Computer Networks (102044501)

Credit – 4

Lecture – 3, Lab Hours – 2

Presented By:

Prof. Brijesh Patel

Reference Books

1. Andrew S Tanenbaum, “Computer Networks”, 5thEdition, Pearson Education

2. Behrouz A Forouzan, “Data Communication and Networking”, 5th Edition, McGraw Hill

3. James Kurose and Keith Ross, “Computer Networking- A Top-Down approach”, 6th edition, Pearson

4. William Stallings, “Data and Computer Communication”, 10th Edition, Pearson Education

Course Outline

- Introduction
- Data Link Layer - Logical Link Control Sublayer
- Data Link Layer - Medium Access Control Sublayer
- The Network Layer
- The Transport Layer
- The Application Layer

Lab Contents

- Cisco Packet Tracer simulator – routing, topologies, DHCP, DNS, HTTP, default, static and dynamic routing (RIP).
- Implementation for identify class of IP address, First, Last and Range of IP addresses.
- Study of various networking commands in Windows
- Configure IIS server and FTP server
- Wire shark Packet Capturing Tool
- Socket Programming for TCP and UDP

Course Outcomes

1. Understand network fundamental, concepts of OSI reference model and real-world protocol suite such as TCP/IP.

2. Learn different link layer terminologies like error detection-correction, multiple access protocol and link layer addressing used in network.

3. Ability to design network architecture and to apply various routing algorithms for network-layer packet delivery.

4. Learn essential principles of a connectionless and connection-oriented protocols used for reliable data transfer, flow control and congestion control.

Unit 1

Introduction

Understanding of Network and Internet, Network Topologies, The OSI Model, TCP/IP Protocol Suite, Guided and Unguided Transmission Media, Network Devices, Fundamental of Circuit-Switched and Packet-Switched Networks, Performance Metrics, Understanding of Delay, Loss and Throughput in the packet-switching network

Internet Usage

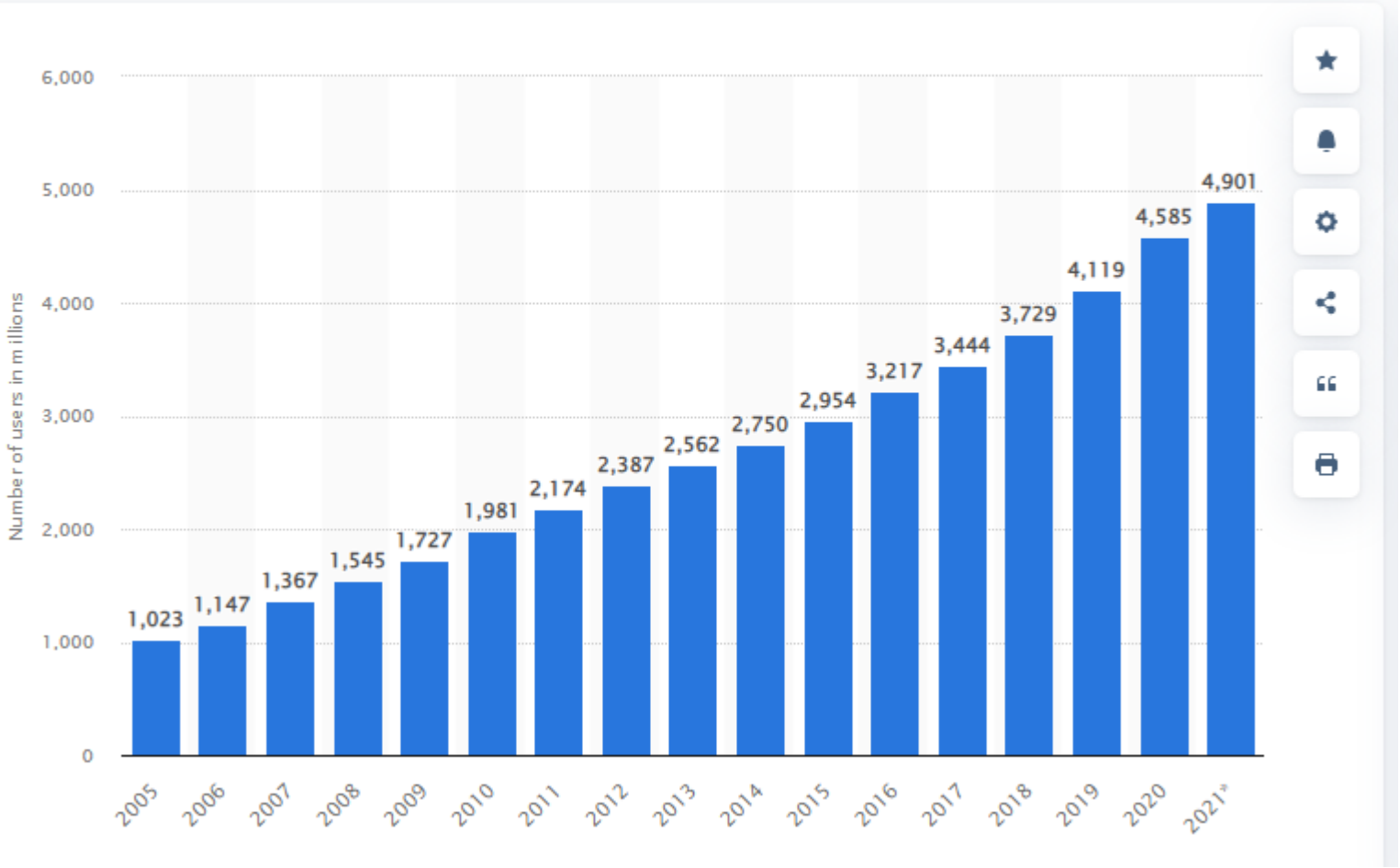
• Internet is arguably the largest engineered system ever created by mankind.

• With hundreds of millions of connected computers, communication links, and switches; with billions of users who connect via laptops, tablets, and smart phones; and with an array of new Internet-connected devices.

• In 2021, the number of internet users worldwide was 4.9 billion, up from 4.6 billion in the previous year, which means that almost two thirds of the global population is currently connected to the world wide web.

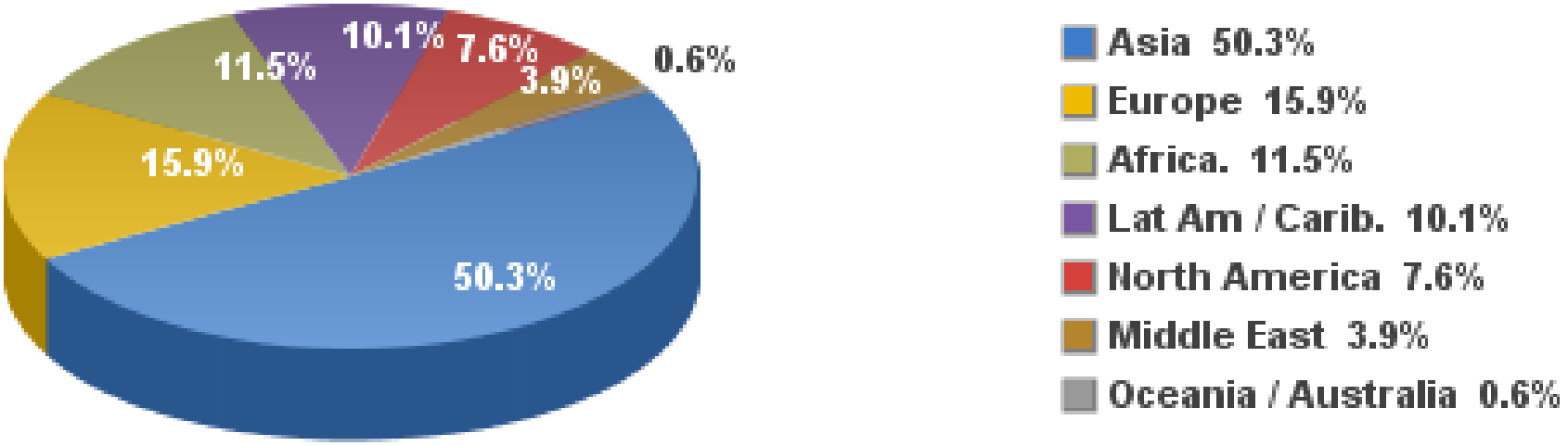
Number of internet users worldwide from 2005 to 2021

(in millions)



https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

Internet Users Distribution in the World - 2020 Q1



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 4,574,150,134 Internet users in March 3, 2020

Source: https://www.internetworldstats.com/stats.htm

Internet 2022 Usage in Asia

Internet Users, Facebook Subscribers & Population Statistics for 35 countries and regions in Asia

INTERNET USERS AND 2022 POPULATION STATISTICS FOR ASIA						
ASIA REGION	Population (2022 Est.)	Pop. % World	Internet Users 30-JUNE-2022	Penetration (% Pop.)	Internet % Users	Facebook 30-JUNE-2022
Asia Only	4,327,333,821	54.9 %	2,772,013,116	64.1 %	53.4 %	1,159,867,200
Rest of World	3,548,431,766	45.1 %	2,415,095,049	68.1 %	46.6 %	1,719,703,577
All the World	7,875,765,587	100.0 %	5,187,108,165	65.9 %	100.0 %	2,879,570,777

Source: https://www.internetworldstats.com/stats3.htm#asia

Computer Network

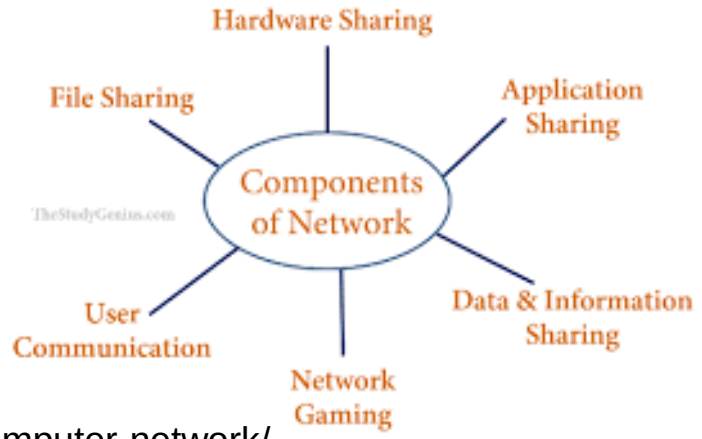
- It is a collection of computers and peripherals devices connected by communication links that allow the network components to work together.

- The network components may be located at any remote place or within the same area.

https://cyber.olympiadsuccess.com/class-4-computer-networks

The Need of Networking

- Sharing Data
- High Reliability
- High Performance
- Scalable
- Sharing of Resources
- Sending Data at Low Cost
- Increased Communication Speed and Accuracy
- Higher Security
- Easy System Access
- Integration of Data Processing and Office Automation
- Multiple Transfers
- Productivity



https://www.thestudygenius.com/what-is-computer-network/

Advantages of Networking

- Resource Sharing
- High Reliability and Availability
- Communication Media
- High Speed
- Easy Transfer
- System Evolution
- Multiple Vendor Support
- Improved Response and Performance
- Decentralization of Data Processing Functions
- Flexibility of Equipment Location

Disadvantages of Networking

- A distributed data raises problems of integrity, security and privacy of data.
- More equipment will be procured than actually required in the system.
- Overall cost of constructing and managing network is high.
- Difficulty in managing and enforcing the standards. Installations and administration of installed components in network requires skilled person, which in turn increase the overall cost of a system.

What is the Internet?[1]

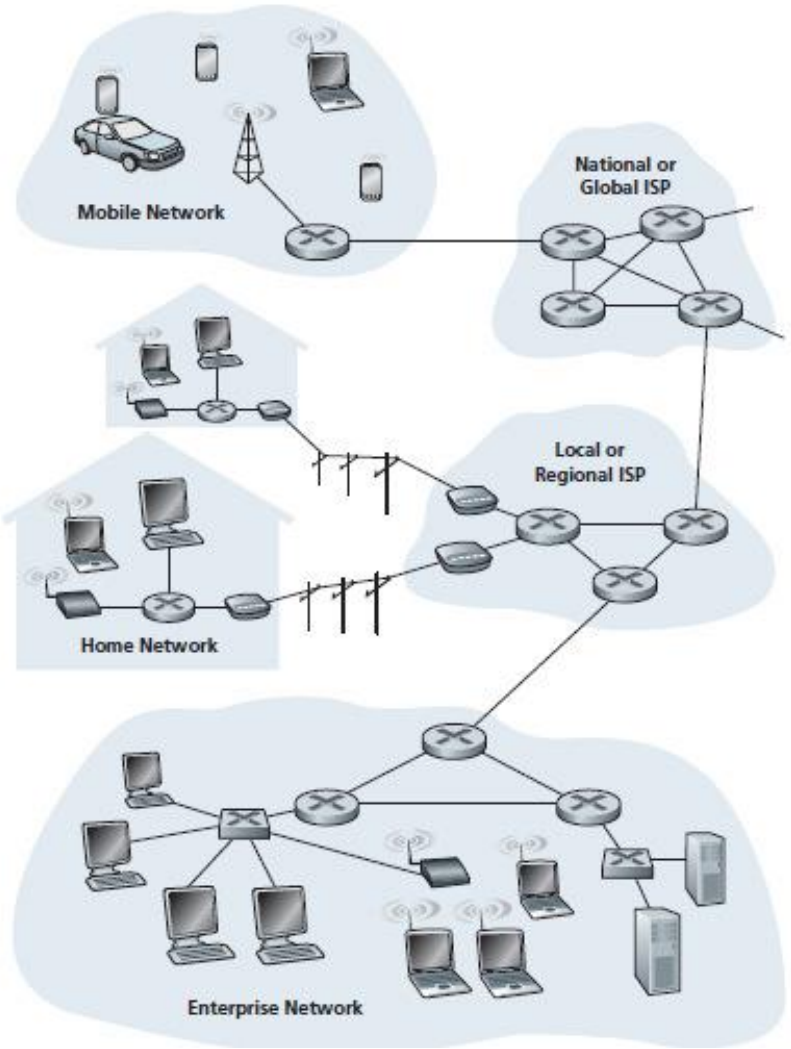
- The Internet is a computer network that interconnects hundreds of millions of computing devices throughout the world.
- Devices are called **hosts** or **end systems**.
- End systems are connected together by a network of communication links and **packet switches**.
- Different links can transmit data at different rates, with the **transmission rate** of a link measured in bits/second.
- **Segments, Encapsulation and Packets.**
- **Packet Switching: Routers and Link-layer switches**
- The sequence of communication links and packet switches traversed by a packet from the sending end system to the receiving end system is known as a **route** or path through the network.

1. Computer Network: A Top-down Approach, Kurose (Fifth Edition)

What is the Internet?

- End systems access the Internet through **Internet Service Providers** (ISPs).
- Internet run protocols that control the sending and receiving of information within the Internet.
- **The Transmission Control Protocol** (TCP) and the **Internet Protocol** (IP) are two of the most important protocols in the Internet.
- Internet standards are developed by the **Internet Engineering Task Force** (IETF).
- The IETF standards documents are called **Requests for Comments** (RFCs).

What is the Internet?



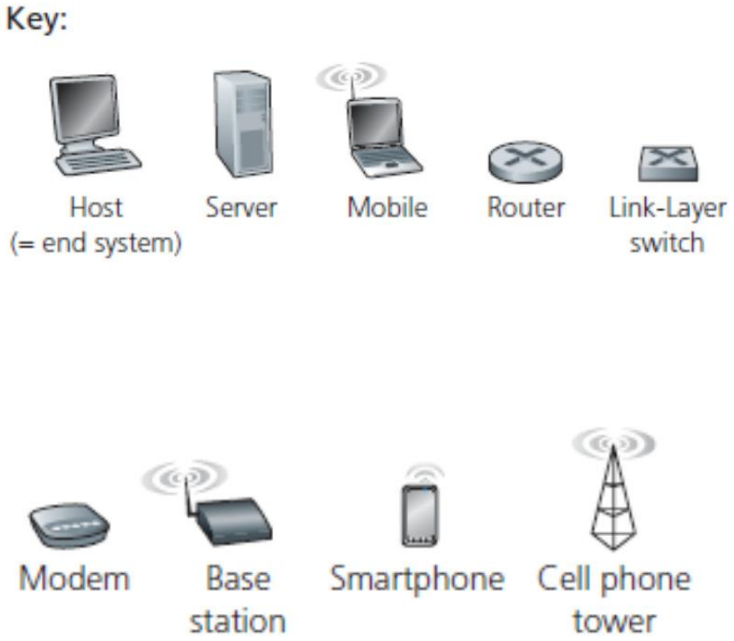


Figure Some pieces of the Internet

Protocol

- **Protocol is a set of Rules**: A protocol defines the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event.

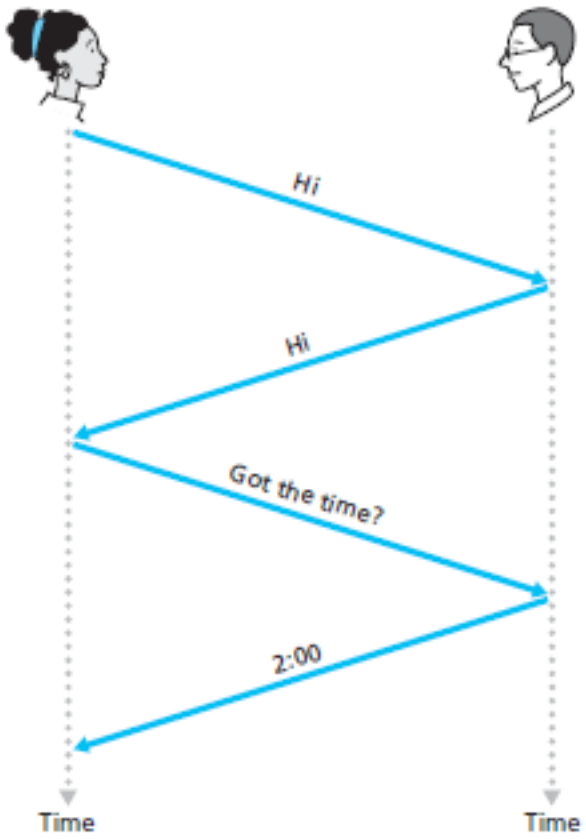
1. **Syntax:** structure or format of data. 8-bits at sender and receiver.

2. **Semantics:** Meaning of each section of bits.

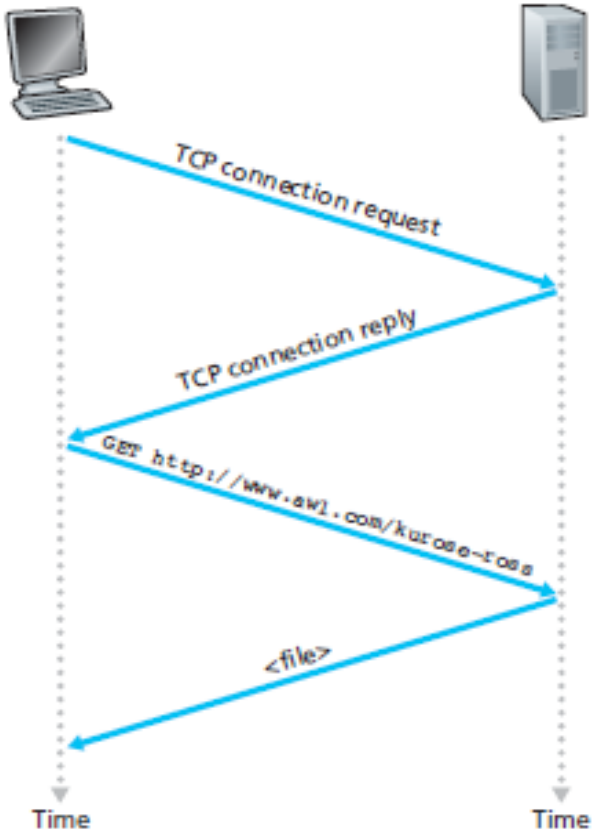
3. **Timing:** two characteristics.
   1. how data should be sent and 2. how fast they can be sent.

Protocol

- Human Protocol



Network Protocol



Network Structure

- Network Edge
  - Applications
  - Hosts
- Network Core
  - Routers
  - Network to Networks
- Physical Media
  - Communication links

Network Edge

- Edge systems are:
  - Desktop computers (Linux, windows, mac etc…)
  - Servers (Web or E-mail servers)
  - Mobile computers (Mobile phones, tablets etc…)

- They are referred to as an End systems.

- End systems are also referred to as hosts because they host (that is, run) application programs such as a Web browser program, a Web server program, an e-mail client program, or an e-mail server program.

Network Edge

Client –Server Programs

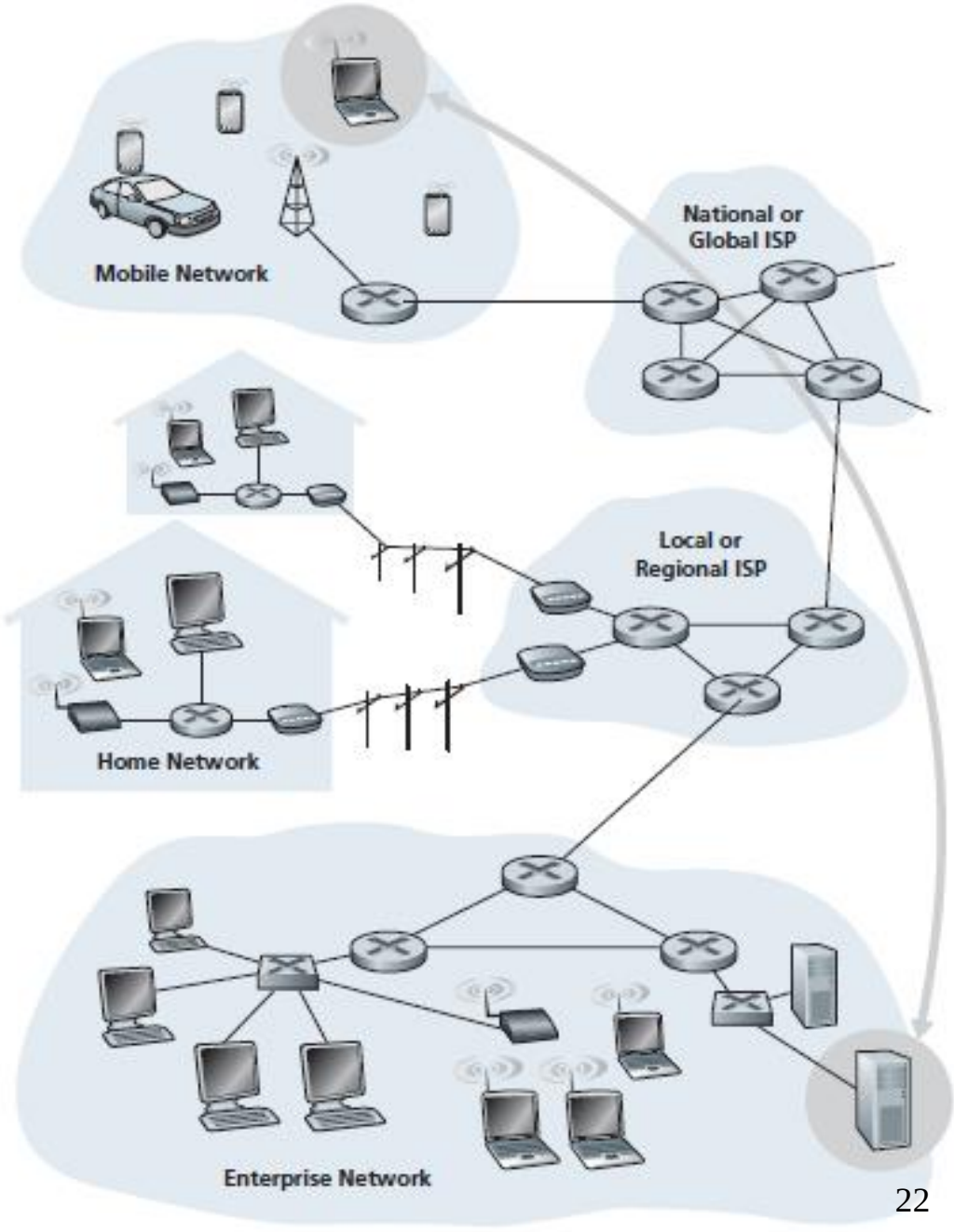


Figure End system interconnection

Network Edge

Access Networks

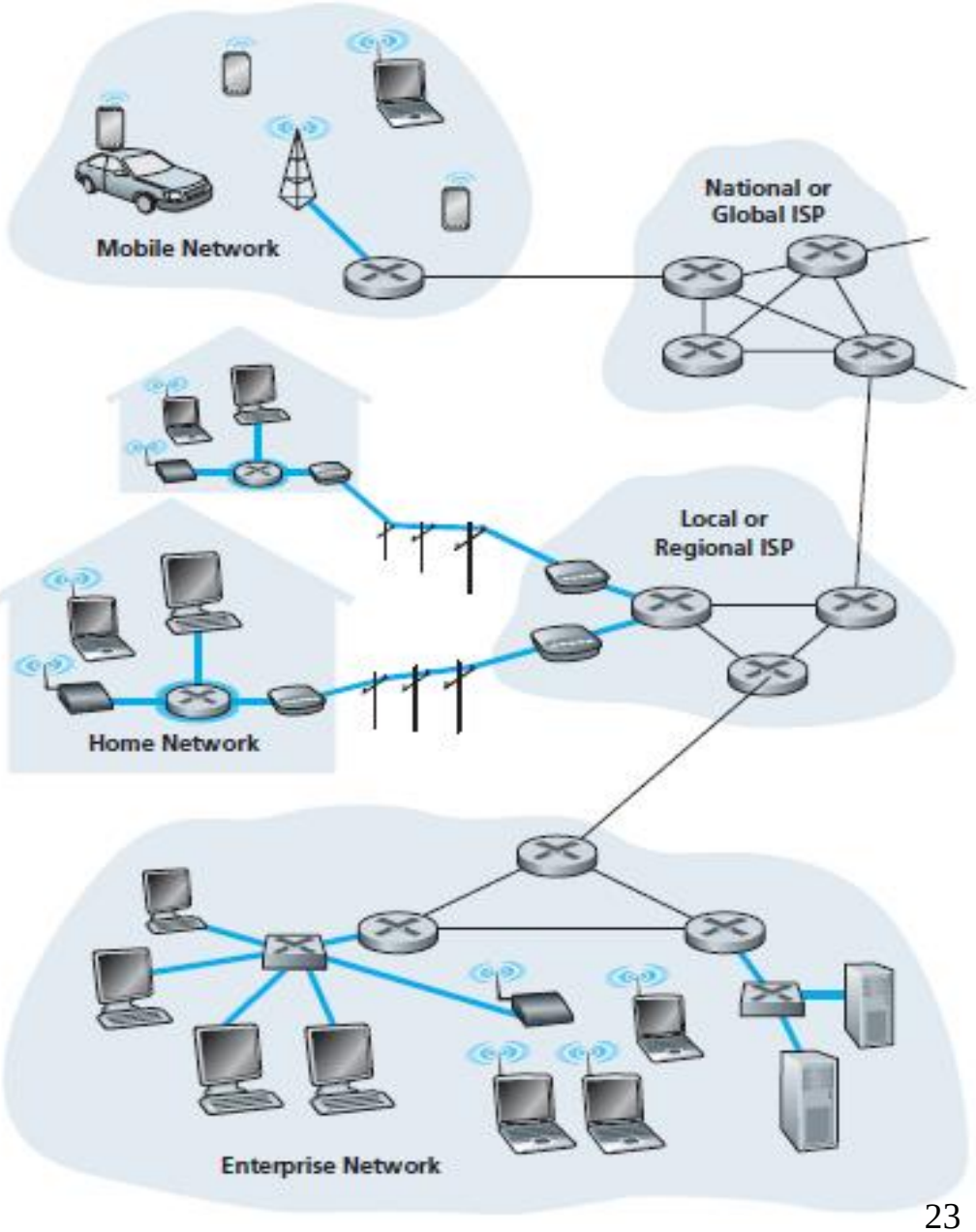
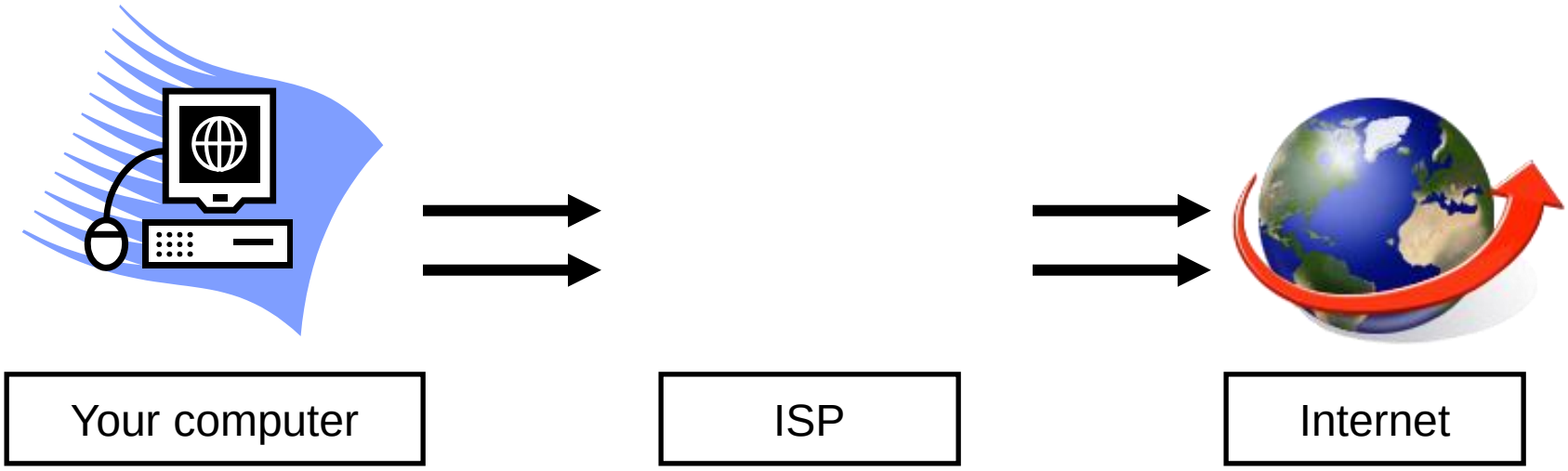


Figure Access Network

Network Edge

Internet Service Provider (ISP)

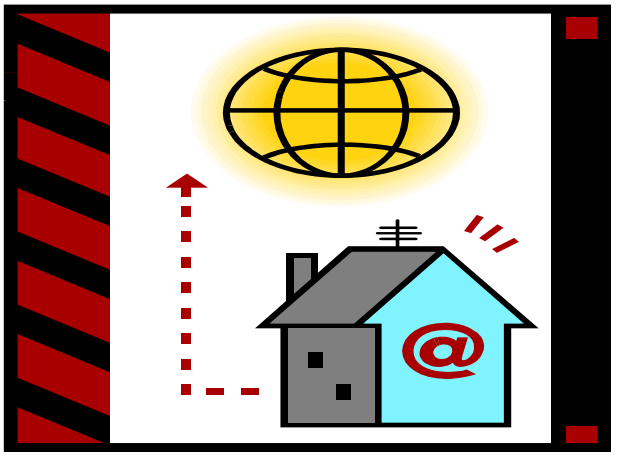
- A company that provides Internet access for customers (examples: Elecon, BSNL, Comcast, Qwest, AOL).
- Your computer connects to the Internet Service Provider (ISP), then to the Internet.



How to connect to the Internet

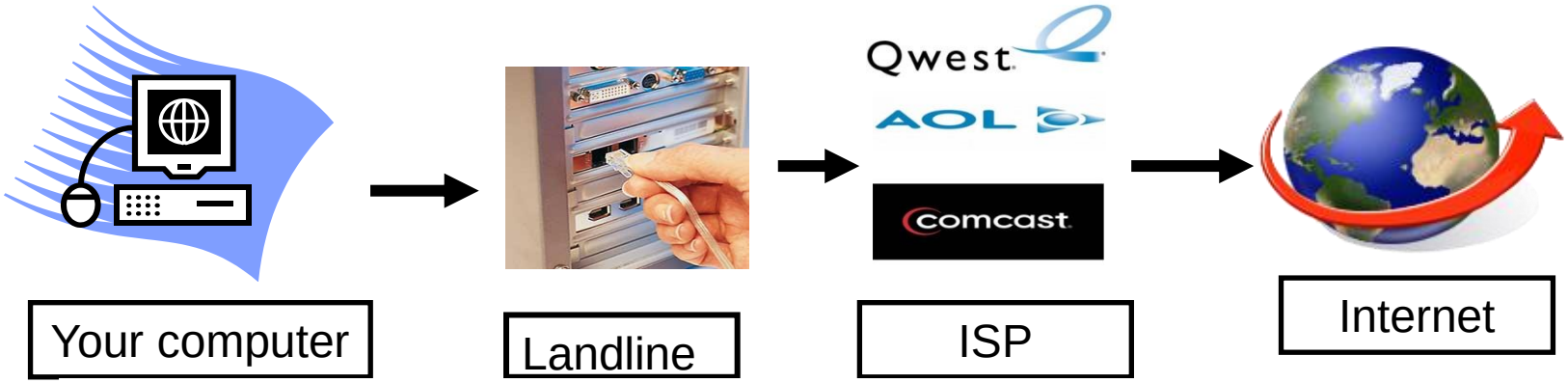
Three main ways to connect to the Internet:

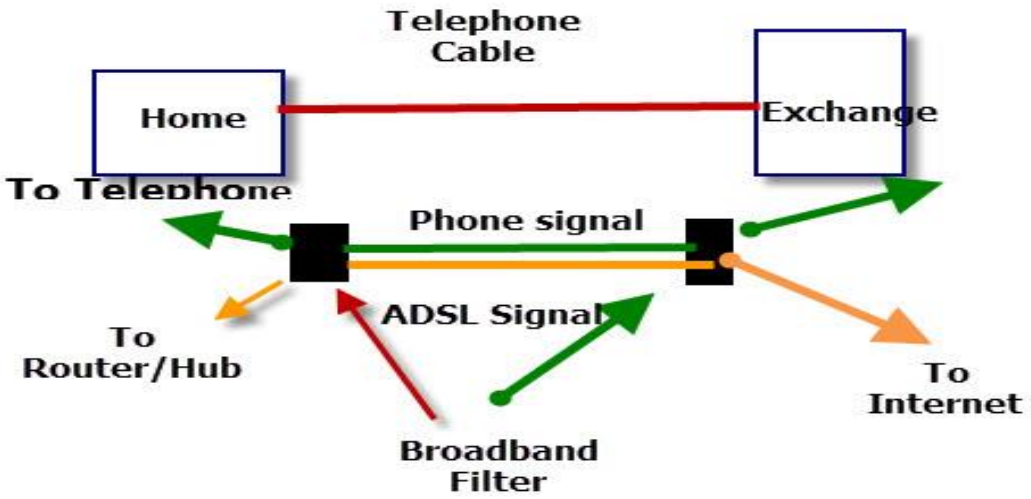
- Dial-Up
- High Speed/DSL
- Wireless Connection (Wi-Fi)



Network Edge

- Access Network:
  - Homes access: Dial Up Internet connection

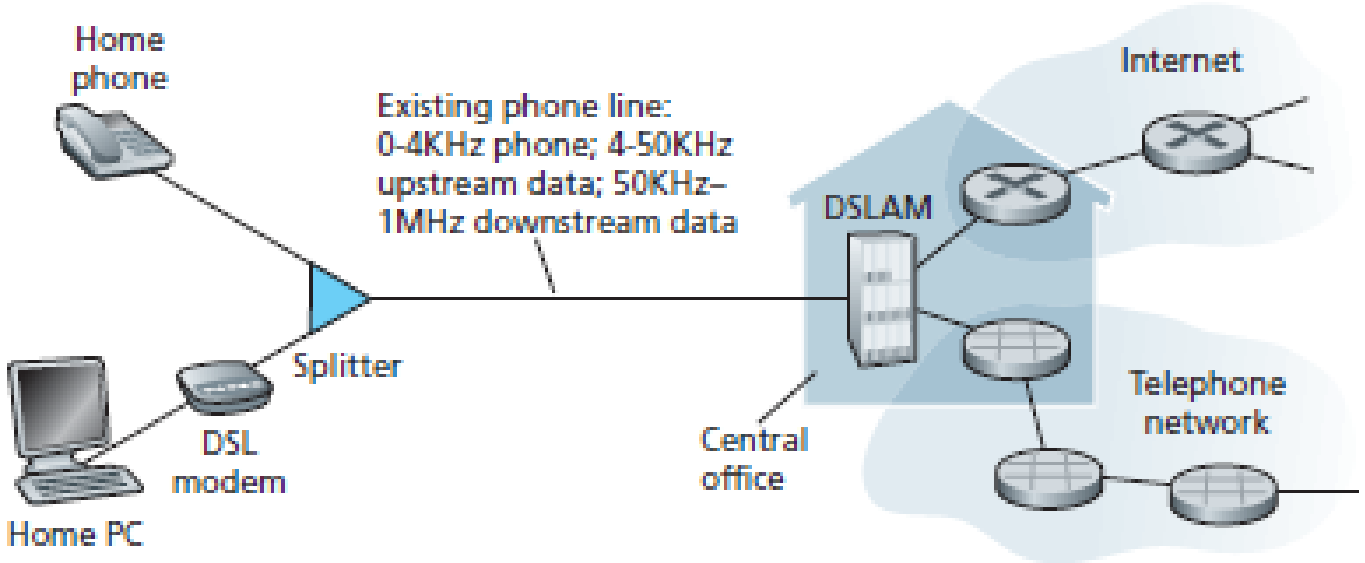




Source: http://www.steves-internet-guide.com/wp-content/uploads/2014/01/adsl-phone-lines.jpg

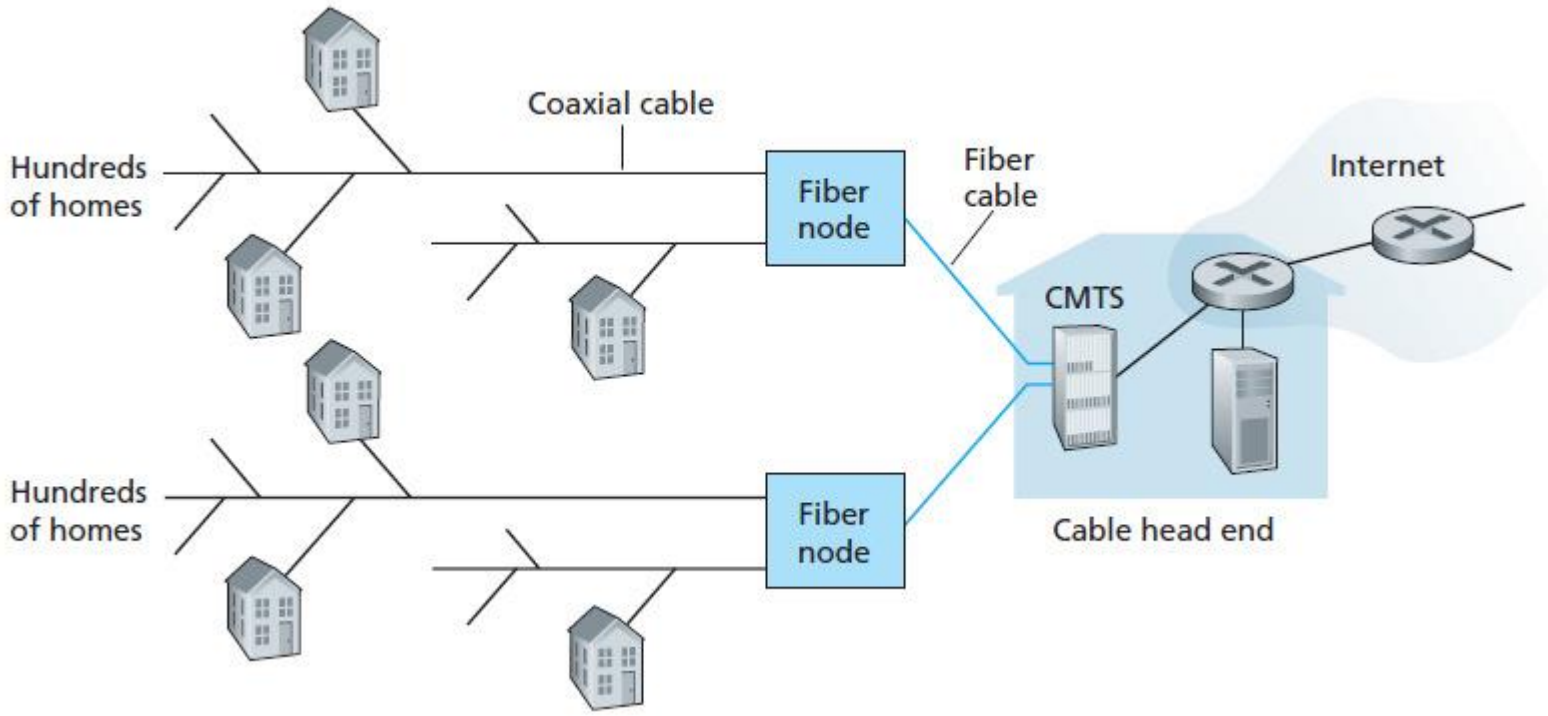
Network Edge

- Access Network:
  - Homes access: DSL (Digital Subscriber Line)
    - The DSL standards define transmission rates of 12 Mbps downstream and 1.8 Mbps upstream [ITU 1999], and 24 Mbps downstream and 2.5 Mbps upstream [ITU 2003]. Because the downstream and upstream rates are different, the access is said to be asymmetric. The actual downstream and upstream transmission rates achieves may be less than the rates noted above.
    - DSLAM - Digital Subscriber Line Access Multiplexer



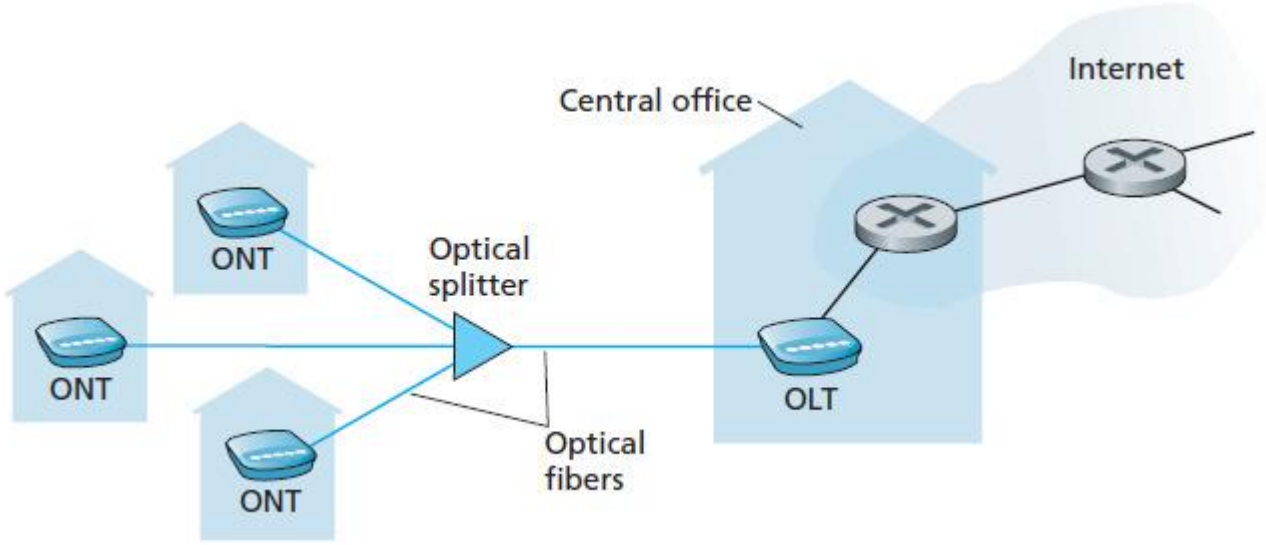
Network Edge

- Access Network:
  - Homes access: cable
    - Hybrid fiber co-axial access Network
      - CMTS- cable modem termination system



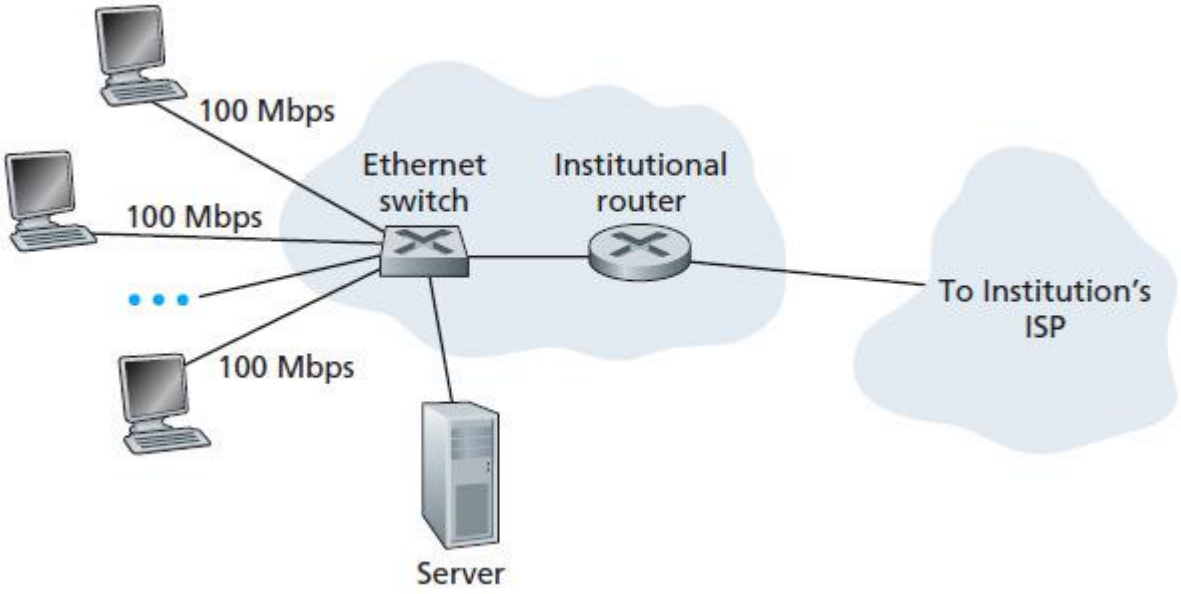
Network Edge

- Access Network:
  - Homes access: FTTH (Fiber-To-The- home)
    - Hybrid fiber co-axial access Network
      - ONT – Optical Network terminator, OLT – optical line terminator



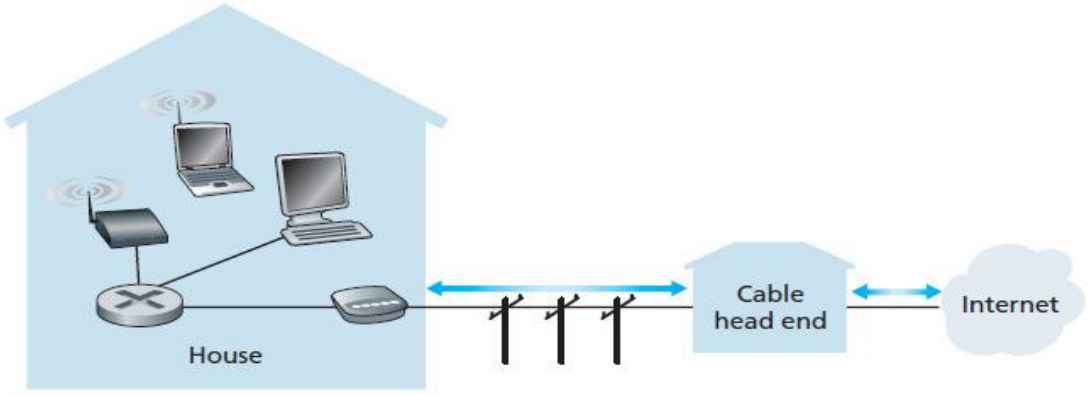
Network Edge

- Access Network:
  - Homes access: Ethernet



Network Edge

- Access Network:
  - Homes access: Wi-Fi
  - Your computer must be a “Wireless enabled” device.
  - Your computer can pick up signals from different wireless networks.
  - Some networks require passwords or a subscription, others are free.



Network Edge

- Access Network: **Wide-Area Wireless Access: 3G and LTE**
  - Employ the same wireless infrastructure used for cellular telephony to send/receive packets through a base station that is operated by the cellular network provider.
  - **Third-generation (3G)** wireless, which provides **Packet-switched wide-area wireless Internet access** at speeds in excess of **1 Mbps.**
  - **Long-Term Evolution (LTE)** has its roots in 3G technology, and can potentially achieve rates in excess of **10Mbps.**
  - **Voice over Long-Term Evolution** (VoLTE) is a standard for high-speed wireless communication for mobile phones and data terminals.

LAN Topologies[2]

- A LAN topology is the basic design of a computer network. It details how key network components such as nodes and links are interconnected.

- Topology, in relation to networking, describes the configuration of the network; including the location of the workstations and wiring connections.

- Basically it provides a definition of the components of a Local Area Network (LAN).

- A topology, which is a pattern of interconnections among nodes, influences a network's cost and performance.

2. Data Communication and Networking, Forouzan (Fourth Edition)

LAN Topologies

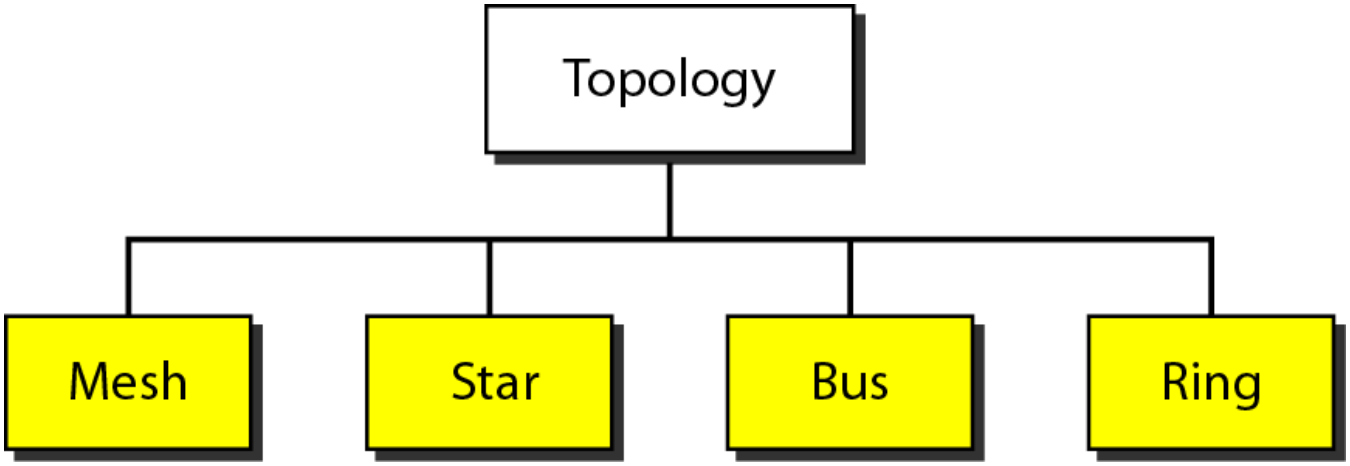


Figure Categories of topology

LAN Topologies

- **Mesh Topology:**
  - Each device has a dedicated point to point link to every device.
  - Dedicated means that the link carries traffic only between two devices connected by the link.
  - Fully connected mesh topology has n (n-1) / 2 links in the network.

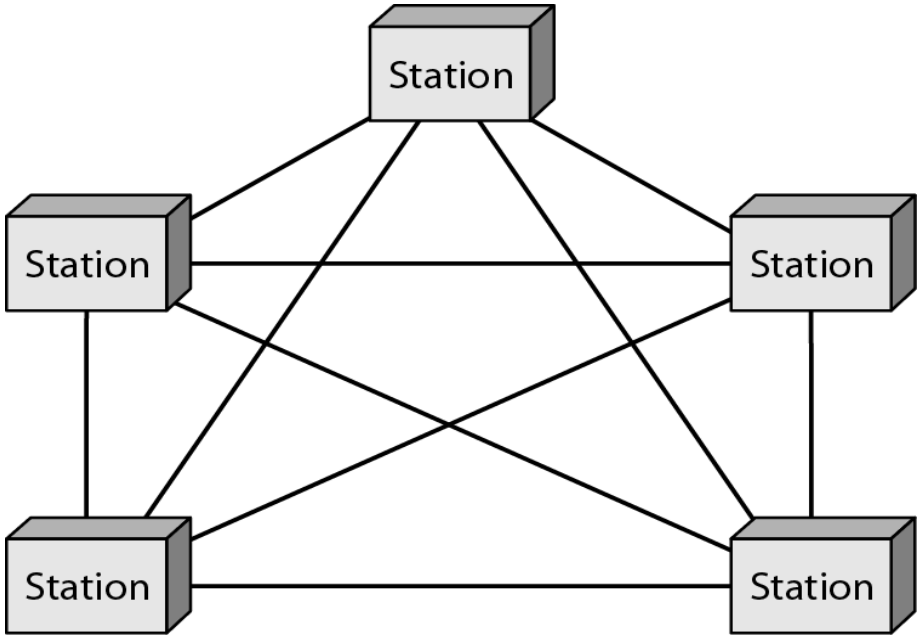


Figure A fully connected mesh topology (five devices)

LAN Topologies

- **Mesh Topology:**

ADVANTAGES

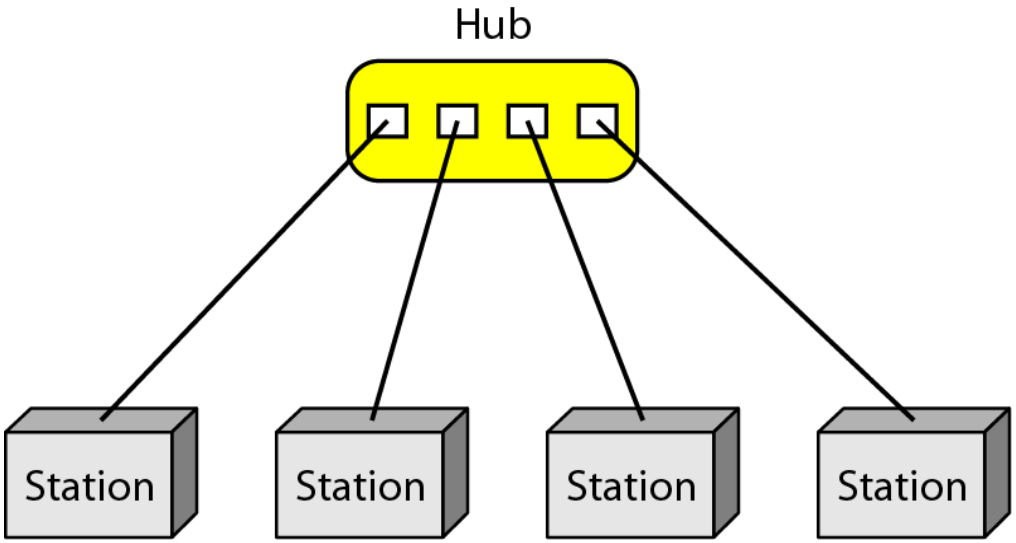
1. Dedicated links guarantees that each connection can carry its own data load, so it eliminates traffic problem.
2. A mesh topology is robust. If one link is unusable it does not harm the entire system.
3. Every message sent travels along a dedicated line one to the intended recipient, thus providing privacy and security.
4. Point-to-point connection makes fault detection and isolation easy.

DISADVANTAGES

1. The amount of cabling required because every device must be connected to every device.
2. The number of I/O ports required will be more.
3. Hardware required to connect each link (I/O ports and cables) can be expensive.

LAN Topologies

- **Star Topology:**
  - All devices connected with a Star setup communicate through a central Hub by cable segments.
  - Signals are transmitted and received through the Hub. It is the simplest and the oldest and all the telephone switches are based on this.
  - In a star topology, each network device has a home run of cabling back to a network hub, giving each device a separate connection to the network. So, there can be multiple connections in parallel.



LAN Topologies

- **Star Topology:**

ADVANTAGES

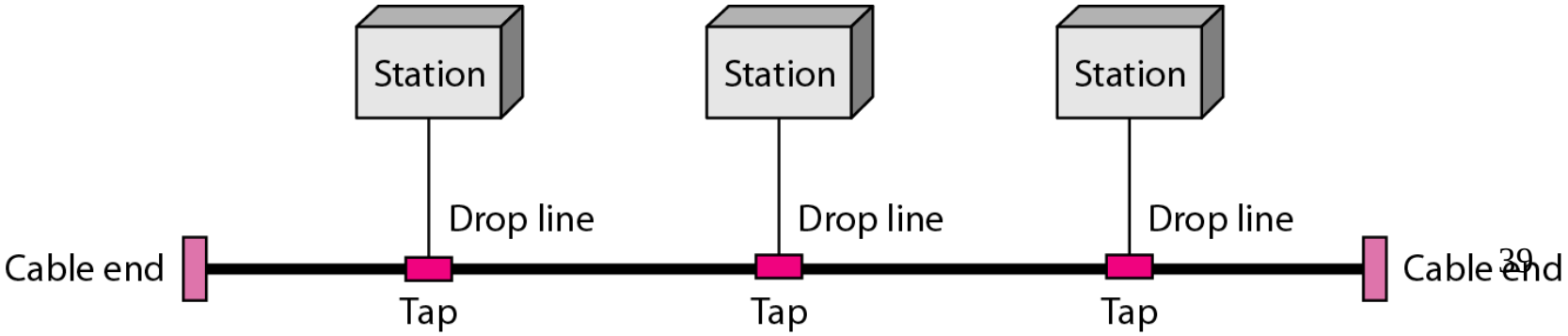
1. Network administration and error detection is easier because problem is isolated to central node.
2. Network runs even if one host fails.
3. Expansion becomes easier and scalability of the network increases.
4. More suited for larger networks.

DISADVANTAGES

1. Broadcasting and multicasting is not easy because some extra functionality needs to be provided to the central hub.
2. If the central node fails, the whole network goes down; thus making the switch some kind of a bottleneck.
3. Installation costs are high because each node needs to be connected to the central switch.

LAN Topologies

- **Bus Topology:**
  - The simplest and one of the most common of all topologies.
  - Bus consists of a single cable, called a Backbone that connects all workstations on the network using a single line.
  - All transmissions must pass through each of the connected devices to complete the desired request. Each workstation has its own individual signal that identifies it and allows for the requested data to be returned to the correct originator.
  - In the Bus Network, messages are sent in both directions from a single point and are read by the node (computer or peripheral on the network) identified by the code with the message.



LAN Topologies

- **Bus Topology:**

ADVANTAGES

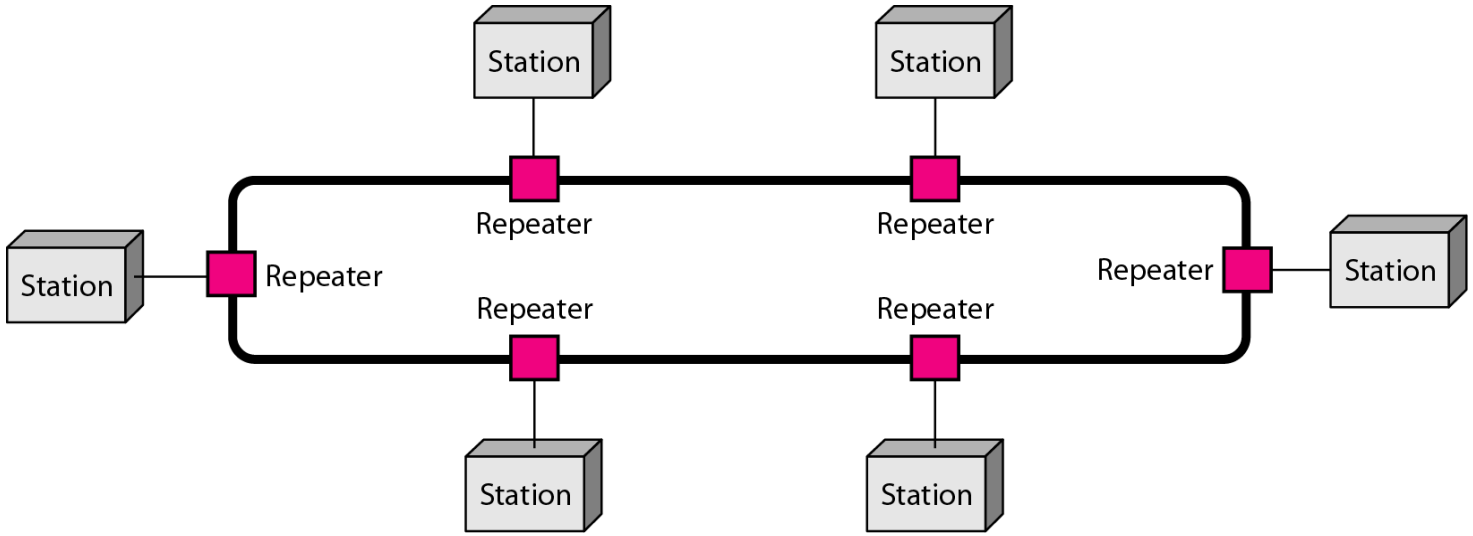
1. Broadcasting and multicasting is much simpler
2. Network is redundant in the sense that failure of one node doesn't effect the network. The other part may still function properly
3. Least expensive since less amount of cabling is required and no network switches are required
4. Good for smaller networks not requiring higher speeds

DISADVANTAGES

1. Trouble shooting and error detection becomes a problem because, logically, all nodes are equal
2. Less secure because sniffing is easier
3. Limited in size and speed

LAN Topologies

- **Ring Topology:**
  - In Ring topology each node is connected to the two nearest nodes so the entire network forms a circle
  - Data only travels in one direction on a Ring network



LAN Topologies

- **Ring Topology**

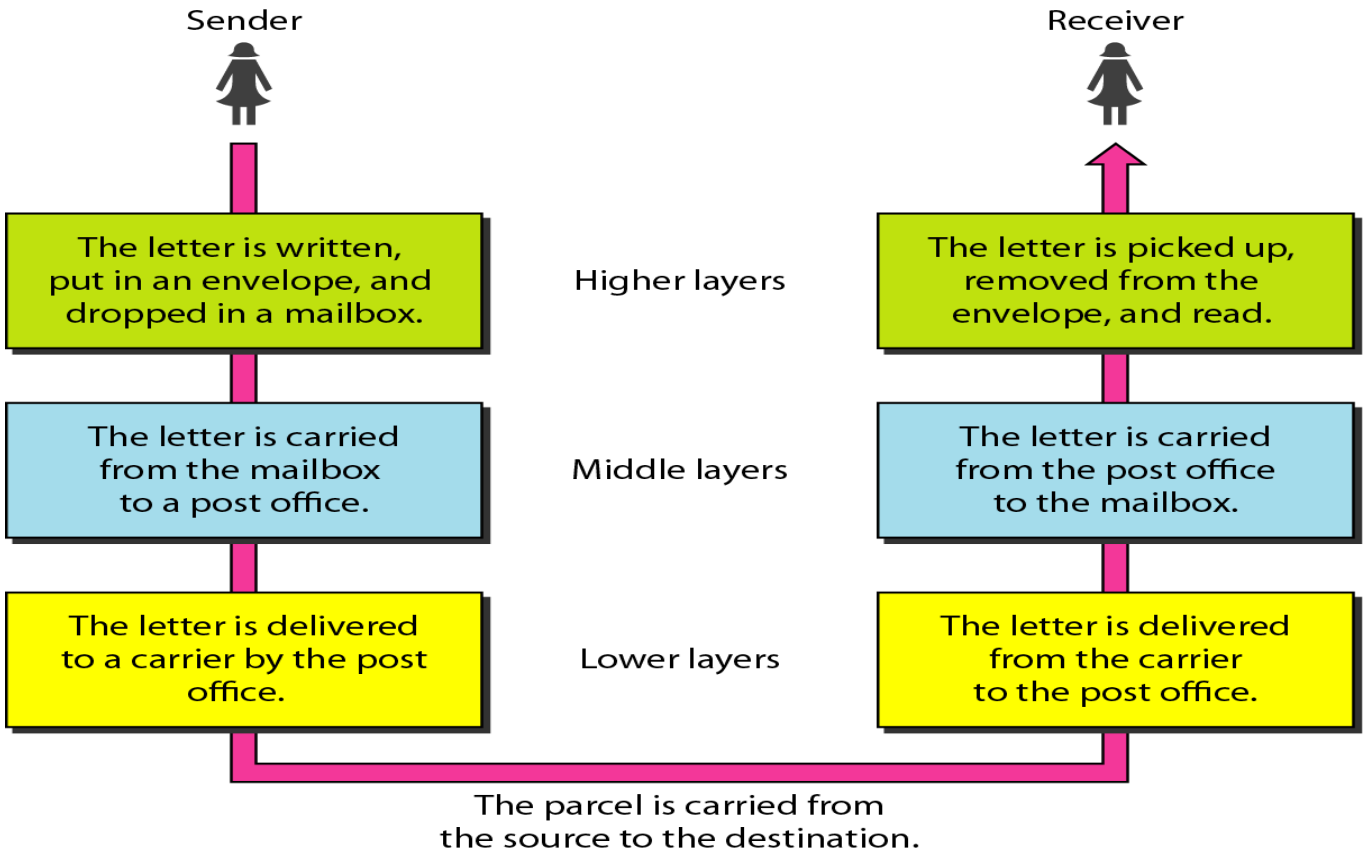
ADVANTAGES

- As it is better to have computers take turns using the connecting Data cable, Ring topologies incorporated a system called Token passing .
- In this topology, to transmit on the wire your computer must have control of the token or wait for the token to be free .
- Larger Token Ring networks use multiple tokens.

DISADVANTAGES

- The drawback to this type of topology is that a single malfunctioning workstation can disable the whole network .
- To make sure all the information is sent, the receiving PC sends the token back to the sending PC after it has received all the data.
- If the sending PC is finished sending it passes the token to the next PC.

Protocol Layers and Their Service[2] Models

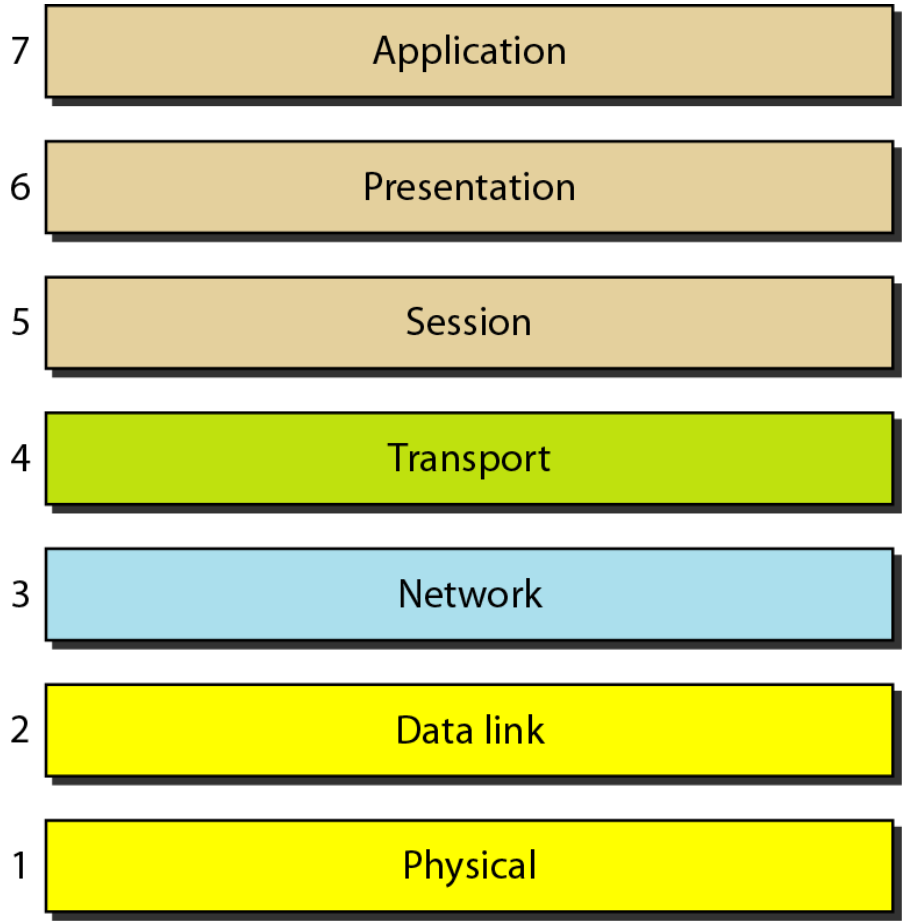


2. Data Communication and Networking, Forouzan (Fourth Edition)

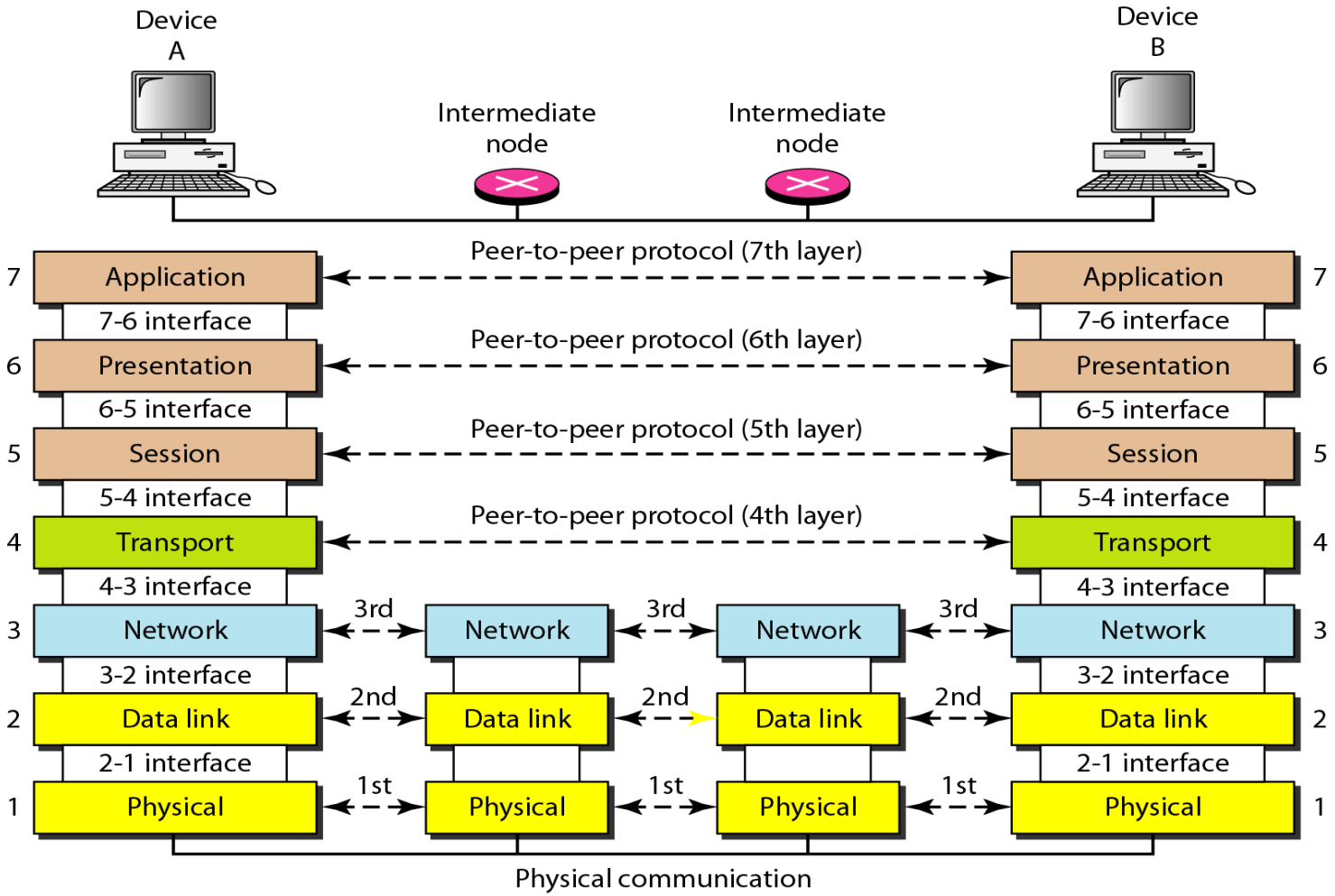
The OSI Model

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.

The OSI Model – Layered Architecture



Interaction between Layers



Interaction between Layers

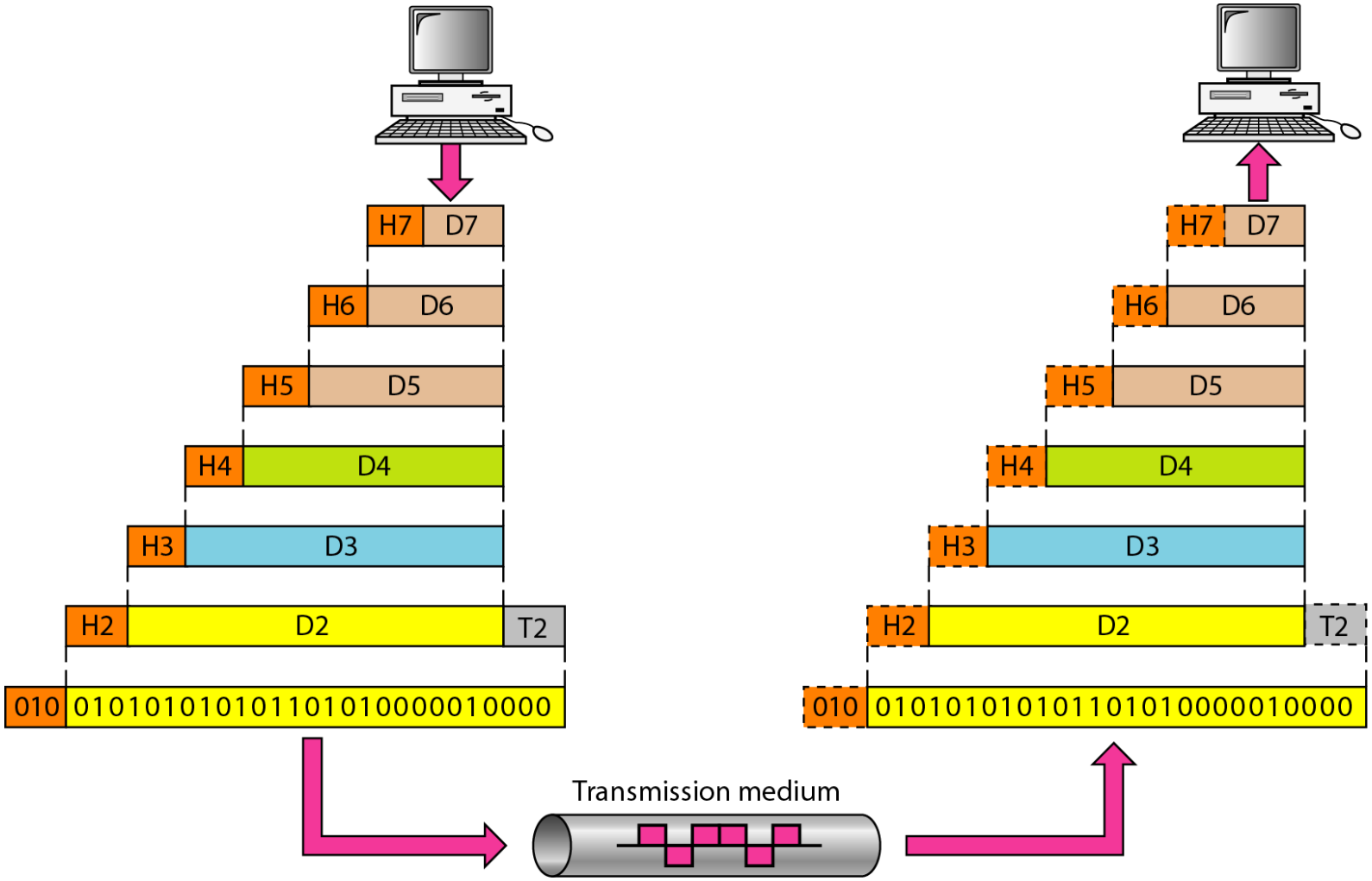
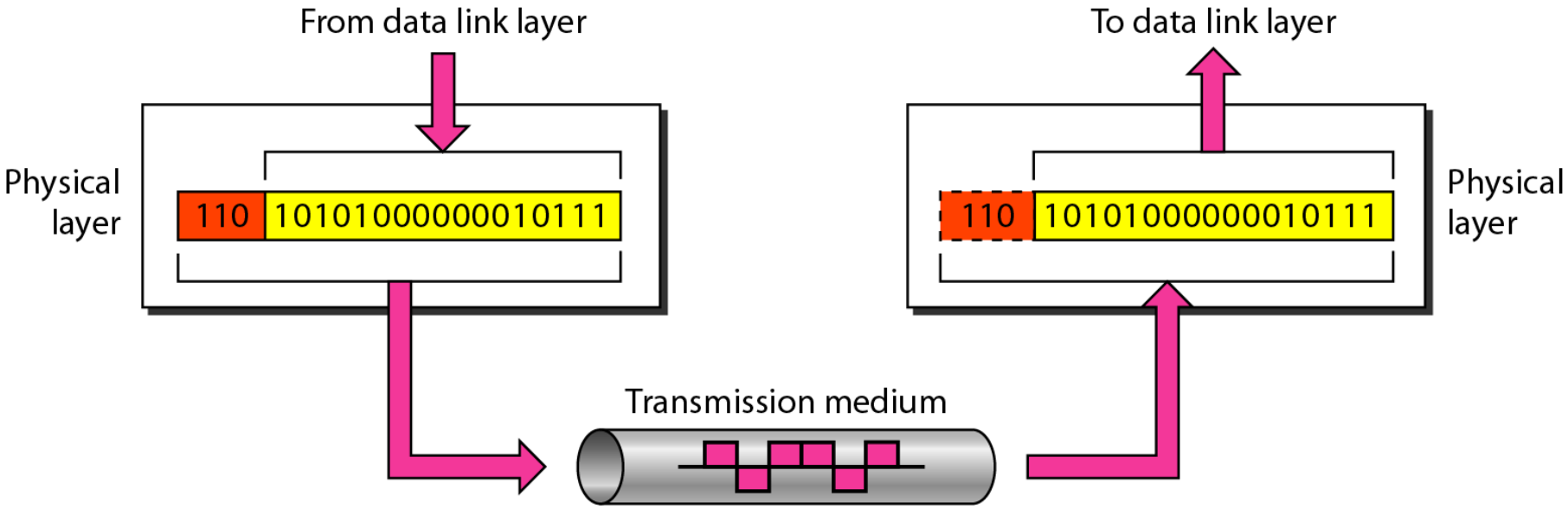


Figure *Physical layer*

The physical layer coordinates the functions required to transmit a bit stream over a physical medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission occur.



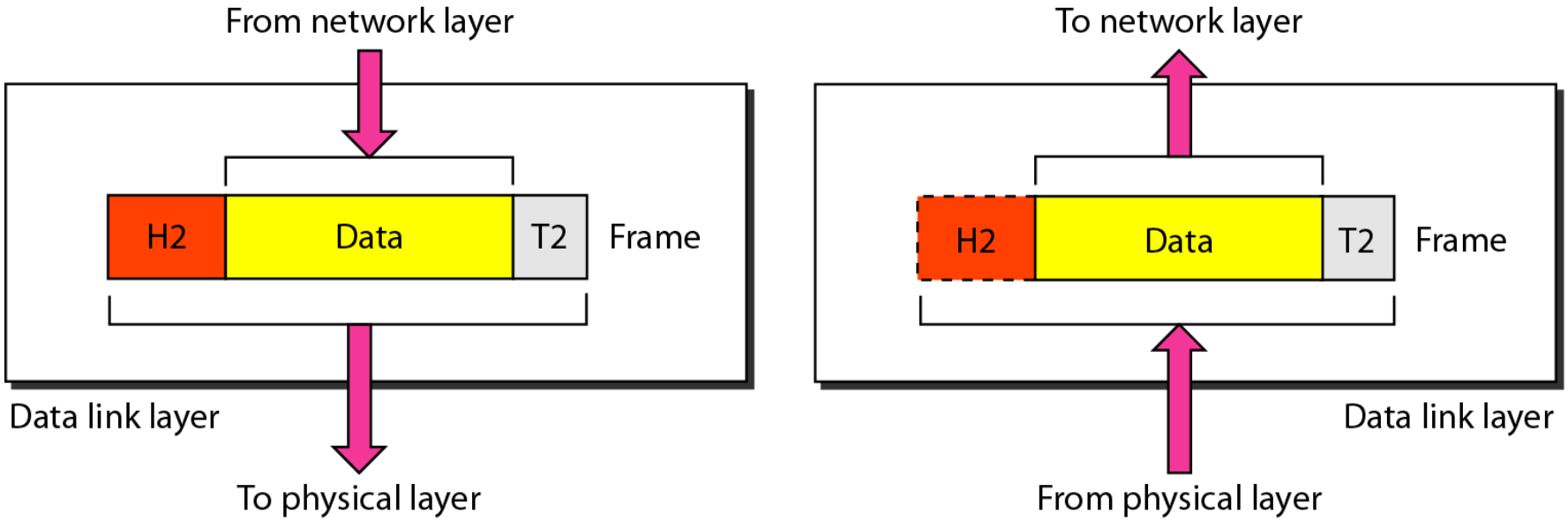
The physical layer is concerned with the following:

- Physical characteristics of interfaces and media: The physical layer defines the characteristics of the interface between devices and the transmission media, including its type.
- Representation of the bits: the physical layer data consist of a stream of bits without any interpretation. To be transmitted, bits must be encoded into signals –electrical or optical-. The physical layer defines the type of **encoding**.
- Data rate: The physical layer defines the transmission rate, the number of bits sent each second.
- Line configuration: the physical layer is concerned with the connection of devices to the medium. Point-to-point, Multi-point
- Physical topology – Mesh, star, ring, bus and hybrid
- Transmission Mode – simplex, half-duplex and full-duplex

Note

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

Figure *Data link layer*



Functions of the data link layer:

- Framing. The data link layer divides the stream of bits received from the network layer into data units called **frames**.
- Physical addressing. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the physical address of the sender (source address) and/or receiver (destination address) of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects one network to the next.
- Flow Control. If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender, the data link layer imposes a flow control mechanism to prevent overwhelming the receiver.

Error control. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. Error control is normally achieved through a trailer to the end of the frame.

Access Control. When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any time.

Note

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

Figure *Hop-to-hop delivery*

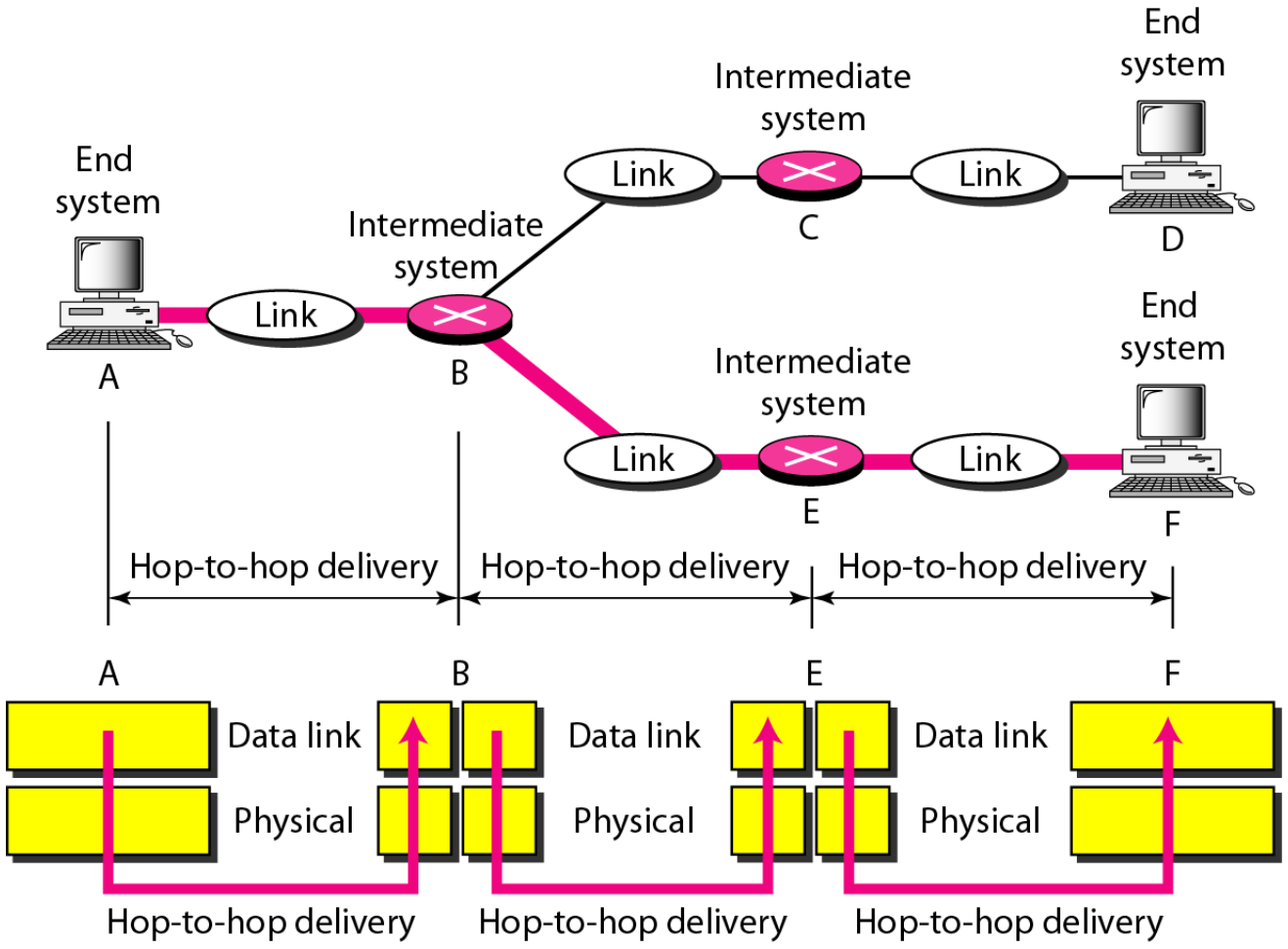
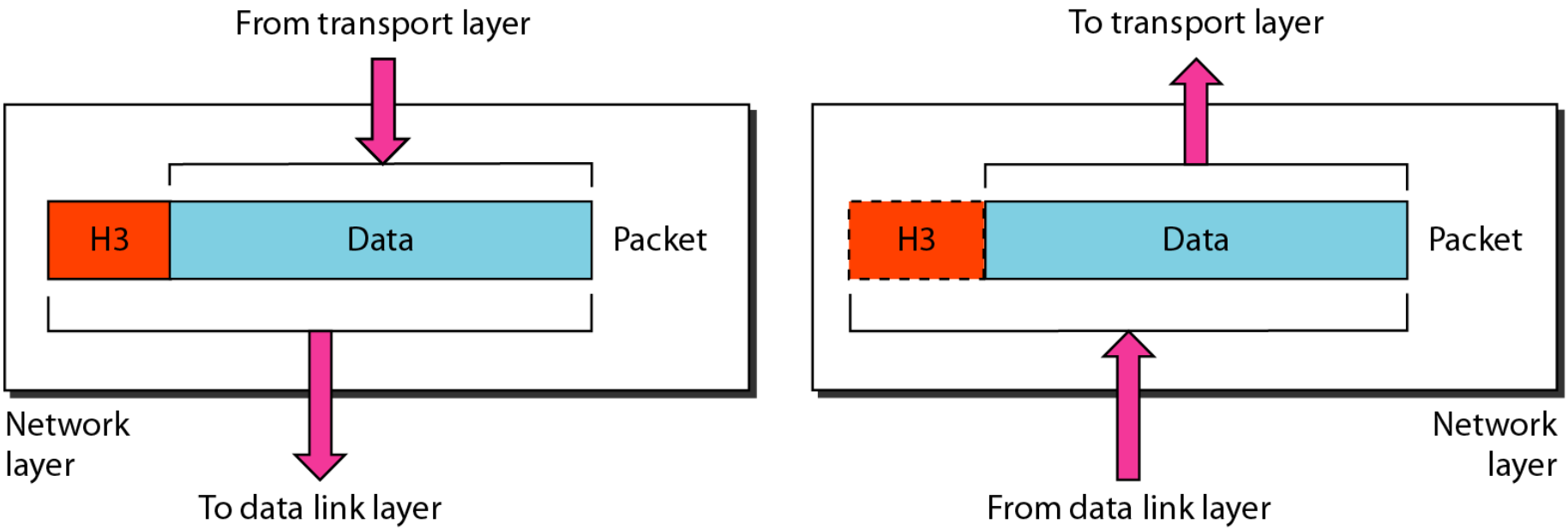


Figure *Network layer*



- Logical addressing. The physical addressing implemented by the data link layer handles the addressing problem locally.

  The network layer adds a header to the packet coming from the upper layer, among other things, includes the logical address of the sender and receiver.

- Routing. When independent networks or links are connected together to create an **internetwork** (a network of networks) or a large network, the connecting devices (called routers or gateways) route or switch the packets to their final destination.

Note

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

Figure *Source-to-destination delivery*

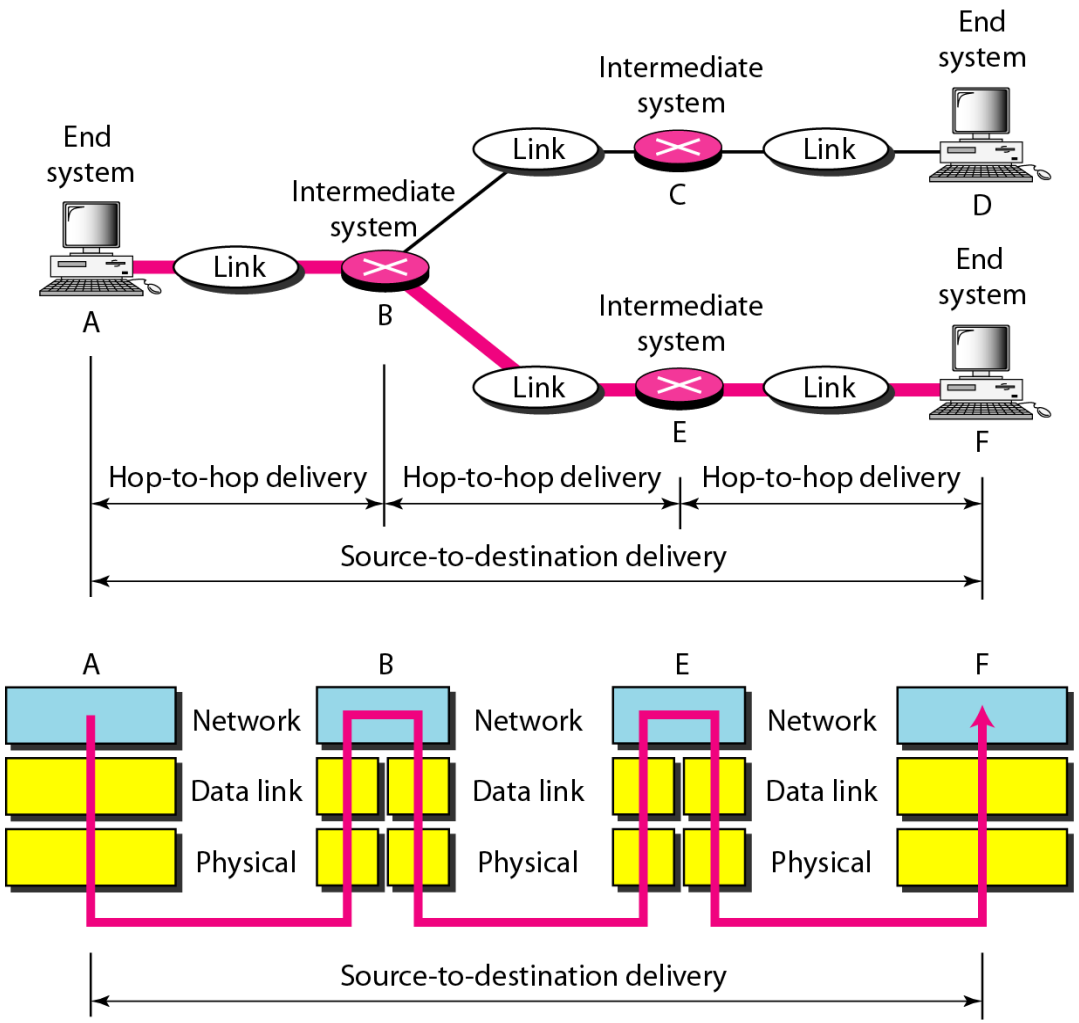
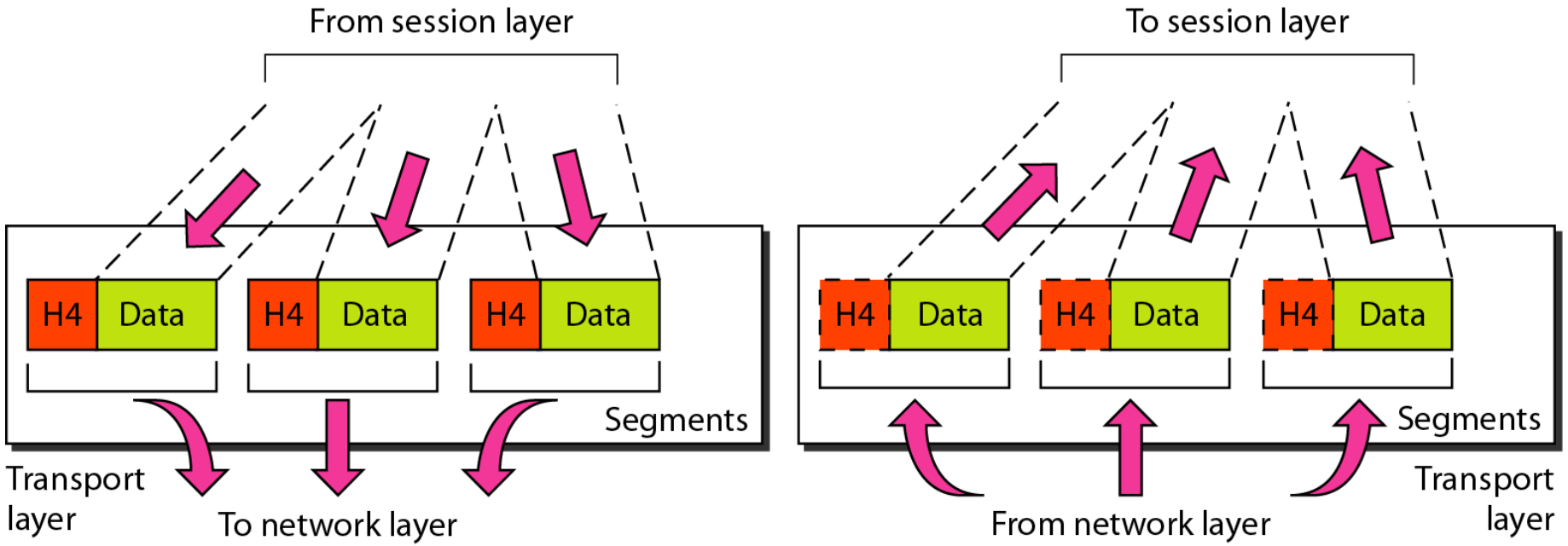


Figure *Transport layer*



- **Service-point address**/port address
- **Segmentation and reassembly**: a message is divided into transmittable segments, each having a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arrival at the destination and to identify and replace packets that were lost in transmission.
- **Connection control**: The transport layer can be either connectionless or connection-oriented.
- A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.
- A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
- **Flow control**: the transport layer performs a flow control end to end. The data link layer performs flow control across a single link.
- **Error control**: the transport layer performs error control end to end. The data link layer performs control across a single link. Error control is achieve using retransmission.

Note

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

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

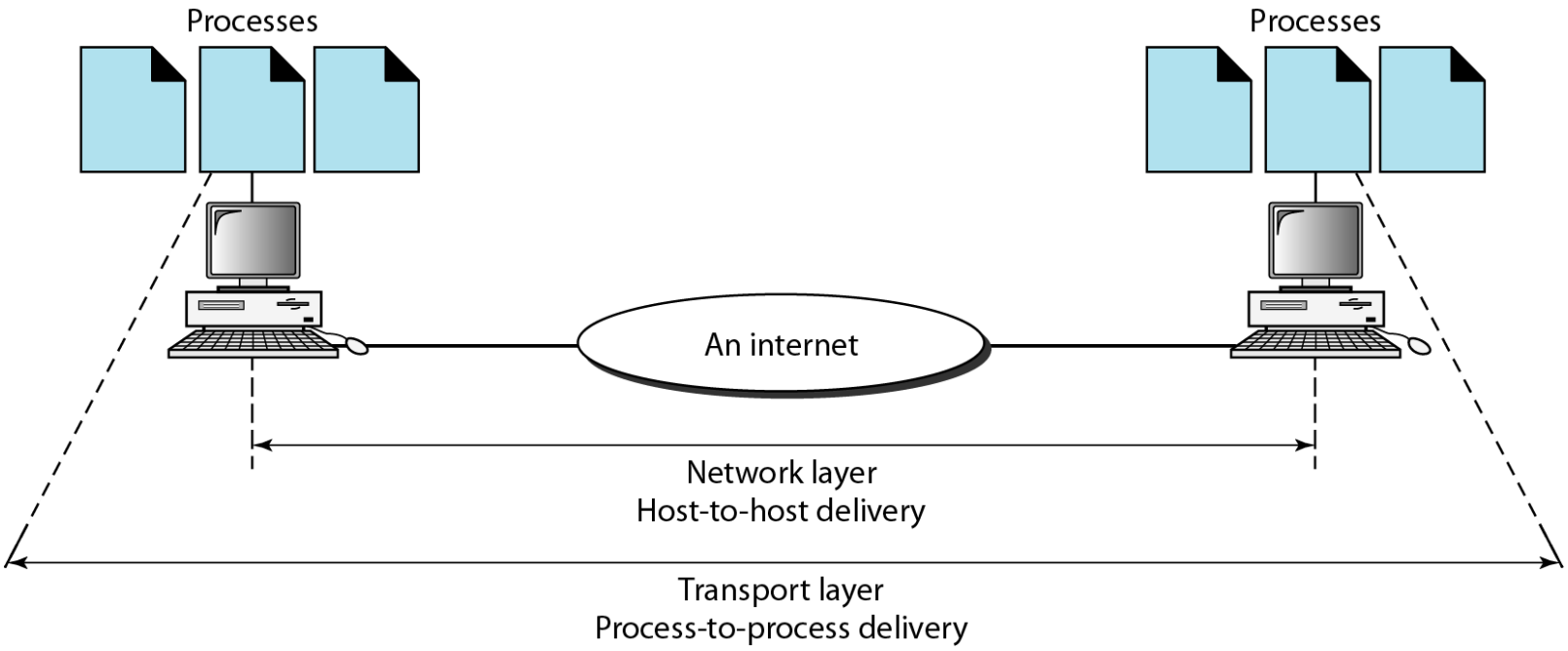
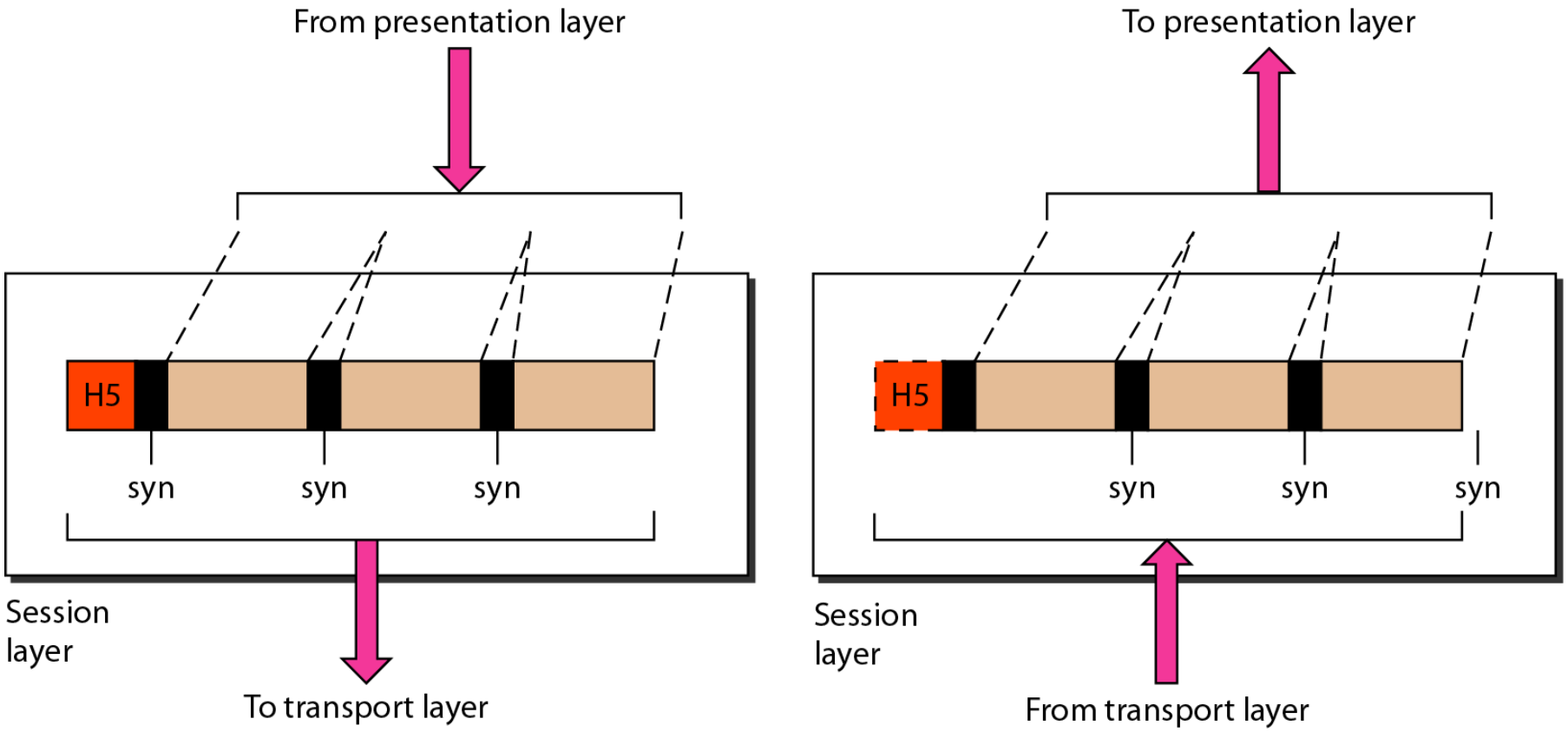


Figure *Session layer*



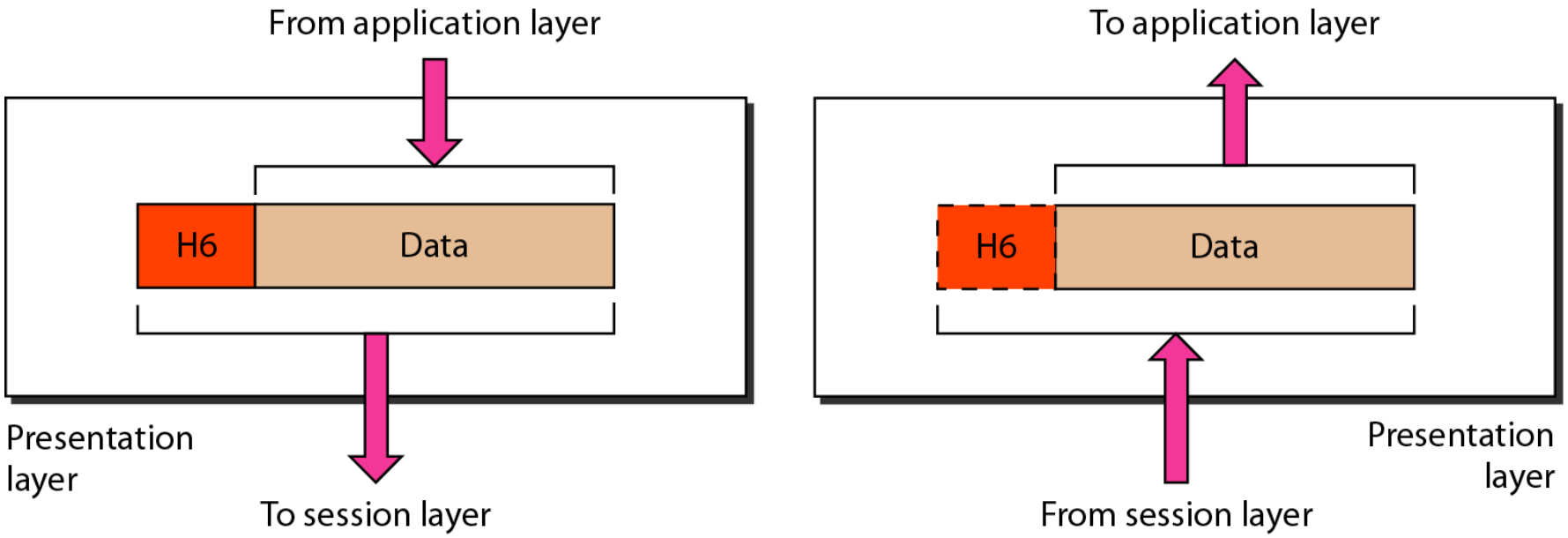
- The service provided by the first three layer is not sufficient for some processes.
- The session layer is the network dialog controller.
- It establishes, maintains, and synchronizes the interaction among communicating systems
- **Dialog control**: communication can be half-duplex or full-duplex
- **Synchronization**: It allows a process to add checkpoints or synchronization points, to stream of data.

Note

The session layer is responsible for dialog control and synchronization.

Figure *Presentation layer*

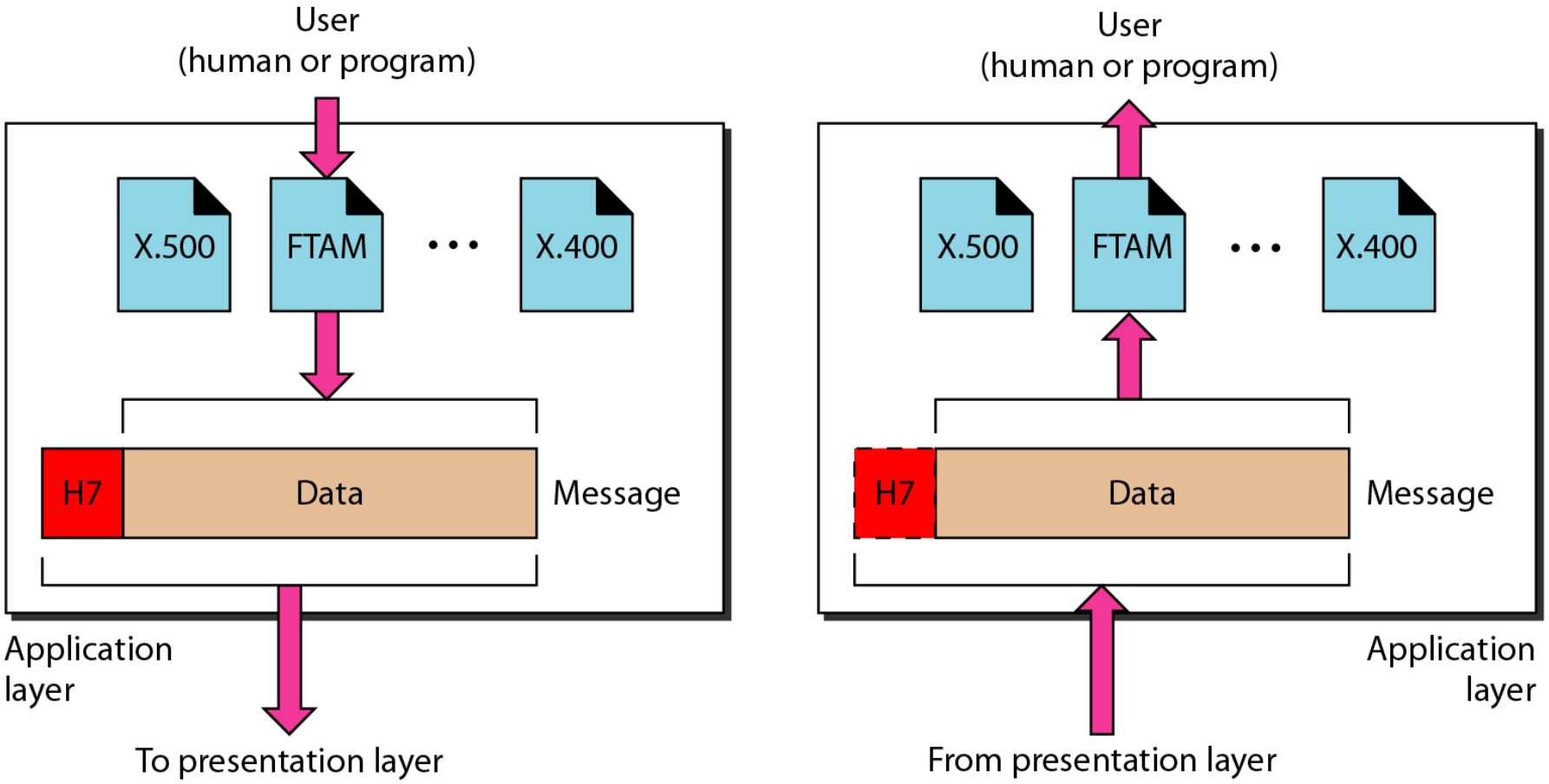
The Presentation layer is concerned with the syntax and semantics of the information exchanged between the two systems.



Note

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

Figure *Application layer*



Network virtual terminal. A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.

File transfer, access, and management. This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

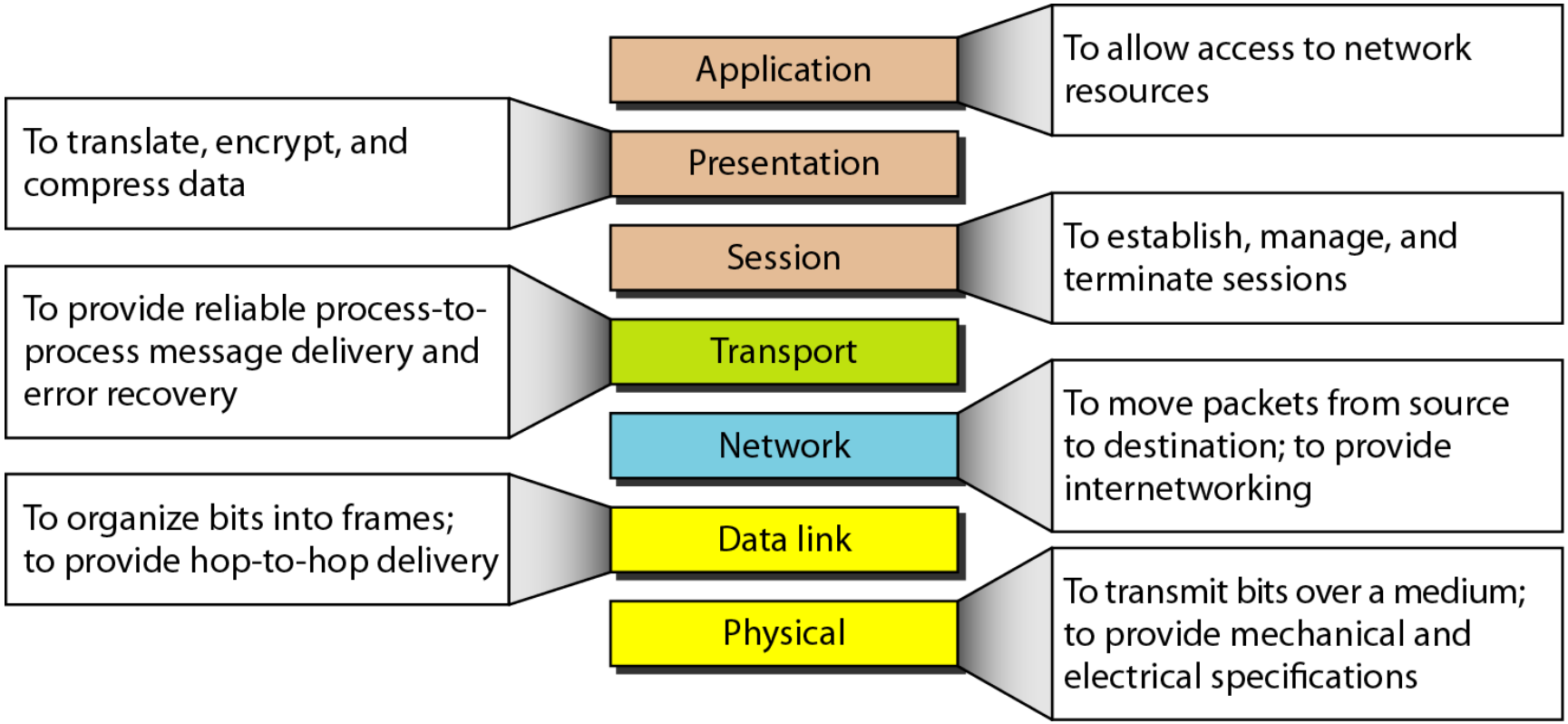
Mail services. This application provides the basis for e-mail forwarding and storage.

Directory services. This application provides distributed database sources and access for global information about various objects and services.

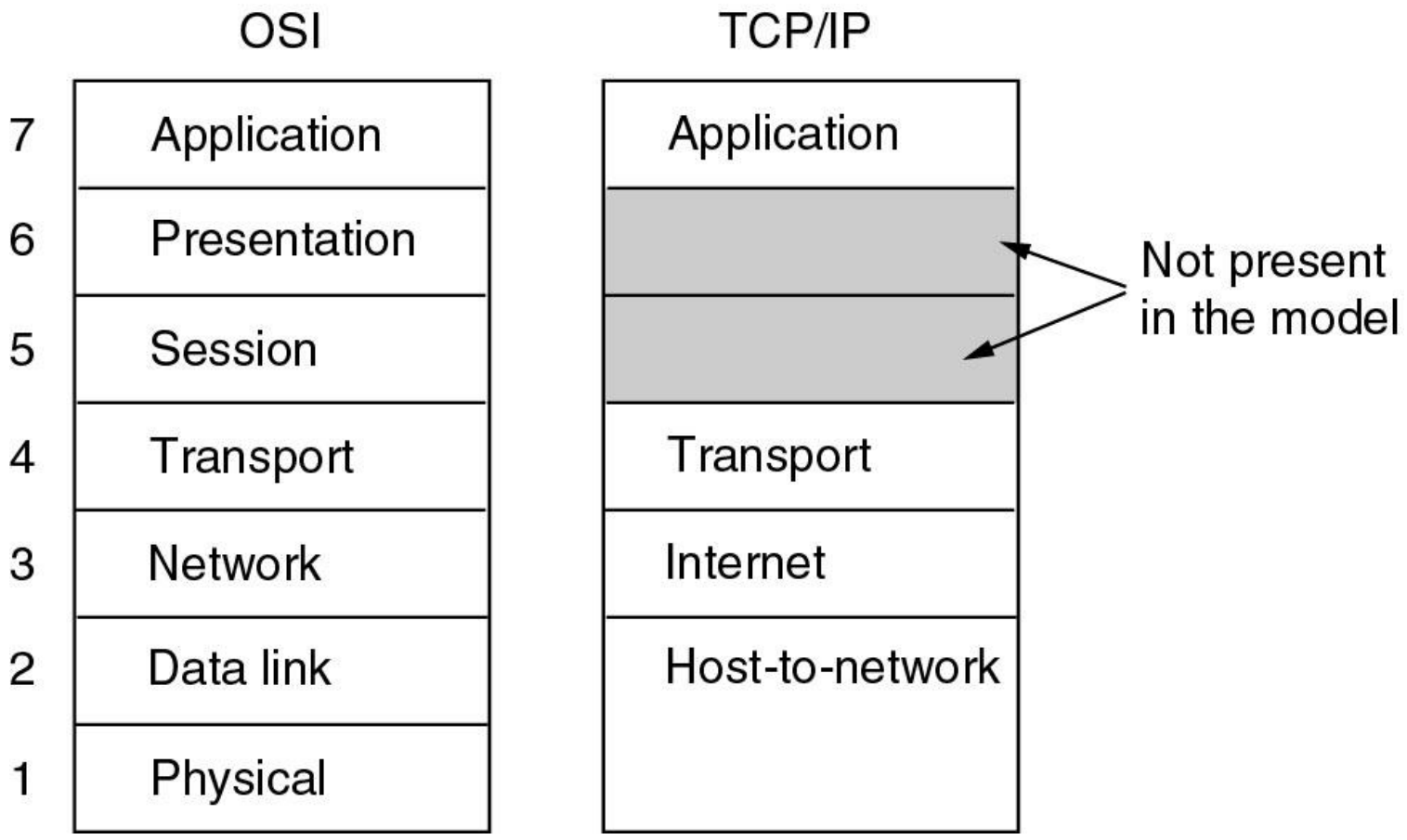
Note

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

Figure *Summary of layers*

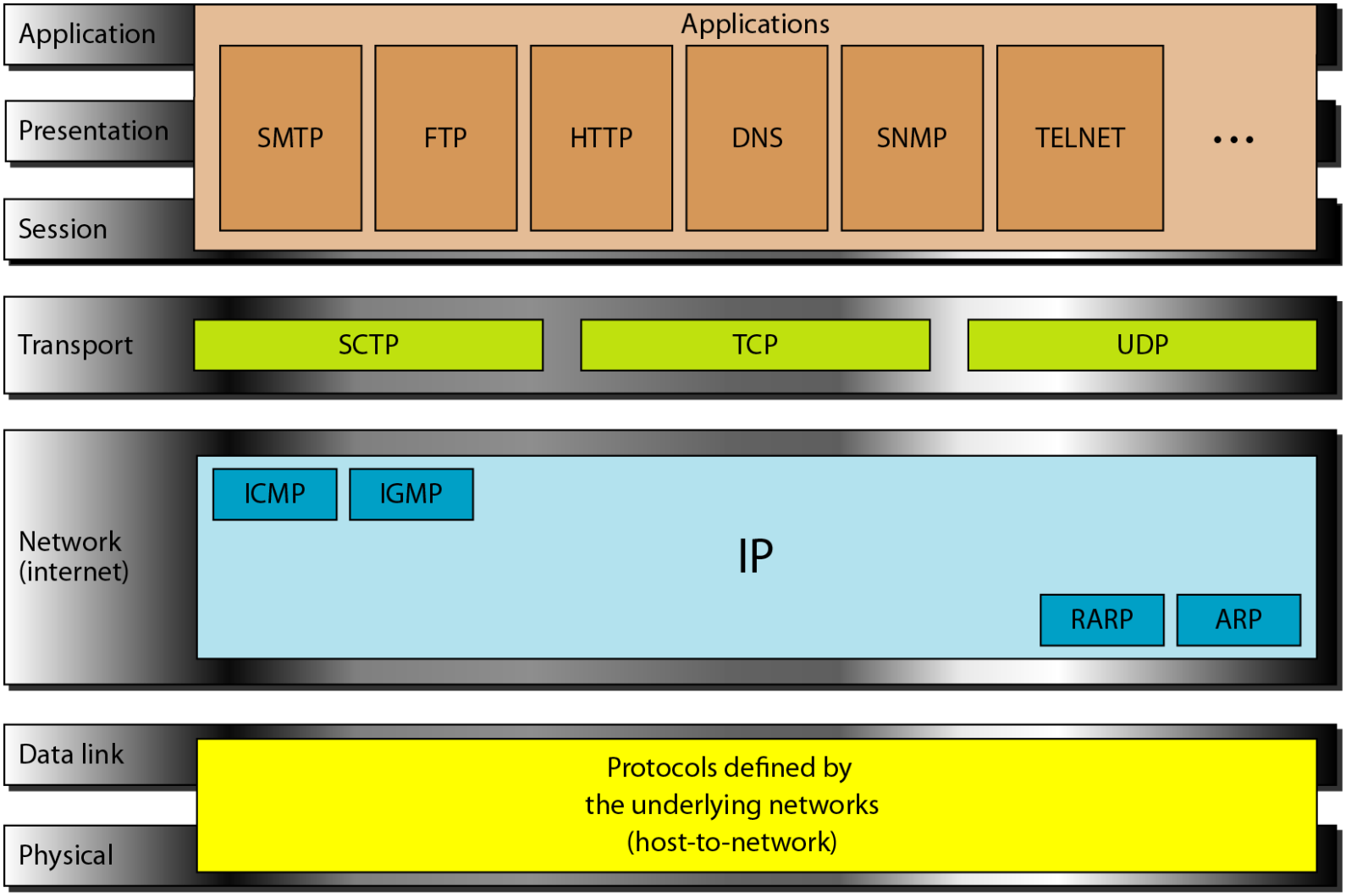


Reference Models (2)



The TCP/IP reference model.

Figure *TCP/IP and OSI model*



Comparing OSI and TCP/IP Models

Concepts central to the OSI model

- Services
- Interfaces
- Protocols

Comparing OSI and TCP/IP Models Continue

- The ***Service*** definitions tells **what the layer does**, not how entities above it access it or how the layer works. It defines the layer's semantics.
- A layer's ***interface*** tells the processes **above it how to access it**. It specifies what the parameters are and what results to expect. It too, says nothing about how the layer works inside.
- Finally, the peer ***protocols*** used in a layer are the layer's own business. It can use any protocols it wants to, as long as it gets the job done.

- The TCP/IP model did not originally clearly distinguish between service, interface and protocol.

- The protocols in the OSI model are better hidden than in the TCP/IP model and can be replaces relatively easily as the technology changes.

- The OSI reference model was **devised before the corresponding protocols were invented** so designer did not have much experience with the subject and did not have good idea of which functionality to put in which layer. **For Ex**. Data link layer originally dealt only with point-to-point networks. When broadcast network came around , a new sub layer had to be hacked in the model.

- With TCP/IP the reverse was true: **Protocols come first, and the model was really just description of the existing protocols.** There was no problem with the protocols fitting the model. They fit perfectly. The only **trouble** was that the model **did not fit** any other **protocol stacks**.

- The OSI Model has seven layers and the TCP/IP has four layers, Both have network, transport and application layers, but the other layers are different.
- The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection-oriented communication in the transport layer.
- The TCP/IP model has one mode in the network layer is connectionless but support both modes in the transport layer, giving the user a choice. This choice is especially important for simple request-response protocols.