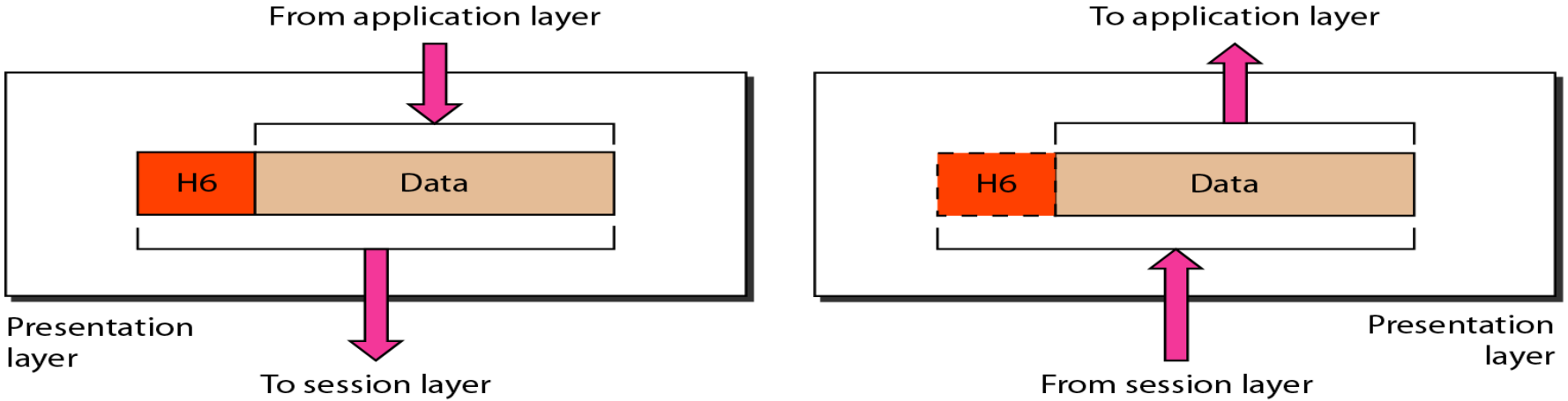




Note

The presentation layer is responsible for translation, compression, and encryption.

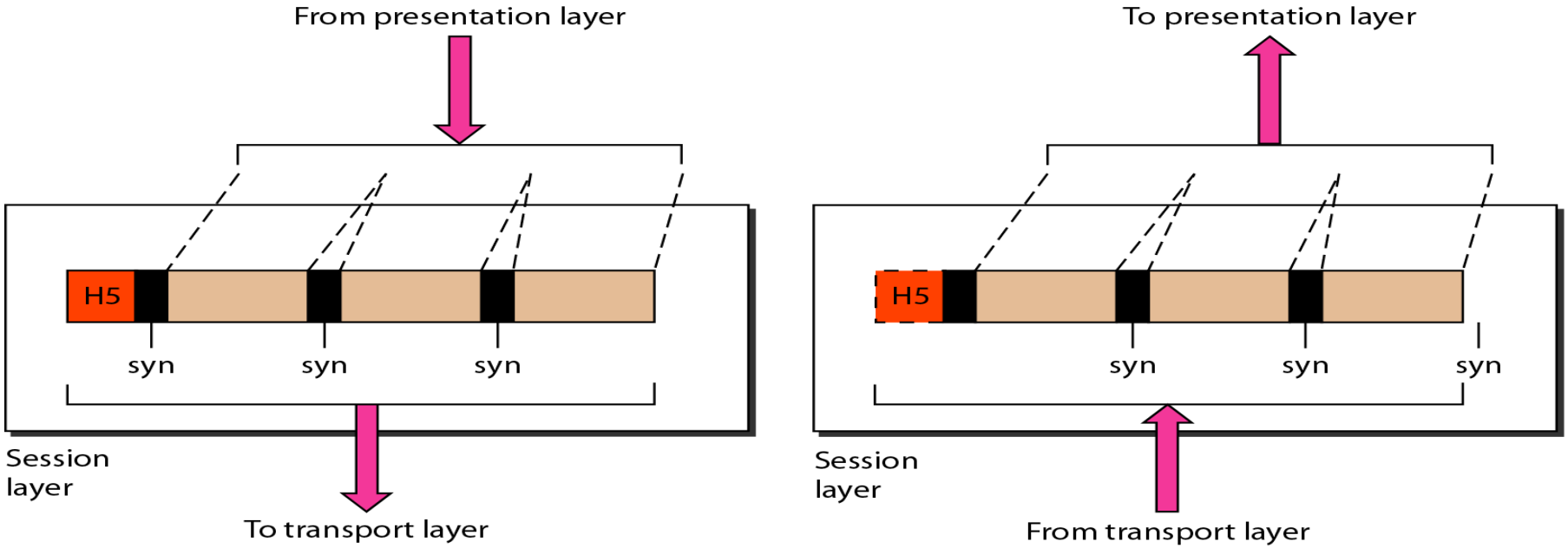
Figure *Presentation layer*



Note

The session layer is responsible for dialog control and synchronization.

Figure *Session layer*



Note

The transport layer is responsible for the delivery of a message from one process to another.

Figure *Transport layer*

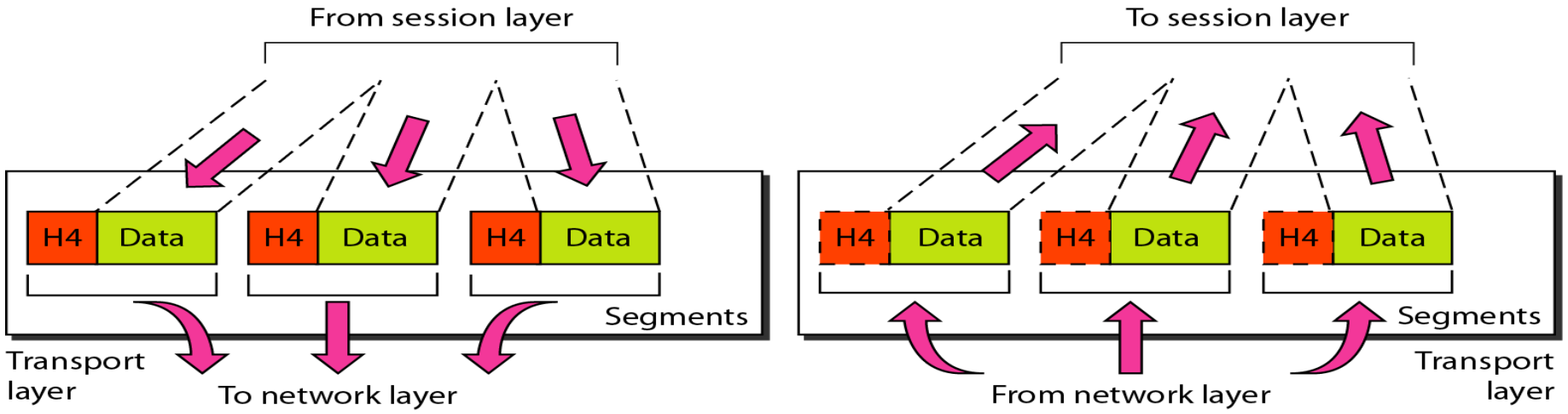
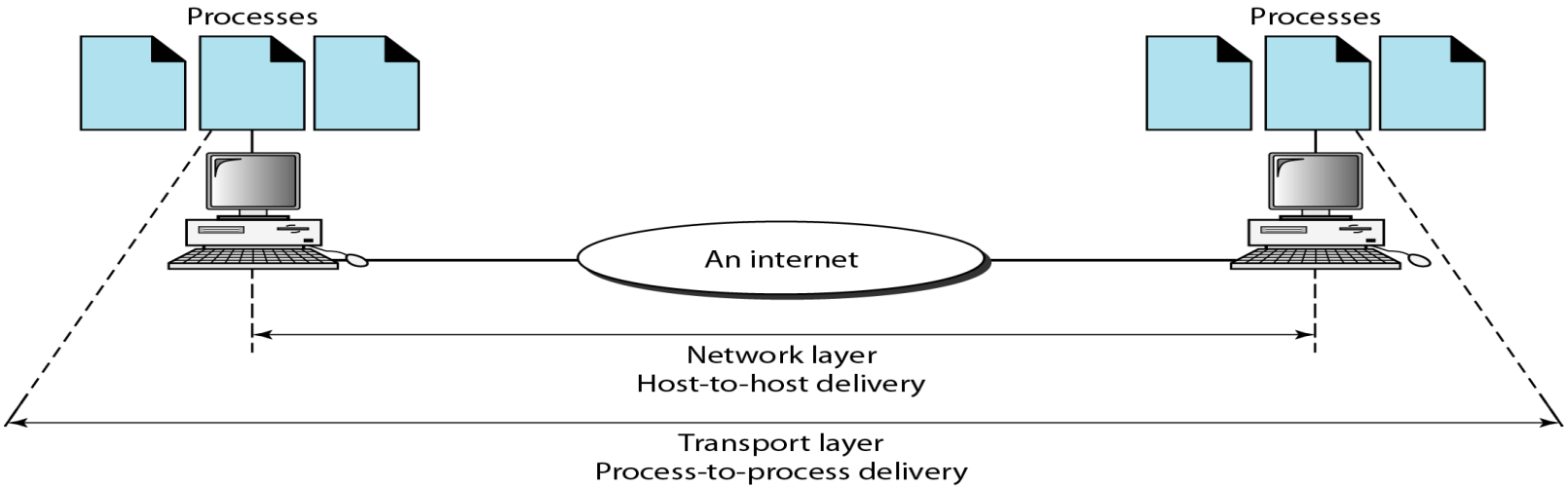


Figure *Reliable process-to-process delivery of a message*



Note

The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Figure *Network layer*

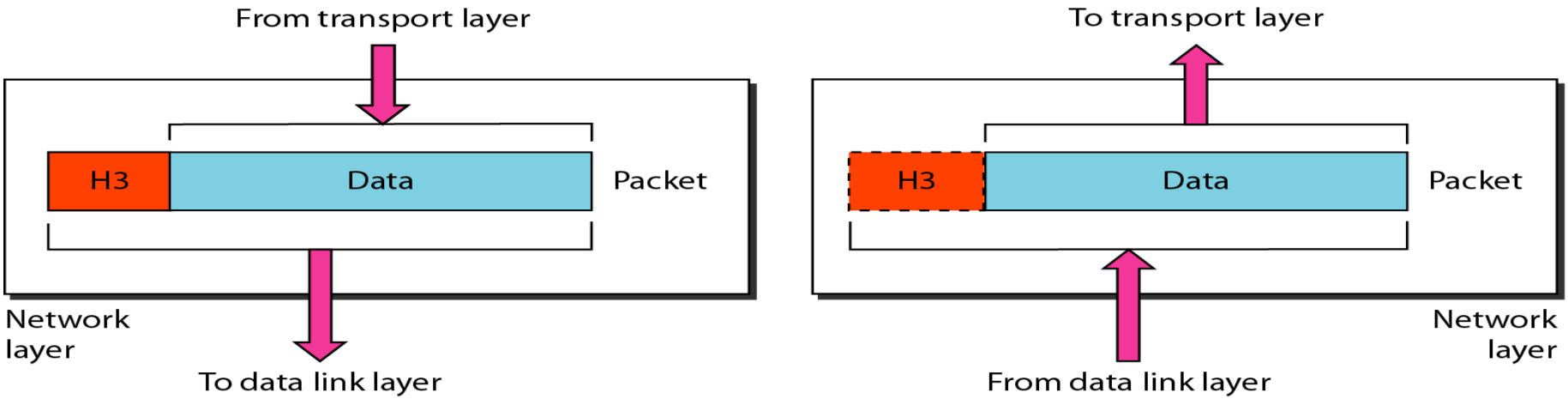
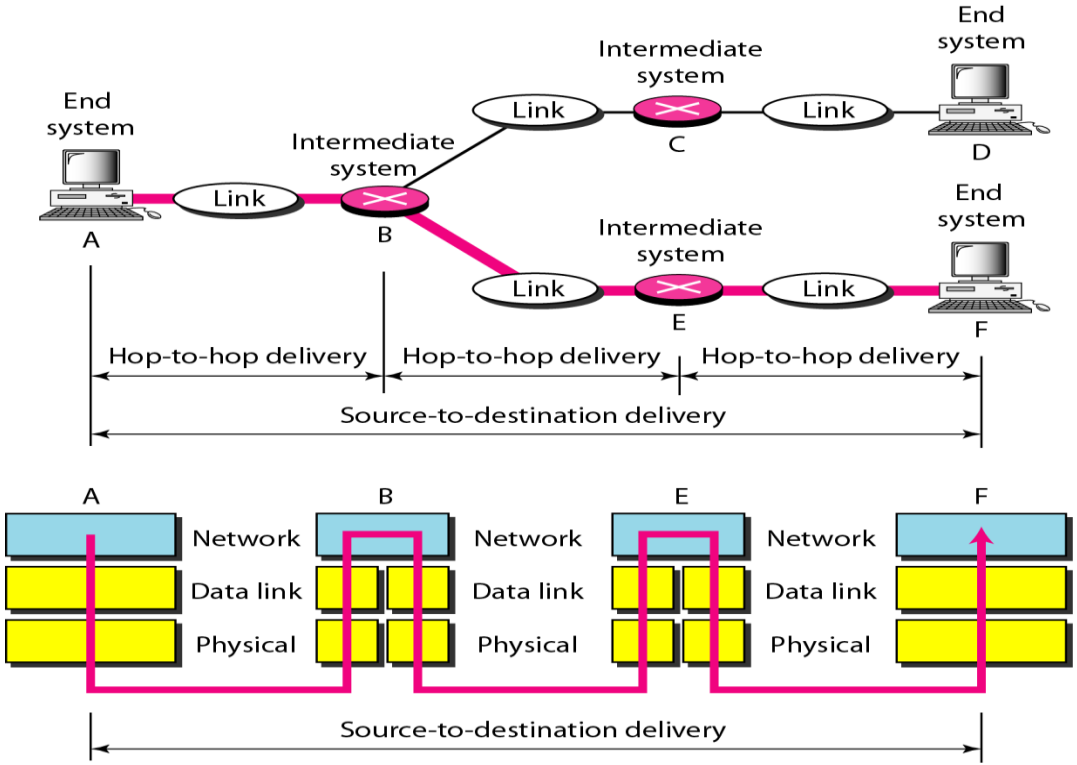


Figure *Source-to-destination delivery*



Note

The data link layer is responsible for moving frames from one hop (node) to the next.

Figure *Data link layer*

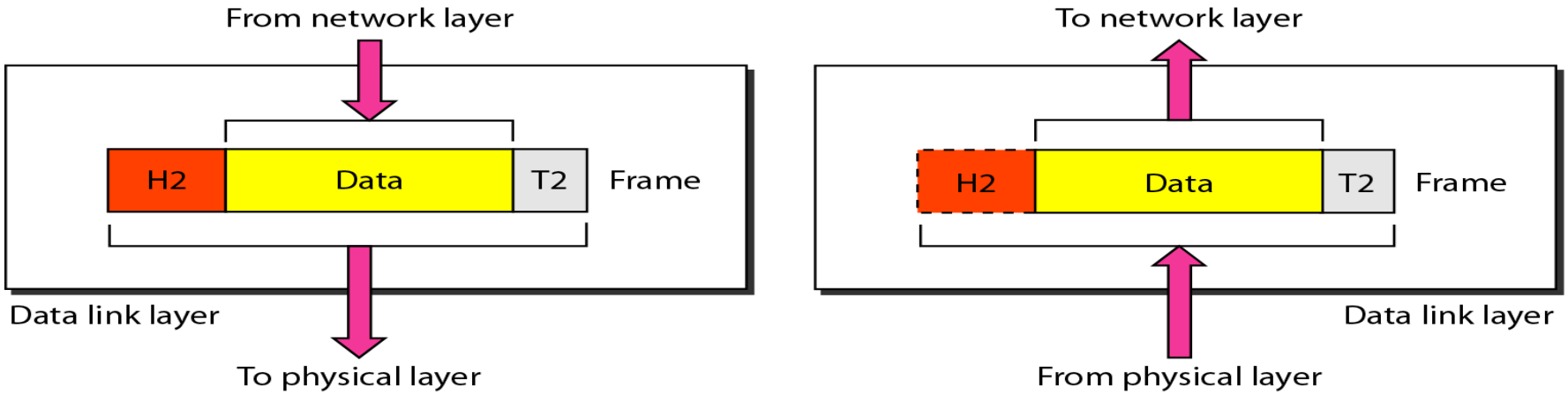
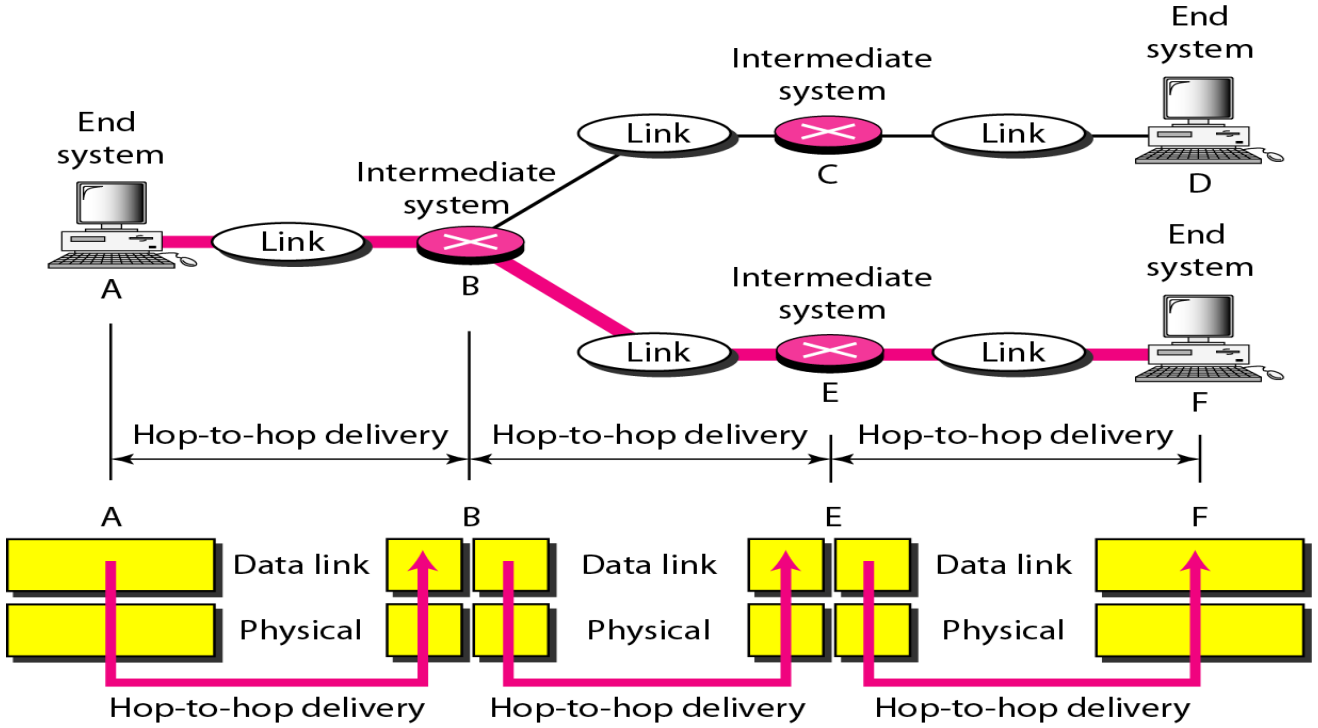


Figure *Hop-to-hop delivery*



Note

The physical layer is responsible for movements of individual bits from one hop (node) to the next.

Figure *Physical layer*

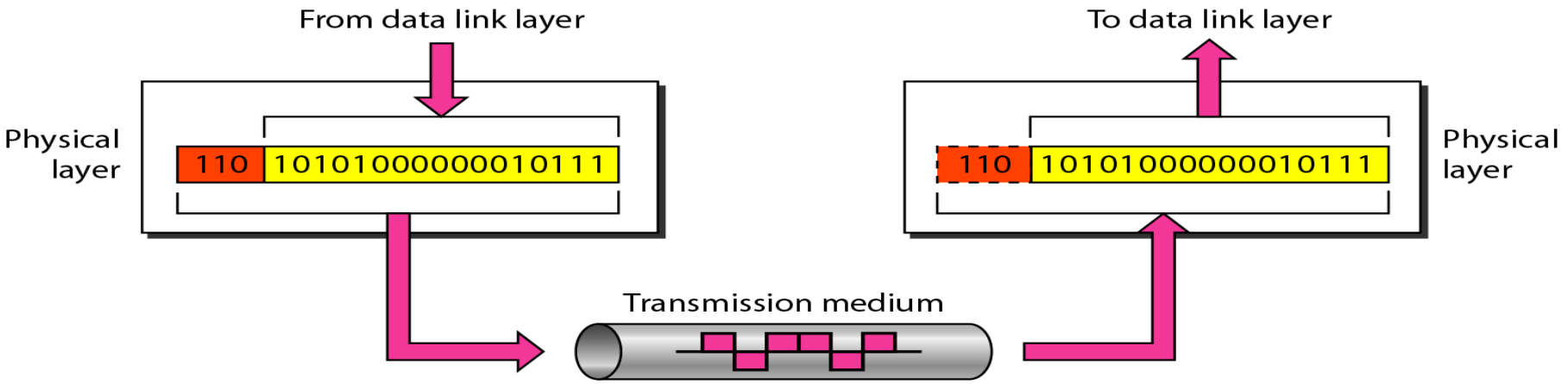
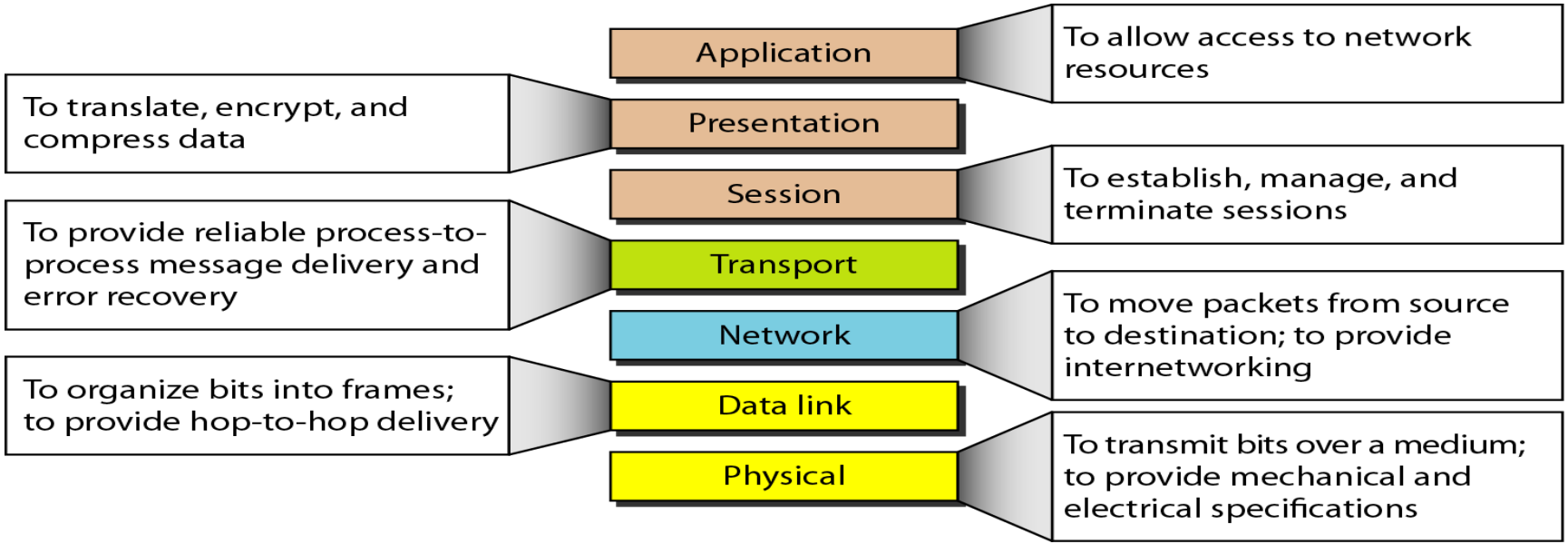


Figure *Summary of layers*



TCP/IP PROTOCOL SUITE

The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.

Topics discussed in this section:

Physical and Data Link Layers
Network Layer
Transport Layer
Application Layer

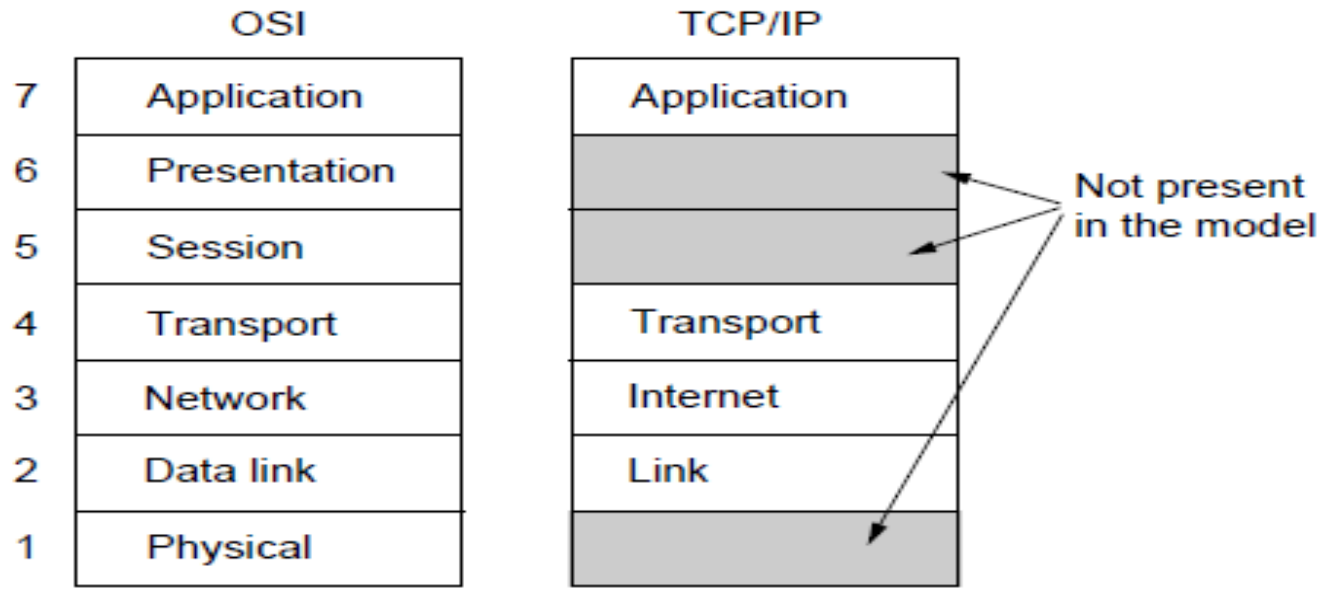
The TCP/IP Reference Model Layers

TCP/IP was developed in the **1970s** and adopted as the protocol standard for ARPANET (the predecessor to the Internet) in **1983**.

Link layer(Host to network layer)

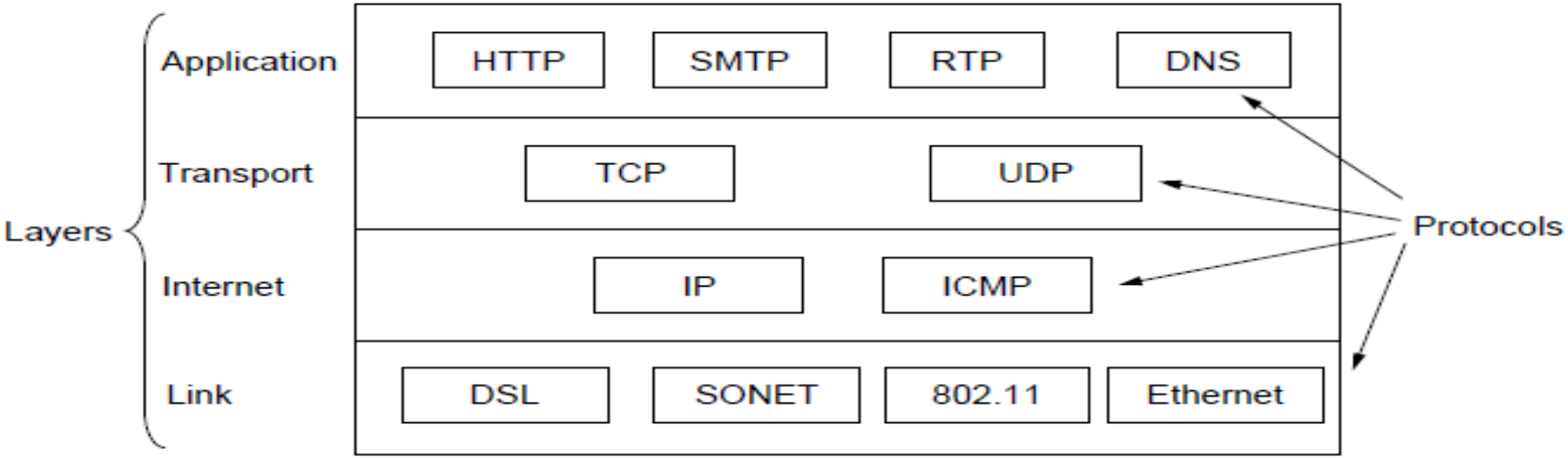
- Internet layer
- Transport layer
- Application layer

The TCP/IP Reference Model (1)



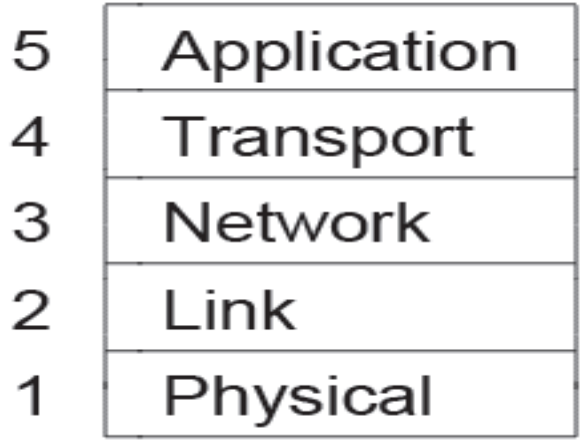
The TCP/IP reference model

The TCP/IP Reference Model (2)



The TCP/IP reference model with some protocols we will study

The Updated Model



ADDRESSING

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port & application specific

Topics discussed in this section:

Physical Addresses
Logical Addresses
Port Addresses
application specific

Figure *Addresses in TCP/IP*

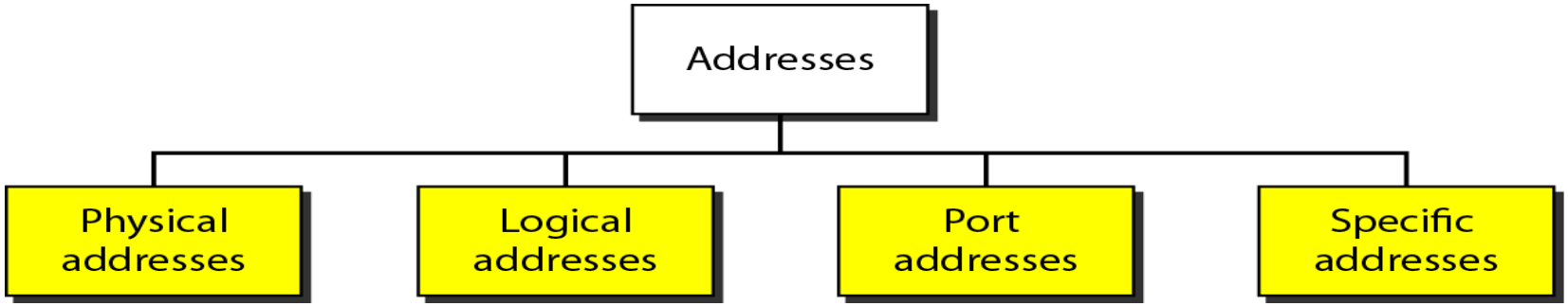
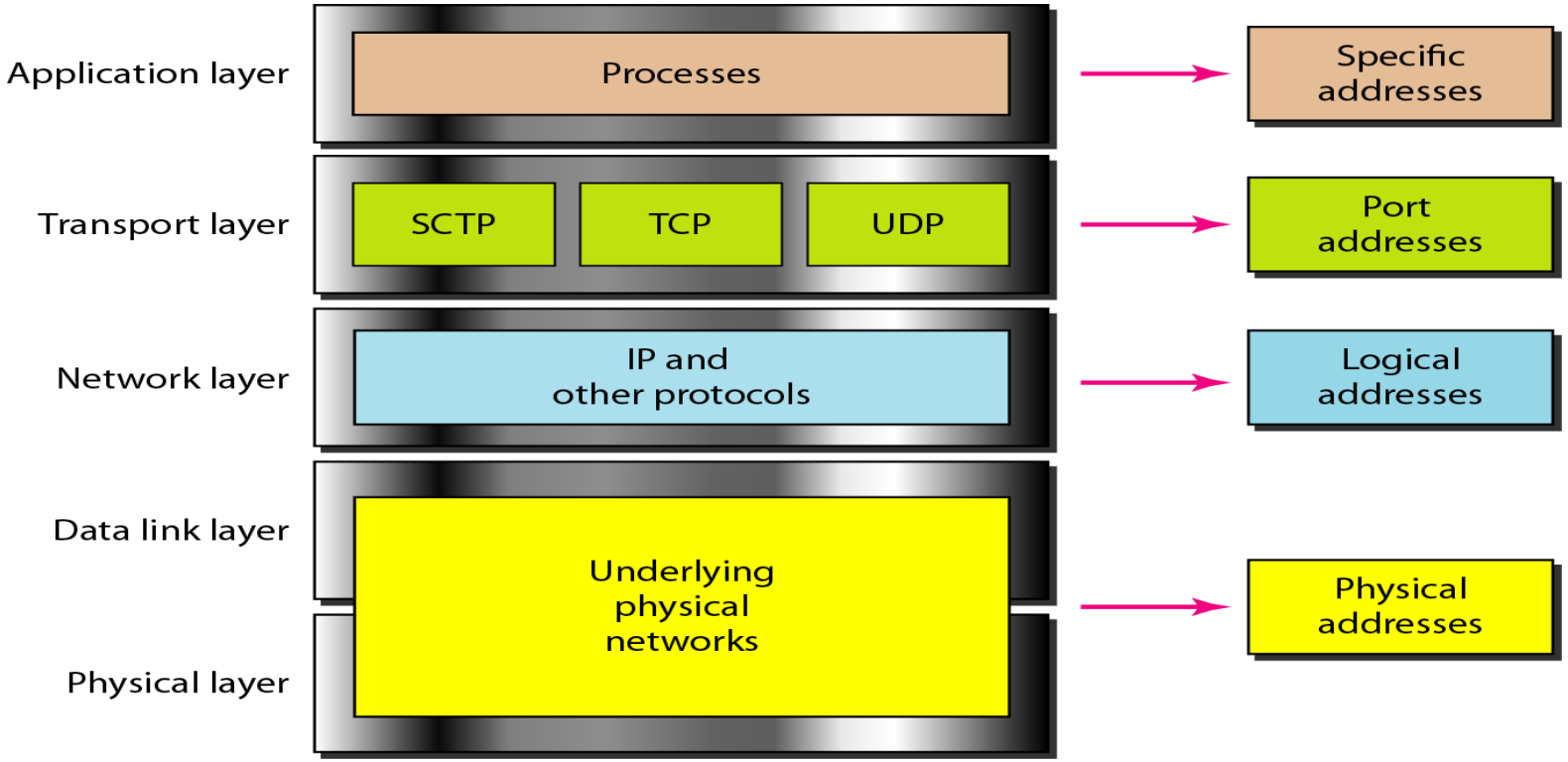
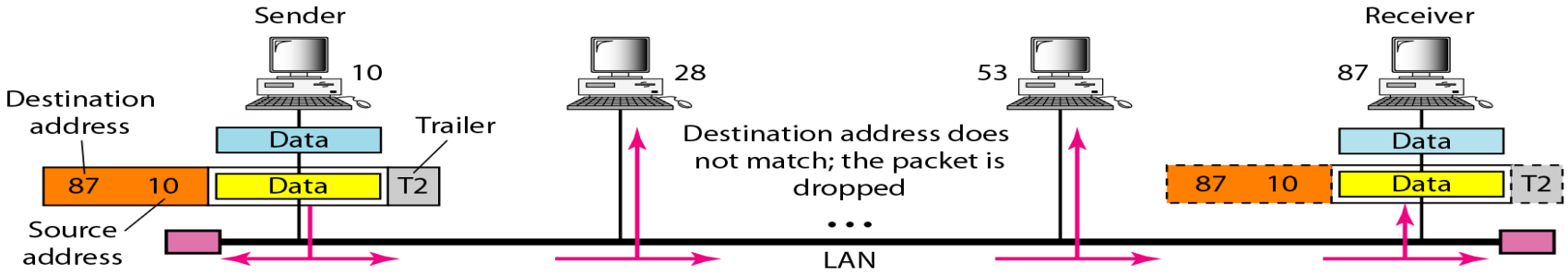


Figure *Relationship of layers and addresses in TCP/IP*



Example 1

In Figure, a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). As the figure shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver.



Example 2

Most local-area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

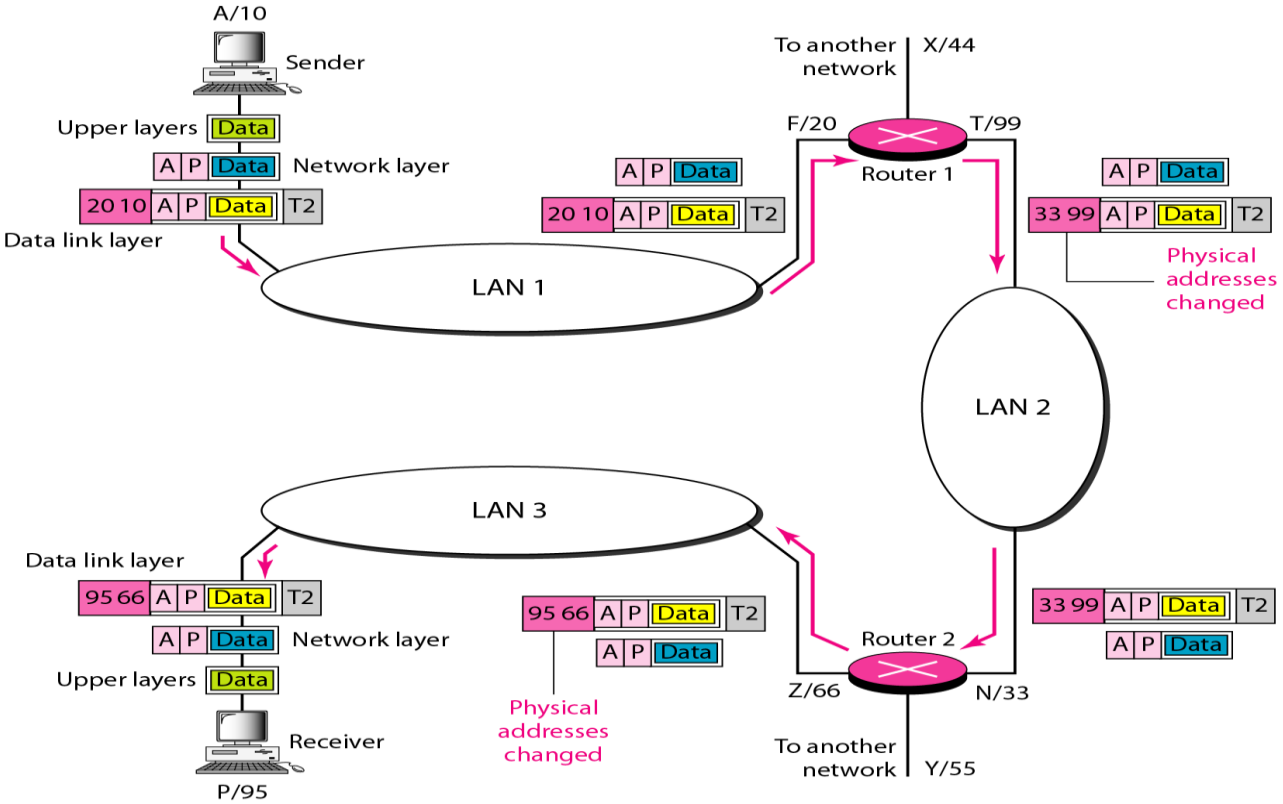
07:01:02:01:2C:4B

A 6-byte (12 hexadecimal digits) physical address.

Example 3

Figure 1.20 shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection.

Figure 1.20 *IP addresses*



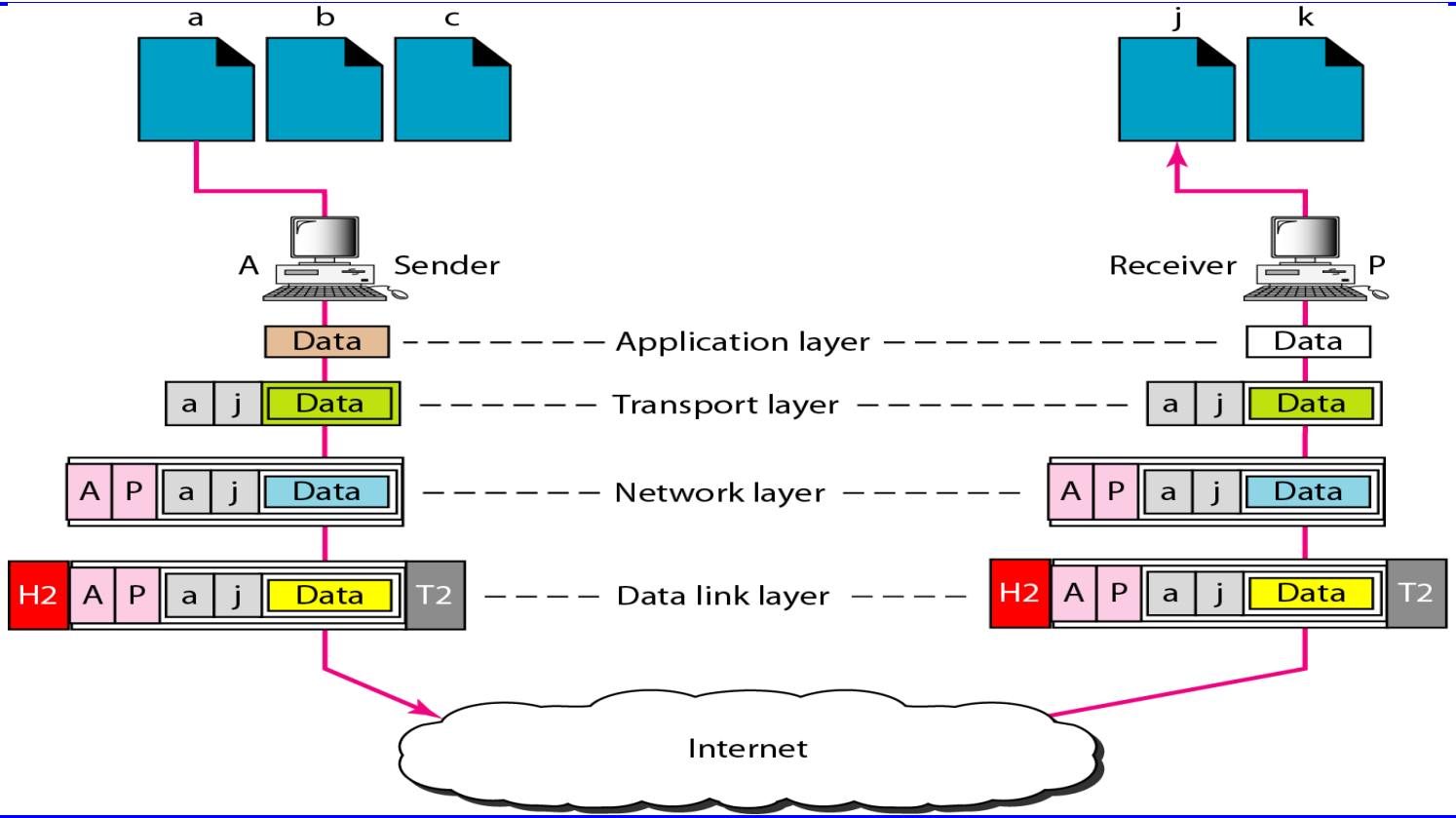
IP ADDRESS or LOGICAL ADDRESS

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	2^{32} = ~4,294,967,296	2^{128} = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456

Example 4

Figure 1.21 shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k. Process a in the sending computer needs to communicate with process j in the receiving computer. Note that although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.

Figure 1.21 *Port addresses*



Note

The physical addresses will change from hop to hop, but the logical addresses usually remain the same.

Example 5

A port address is a 16-bit address represented by one decimal number as shown.

753

A 16-bit port address represented
as one single number.

Specific Address

- Some applications have user-friendly addresses that are designed for that specific application.
- Examples include the e-mail address (for example, co_sci@yahoo.com) and the Universal Resource Locator (URL) (for example, www.mhhe.com).

Internet

- Internet stands for Internetwork(Network of networks)
- a collaboration of more than 100 of 1000 interconnected networks.

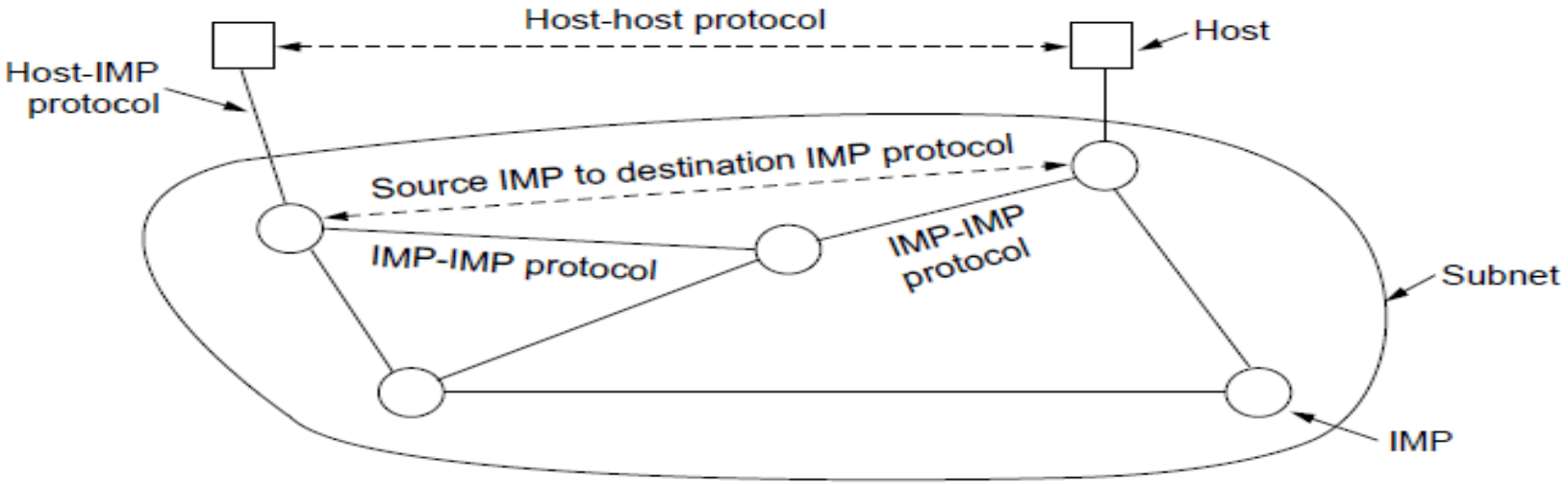
- In mid of 1960:

  - The Advanced Research Projects Agency (ARPA) in the department of defense was interested in finding a way to connect computers so that the researchers they funded could share their findings, to reduce costs and eliminating duplication of effort.

Brief History

- In1967
  - ARPA presented its ideas for ARPANET, small network of connected computers (mainframe).
- In 1969
  - ARPANET was reality. Four nodes at the UNV. Of California,(at los angles and Santa Barba), univ. of utah and SRI (Stand ford Research Institute)connected via **IMPs (Interface message Processors**)computers to form a network. Software called Network Control Protocol (NCP) provided communication between the hosts.

The ARPANET



The original ARPANET design

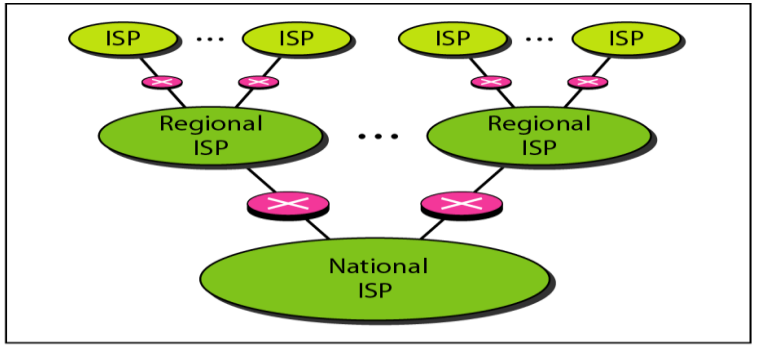
Brief History

- ARPANET adopted TCP/IP on January 1, 1983, and from there researchers began to assemble the “network of networks” that became the modern Internet. The online world then took on a more recognizable form in 1990, when computer scientist Tim Berners-Lee invented the World Wide Web.
- **Internet today**
  - Made up of many wide and local area networks joined by connecting devices and switching stations. Today most end users use the **services of internet service providers (ISPs).**

Internet Service Providers (ISPs)

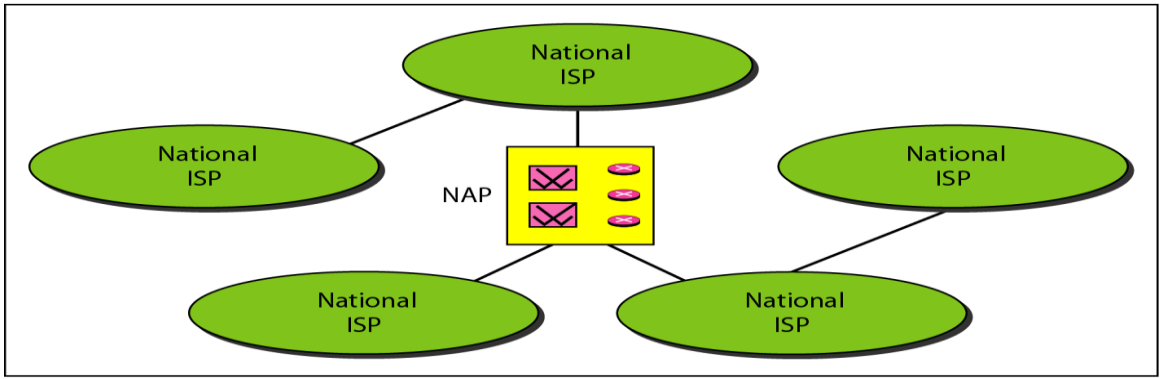
- Hierarchical organization of the Internet includes:
  - **International Internet Service Providers**
  - **National Internet Service Providers**
  - **Regional Internet Service Providers**
  - **Local Internet Service Providers**

Internet Service Providers (ISPs)



a. Structure of a national ISP

NAP-> Network Access Point

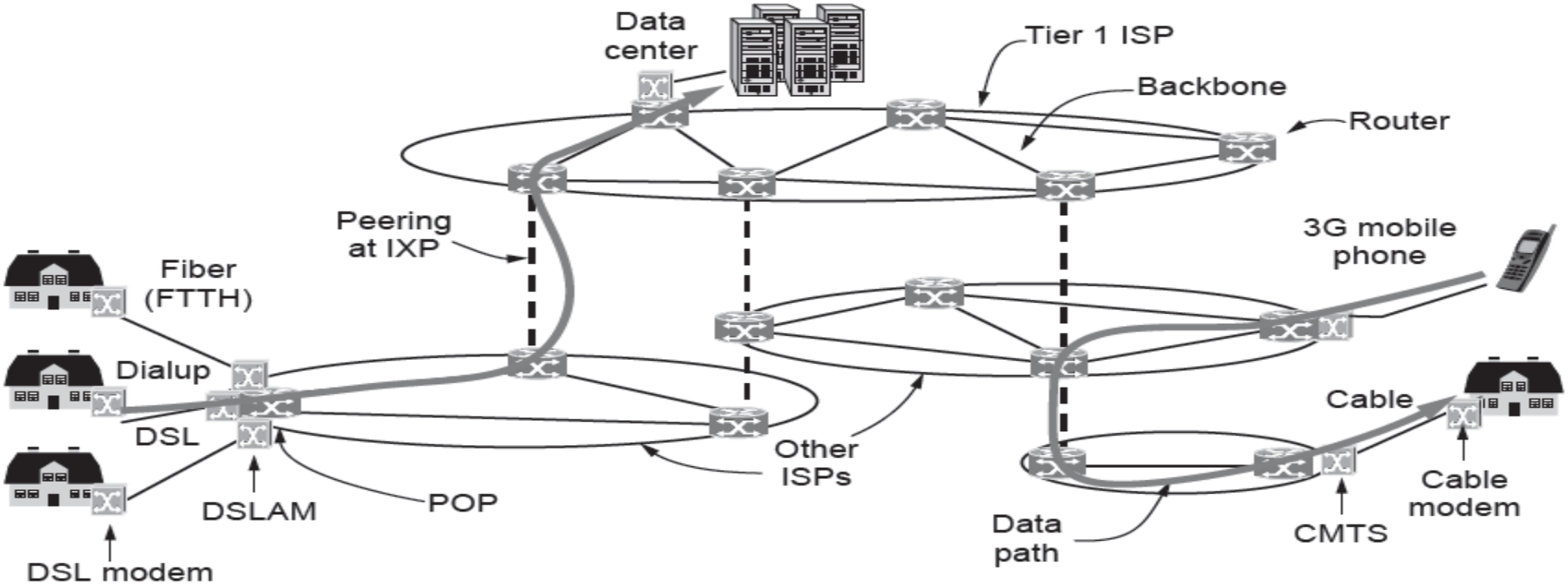


b. Interconnection of national ISPs

Types of internet connections

- Dial-up(Telephone)
- DSL (Digital Subscriber Line)
- Cable TV
- Mobile(Wireless)
- FTTH

Architecture of the Internet



Overview of the Internet architecture

MCQ’s

- In the layer hierarchy as the data packet moves from the upper to the lower layers, headers are _____

a) Added
b) Removed
c) Rearranged
d) Modified

Answer: Option a

- Communication between a computer and a keyboard involves _____ transmission.
  a) Automatic
  b) Half-duplex
  c) Full-duplex
  d) Simplex

Answer: Option d

- Which of the following tasks is not done by data link layer?
  a) framing
  b) error control
  c) flow control
  d) channel coding

Answer: Option d

- The network layer is concerned with _____ of data.

  a) bits
  b) frames
  c) packets
  d) bytes

Answer: Option C

- The network layer protocol for internet is _____

a) ethernet
b) internet protocol
c) hypertext transfer protocol
d) file transfer protocol

Answer: Option b

- Bluetooth is an example of _____
  a) personal area network
  b) local area network
  c) virtual private network
  d) wide area network

Answer: Option a