Module 1

Introduction to networking

Dr. Prasanna Shete

Dept. of Computer Engineering
K. J. Somaiya College of Engineering

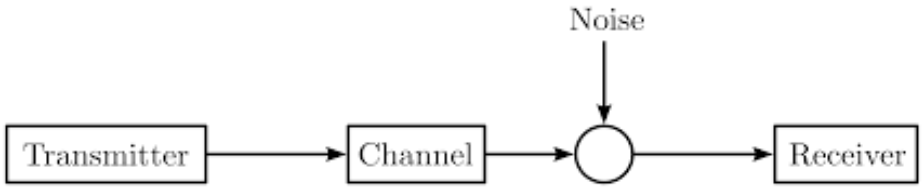
Slide Source: B. A. Forauzan, Data Communications and Networking, McGraw-Hill Online Learning Centre
http://highered.mheducation.com/sites/0072967757/information_center_view0/index.html

Syllabus Contents

1. Data Communication basics
2. Types of Networks: LAN, WAN, MAN; Network Topology (types)
3. Network Software: Protocol hierarchy, Design Issues for layers, Connection oriented and connectionless services, Reliable and Un-reliable services
4. OSI and TCP/IP reference model, Comparison of OSI and TCP/IP reference model
5. Overview of connecting devices- NIC, Repeater, Hub, Switch, Router, Gateway
6. Self learning: Guided and unguided transmission

Communication

- Exchange of ideas/ information
  - Verbal and non-verbal
- Long distance communication historical form- Smoke/fire, Sound (drum beats), Pigeons, Mail etc.
- Electronic Communication- Transfer of information from one place to other through electronic signal
- Types: Wired/ Wireless
- Components of Communication System
  - Sender, Receiver, Message, Channel; (noise)



1-1 DATA COMMUNICATIONS

- Telecommunication means communication at a distance
- Data refers to information presented in whatever form
- ***Data communication refers to exchange of data between two devices via some form of transmission medium such as a wire cable or radio signal***

Topics discussed in this section:

Components
Data Representation
Data Flow

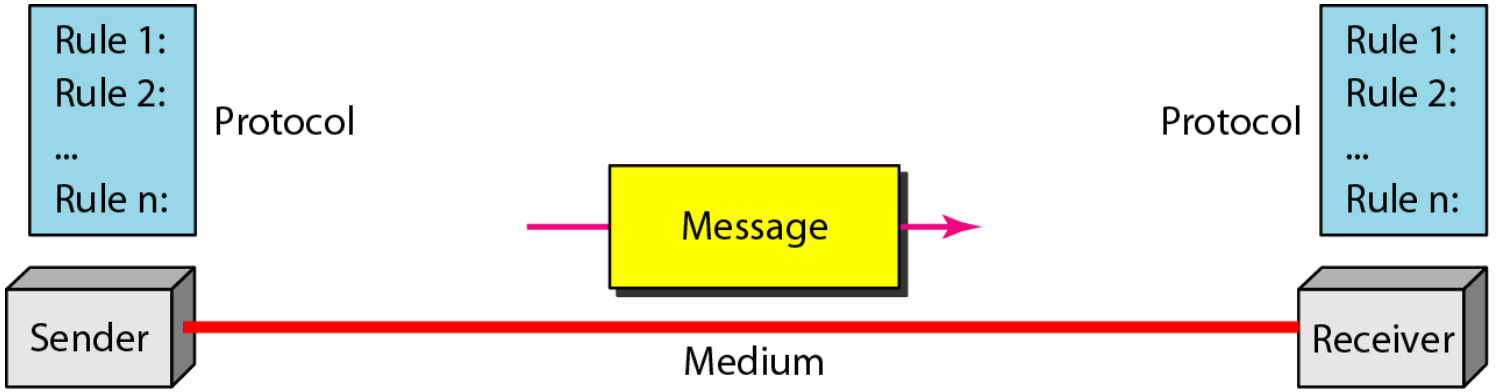
1.4 Source: http://highered.mheducation.com/sites/0072967757/information_center_view0/index.html

Data Representation

- Different forms of Information/Data
  - Text- Unicode (32 bits), ASCII
  - Numbers- numbering systems
  - Images- pixels; gray scale, colour (RGB etc)
  - Audio- sound / music; continuous not discrete
  - Video- continuous or discrete entity

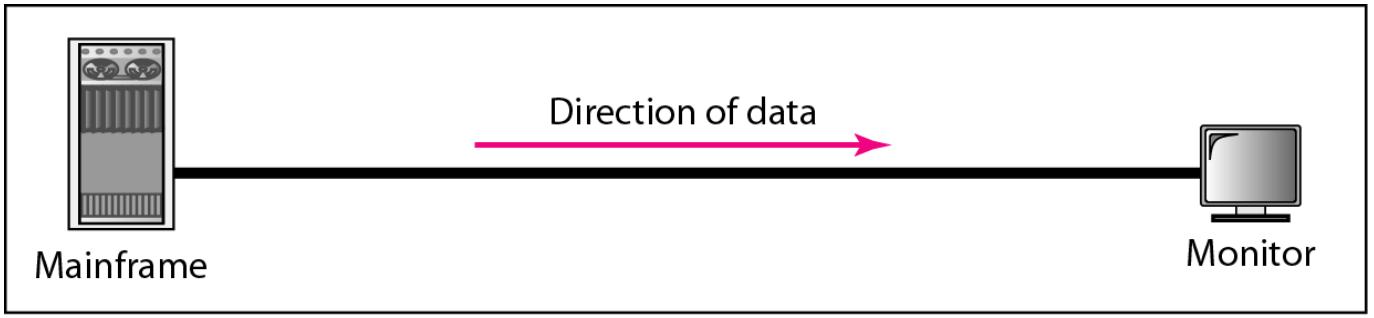
Figure 1.1 *Five components of data communication*

- → Sender, Receiver, Medium, Message and Protocol

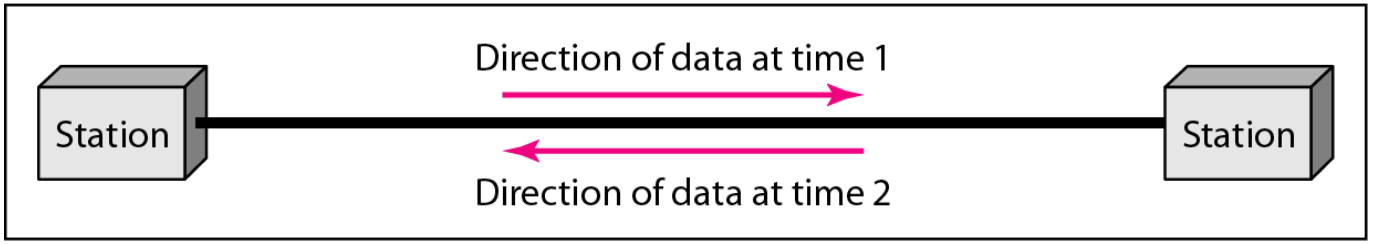


- →Protocol is a set of rules that govern data communication
  - agreement between the communicating devices
  - without a protocol, two devices may be connected but not communicating

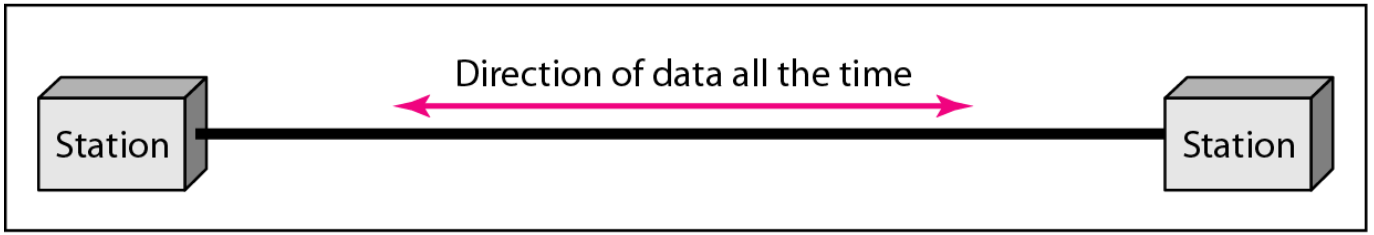
Data flow: Simplex (one way), half-duplex (two way communication but not simultaneously) and full duplex (2 way)



a. Simplex



b. Half-duplex



c. Full-duplex

1-2 NETWORKS

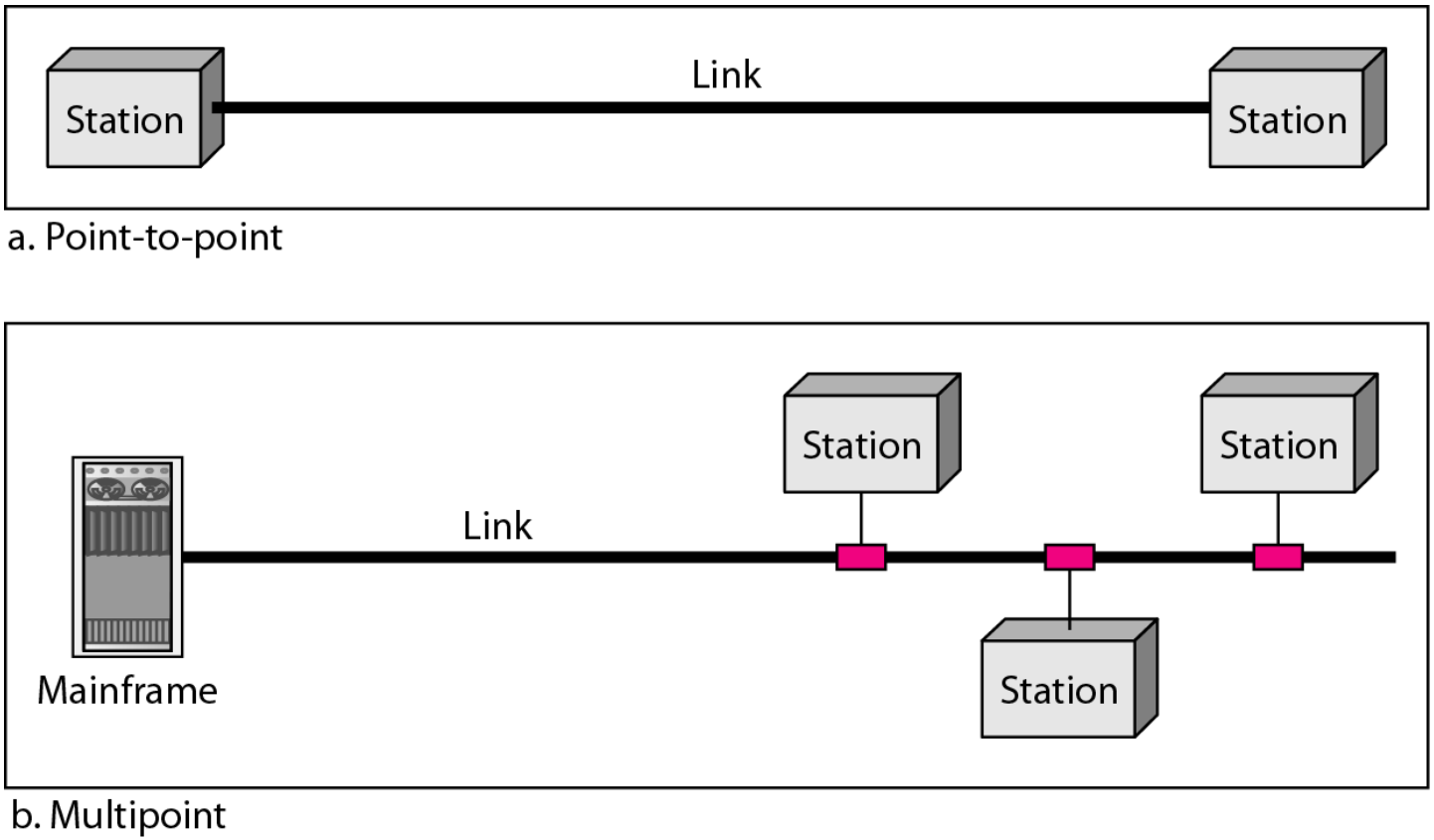
A network is a set of devices (often referred to as nodes) connected by communication links.

- ***A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network***

Topics discussed in this section:

Physical Structures
Network Models
Categories of Networks
Interconnection of Networks: Internetwork

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



Types of connection/link (***Point-to-point and multipoint***)

- Point-to-point- dedicated link between two devices
  - Capacity reserved only for these devices
  - Dedicated wire cable or microwave links, IR etc.

- Multipoint- More than two devices share a single link
  - Capacity of the channel is shared spatially or temporally

Physical Topology:

-Refers to the way in which a network is laid physically;
Geometric representation of the relationship of all the links and devices (nodes) to one another

Figure 1.4 ***Categories of topology***

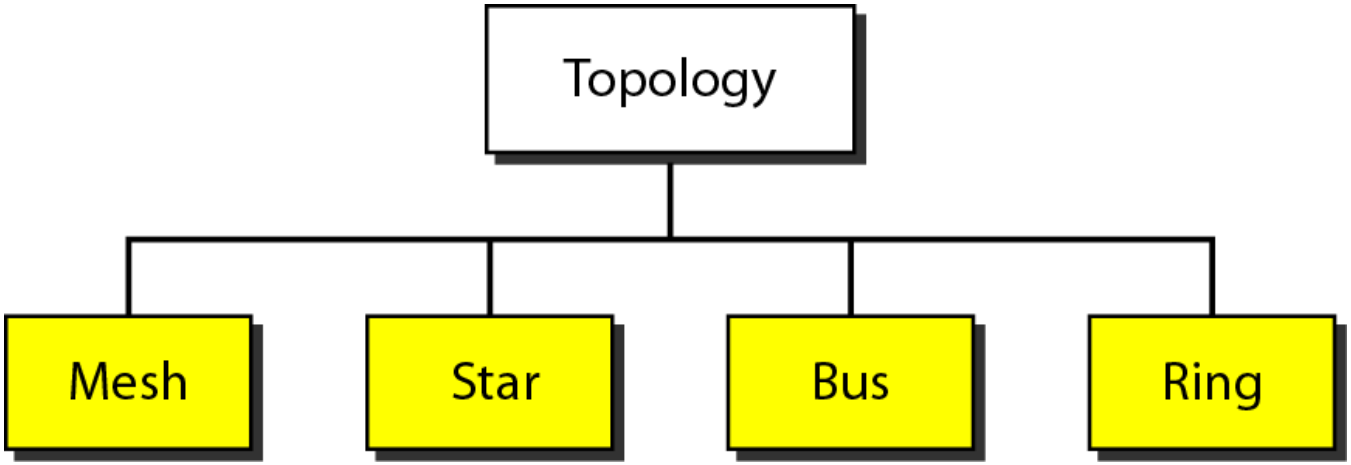
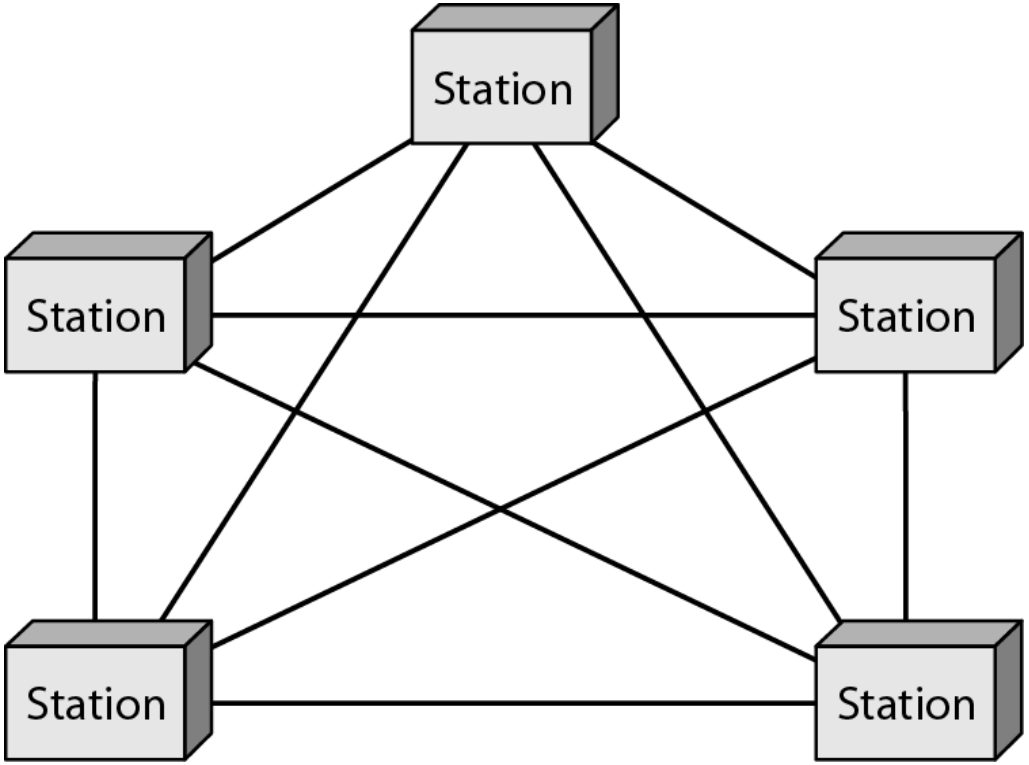


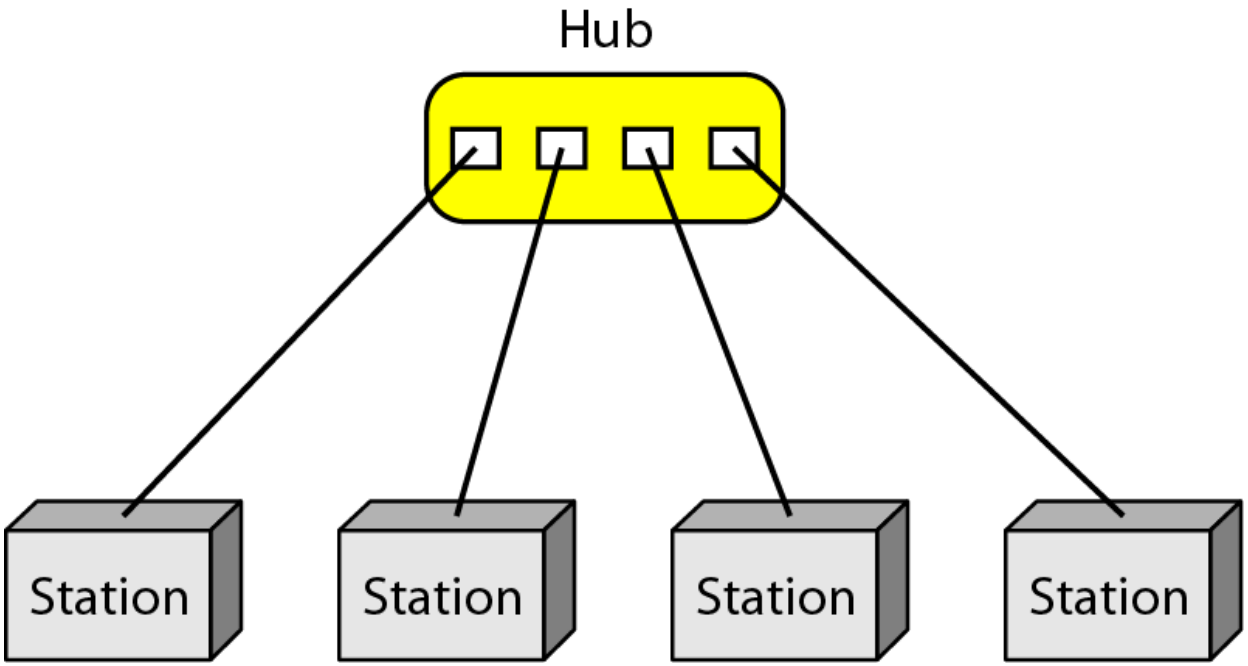
Figure 1.5 *A fully connected mesh topology (five devices)*



MESH Topology

- Every device has dedicated point-to-point link to every other device
- For network consisting of '*n*' nodes, *n(n-1)* links are required
  - *(n-1)* I/O ports required
  - Robust; easy fault identification and isolation
  - Privacy & Security
  - Large amount of cabling reqd→ large space, expensive
  - Ex. Backbone networks; connecting Telephone regional offices

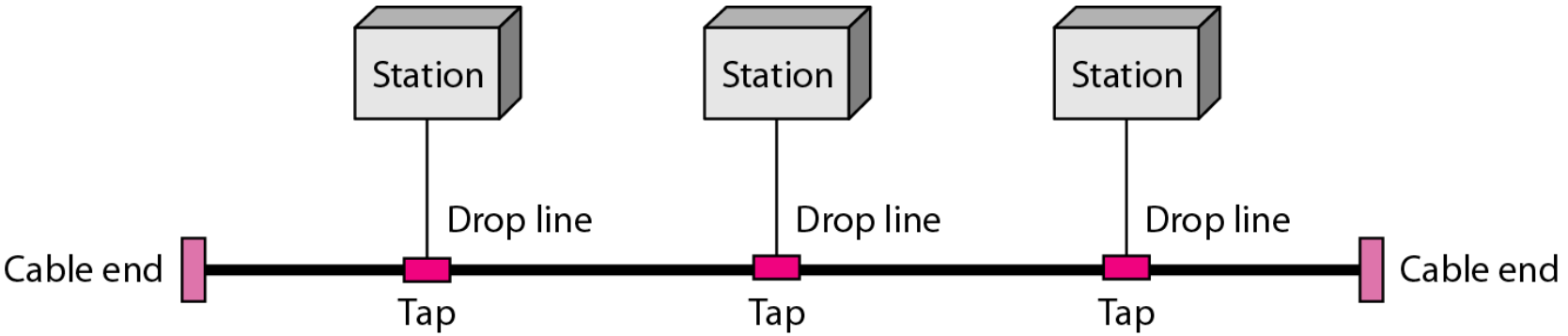
Figure 1.6 *A star topology connecting four stations*



STAR Topology

- Each device has a dedicated point-to-point link only to a central controller → Hub
  - Does not allow direct communication between devices
  - Less expensive than Mesh
  - If one link fails only that node is affected; others can communicate
  - Less cabling reqd; in-expensive
  - Not as Robust as Mesh; Hub is single point of failure
  - Ex. LAN

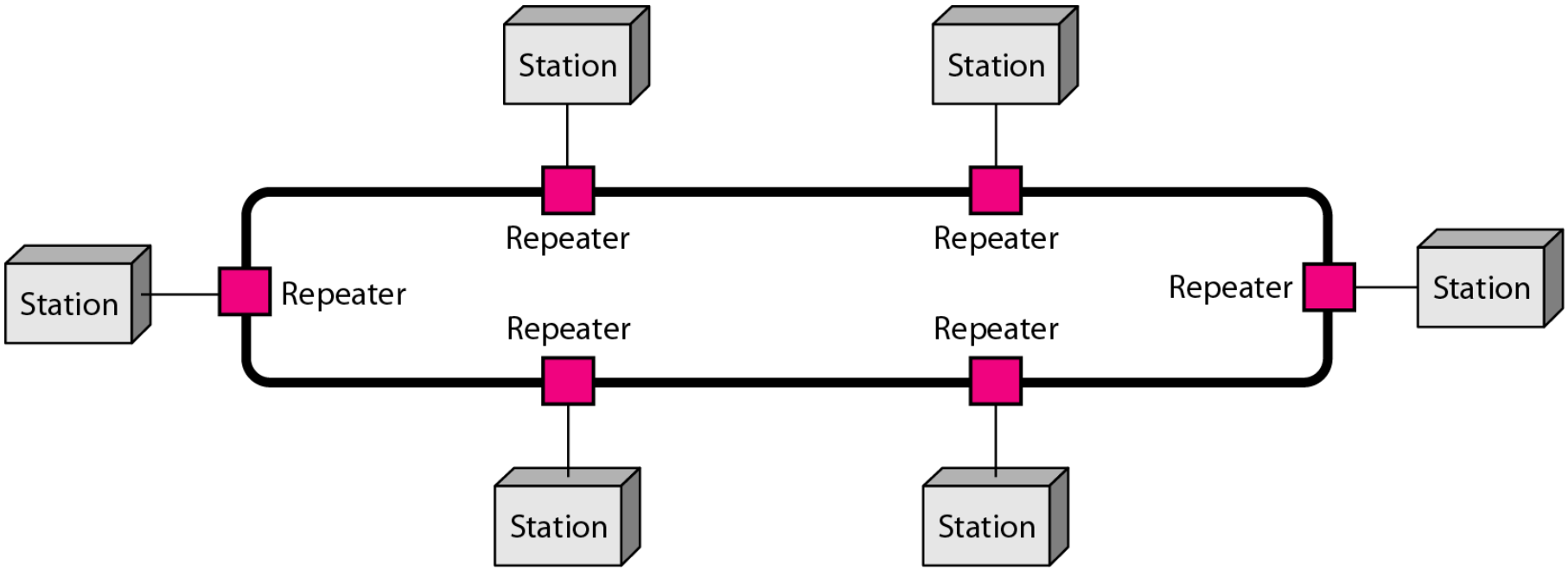
Figure 1.7 *A bus topology connecting three stations*



BUS Topology

- Multipoint topology
- one long cable acts as a **backbone** to which all devices are connected with the help of drop lines and taps
  - Least cabling hence inexpensive than other topologies
  - Signal becomes weaker as it travels farther
  - Difficult fault isolation and reconnection; break in cable stops communication
  - Ex. Early Ethernet LANs, now obsolete

Figure 1.8 *A ring topology connecting six stations*



Ring Topology

- Each device has a dedicated point-to-point connection to only two devices on either side of it
- Each device incorporates a repeater
- Signal passed along the ring in one direction
  - Easy to install and reconfigure; Less expensive than Mesh
  - Easy fault isolation
  - In simple ring (simplex links), break in ring/disabled station can disable entire network
    - Solved using dual ring with switching capability
  - Ex. Token Ring LAN

Figure *A dual-ring topology connecting six stations*

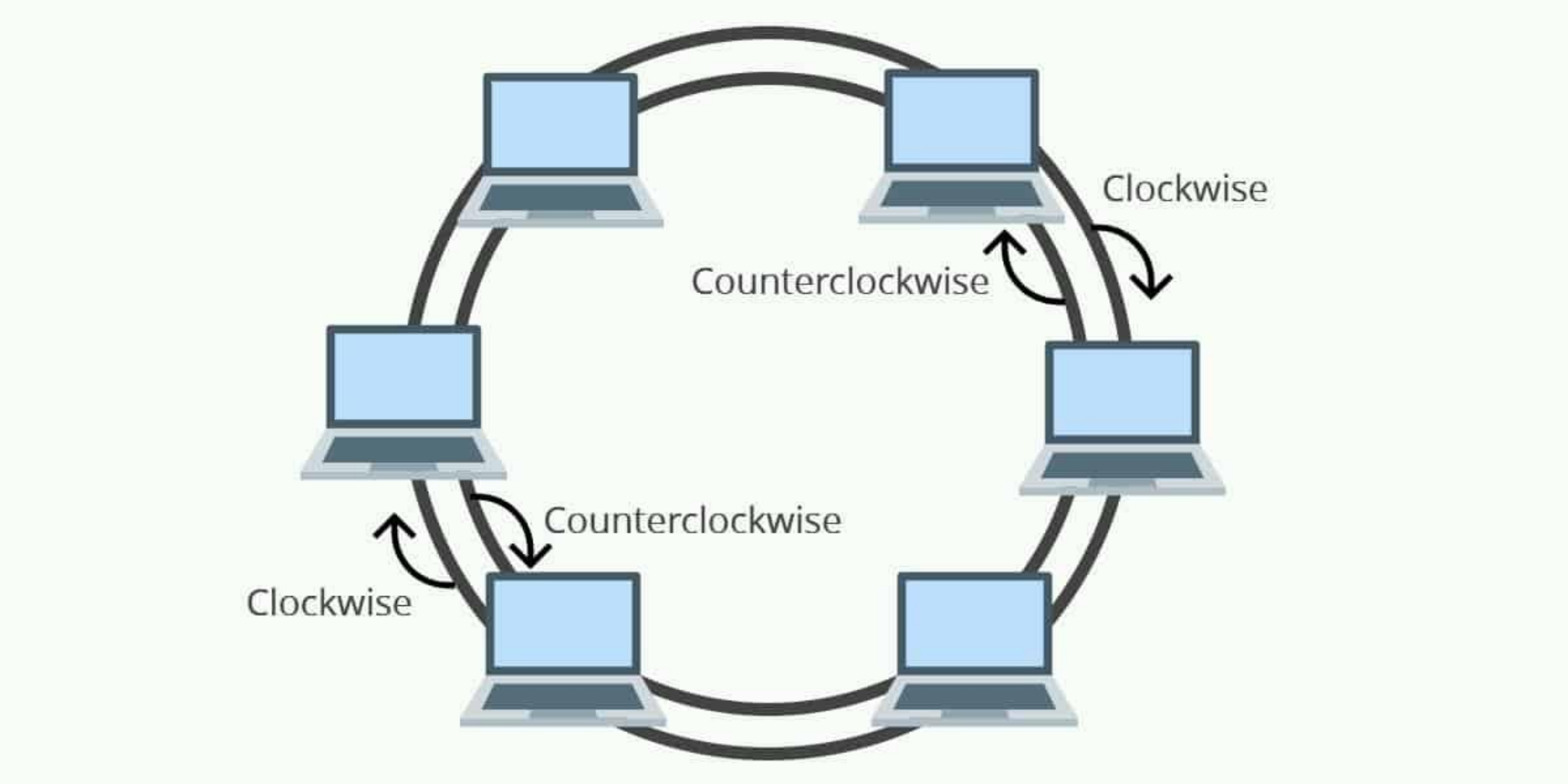
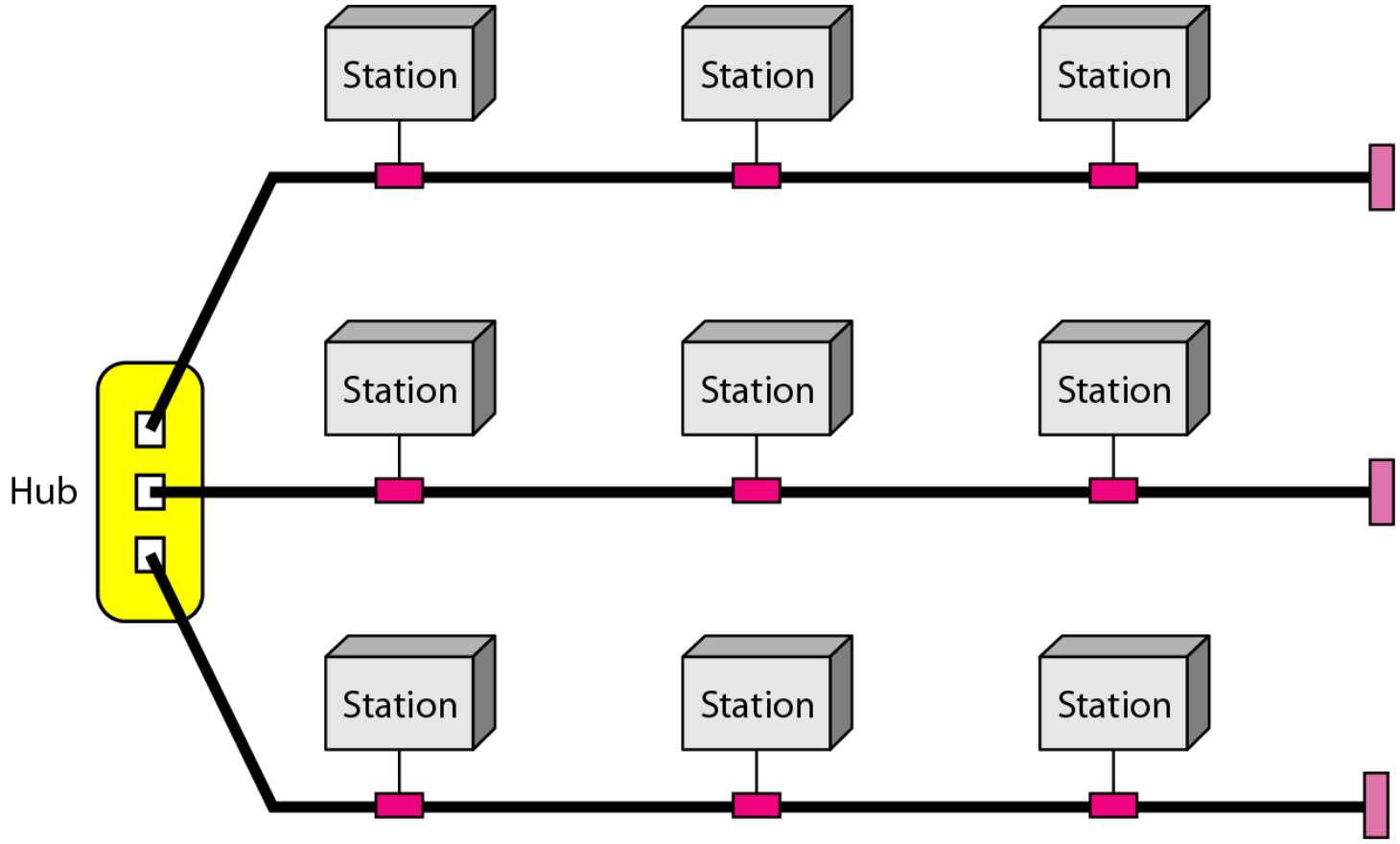


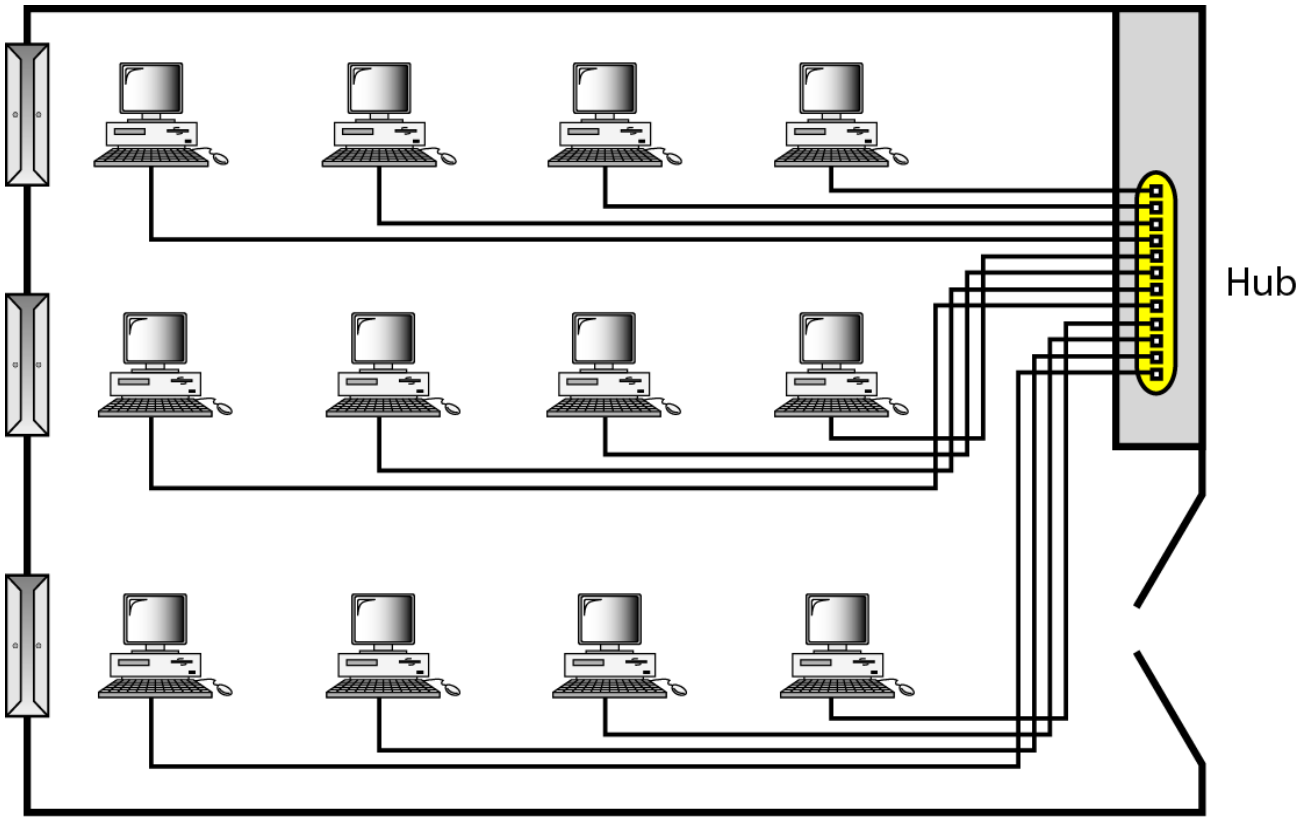
Figure 1.9 *A hybrid topology: a star backbone with three bus networks*



Types of Networks: LAN, MAN, WAN

- LAN- Local Area Network
  - Privately owned; allows resources to be shared among computers
  - Linking the devices in a single office, building or campus;
  - High capacity device acts as a Server; clients use the resources (storage, files, software etc.) available on server
  - Topologies: Star, Bus and Ring
  - LAN size/Area Restricted to few kms
  - Data Rate: 10 to 1000Mbps

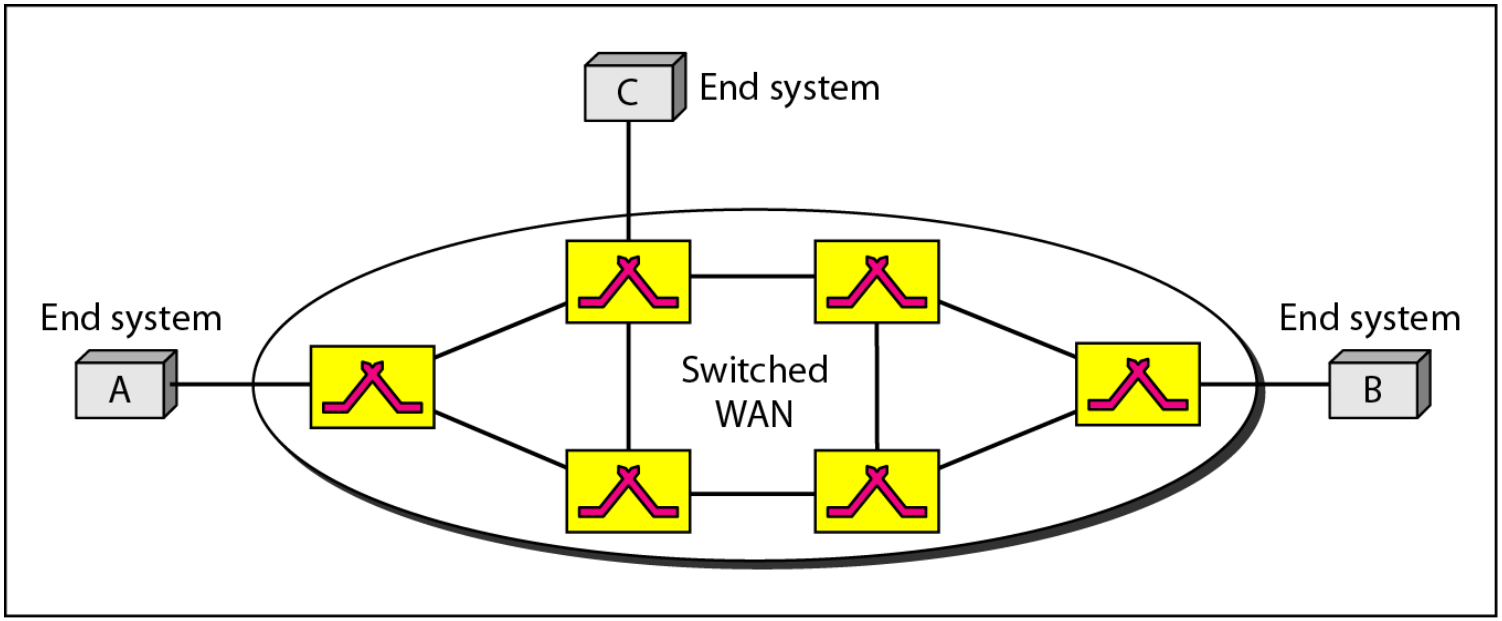
Figure 1.10 *An isolated LAN connecting 12 computers to a hub in a closet*



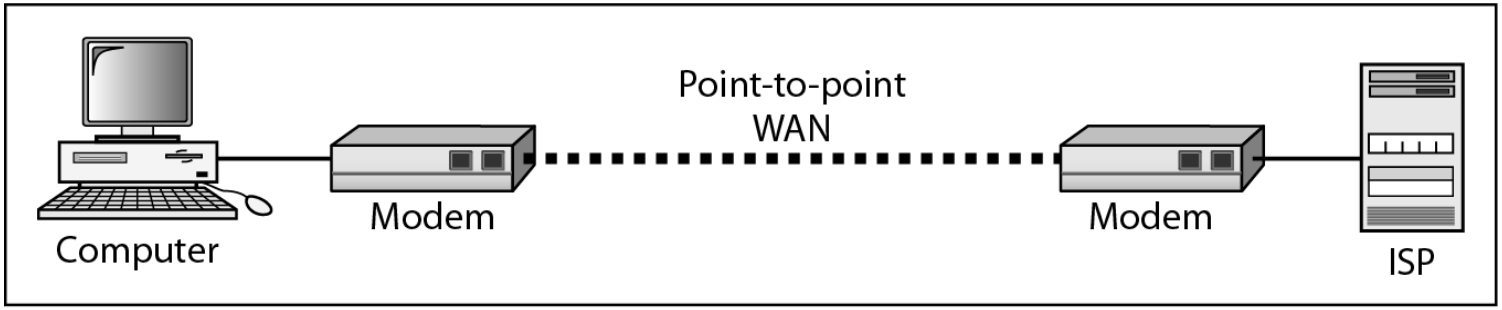
Types of Networks: LAN, MAN, WAN

- WAN- Wide Area Network
  - Provides long distance transmission of data
  - spans large geographical area that may comprise a country, a continent or entire globe
  - Types- Switched, Point-to-Point
  - Switched WAN- connects the end systems, which comprise a *Router* that connects to another LAN or WAN
    - X.25, Frame relay, ATM, wireless WAN
  - Point-to-Point WAN- Home computer/LAN connected to Internet Service Provider (ISP) via Dialup/Leased line or cable TV network

Figure 1.11 *WANs: a switched WAN and a point-to-point WAN*



a. Switched WAN



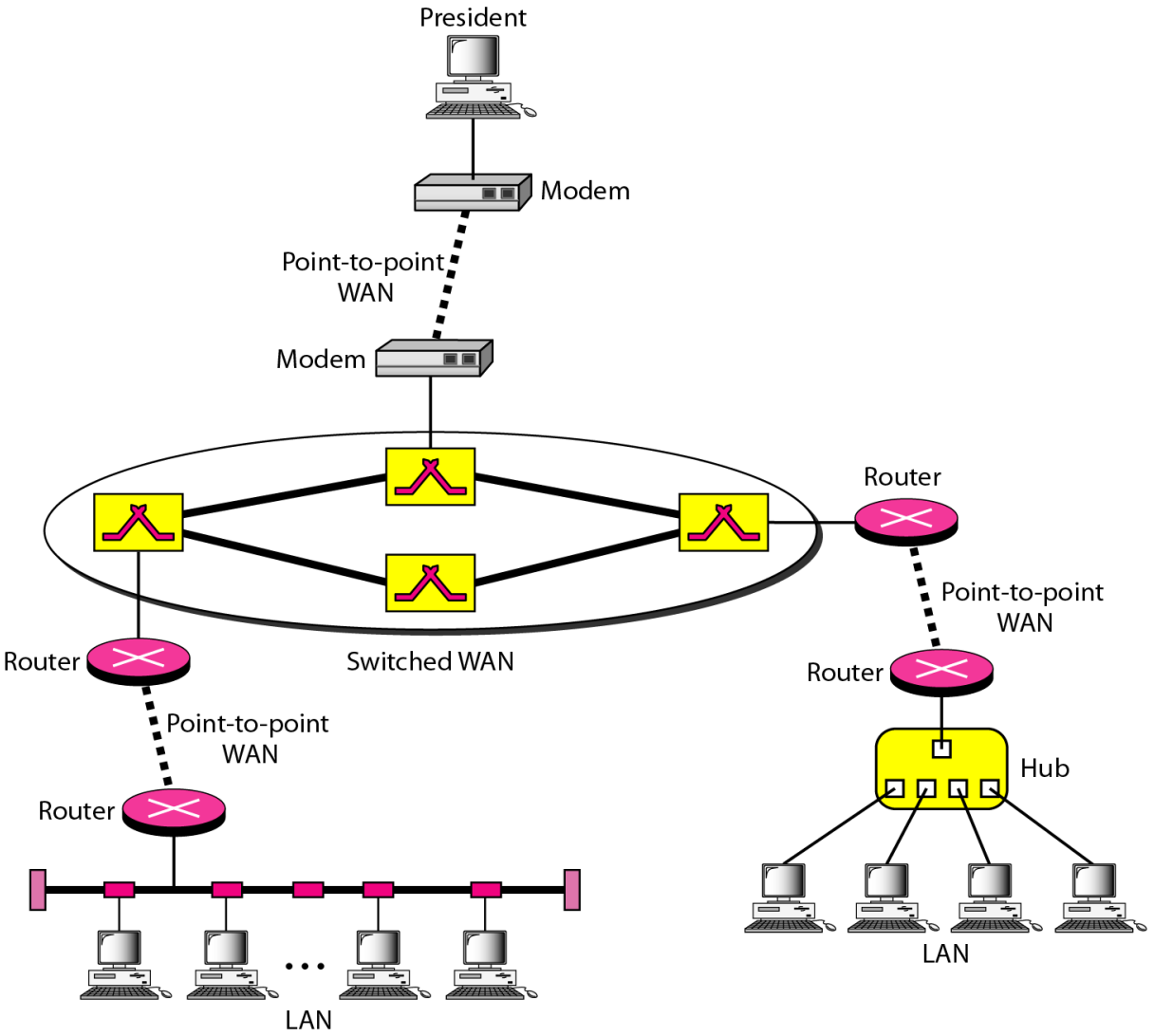
b. Point-to-point WAN

Types of Networks: LAN, MAN, WAN

- MAN- Metropolitan Area Network
  - Fits between LAN and WAN; covers region/area within a city restricted to few tens of kms
  - Designed for customers who need high speed connectivity; offices spanning over the city
  - E.g. Telephone company network that provides high-speed DSL line to customers

Internetwork: interconnection of networks

Figure 1.12 A heterogeneous network made of four WANs and two LANs



1-3 THE INTERNET

- An *internet* comprises of two or more networks that can communicate with each other
- *Internet* is a collaboration of more than hundreds of thousands of interconnected networks

- *Internet has revolutionized many aspects of our lives*
- *Changed the way we do business as well as the way we spend our leisure time*
- *It is a communication system that has brought a wealth of information to our fingertips and organized it for our use*

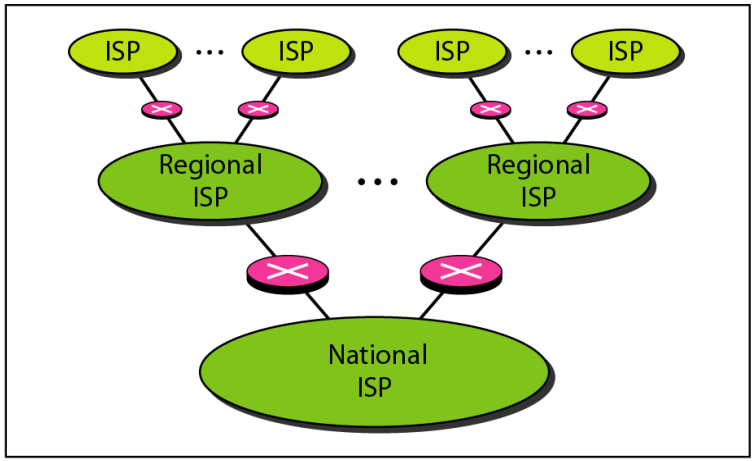
History

- First network/internet- ***ARPANET***- 1969
  - Advanced Research Projects Agency (ARPA), Dept. of Defense
  - Small network of connected computers; each host computer attached through specialized computer called IMP (interface message processor)
  - 4 nodes at the University of California at Los Angels (UCLA), University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI) and University of Utah connected via IMP
  - Network Control Protocol (NCP) provided communication between the hosts
  - 1973- V. Cerf and B. Kahn-TCP (Transmission Control Protocol); later split into TCP and IP

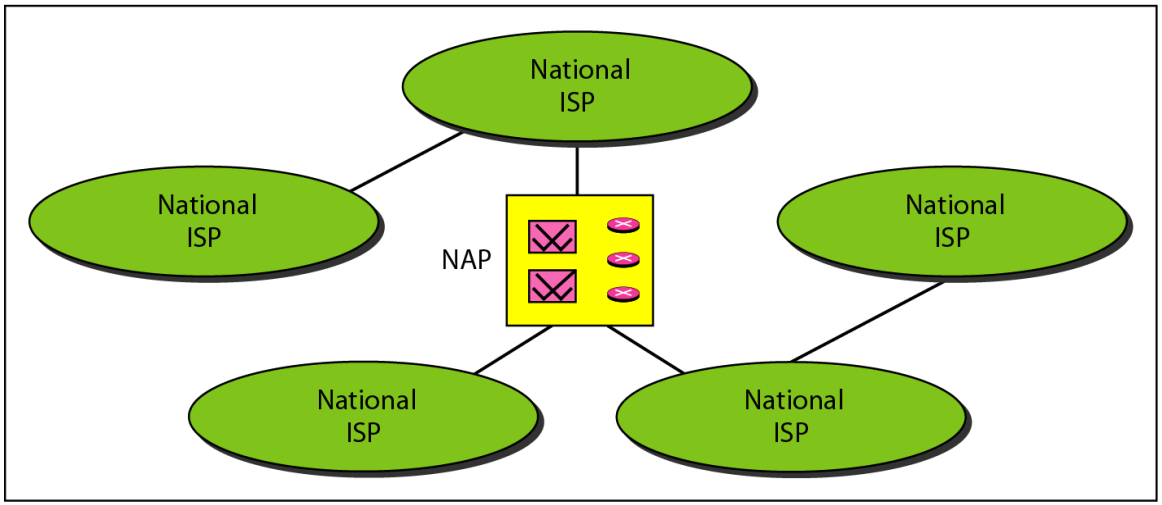
Internet Service Providers (ISPs)

- For connecting to Internet, end users use the service of Internet Service Providers (ISPs)
  - Types: International service providers, national service providers, regional service providers and local service providers
- Local ISPs- provide direct service to end users and are connected to regional ISPs or national ISPs
  - Can be a company providing Internet services, corporation or a non profit organization e.g college/University, civic body…
- Regional ISPs are connected to one or more national ISPs
- National ISPs- backbone networks created and maintained by specialized companies
  - interconnected by switching stations called Network Access Points
- International ISPs- connect National ISPs together

Figure 1.13 *Hierarchical organization of the Internet*



a. Structure of a national ISP



b. Interconnection of national ISPs

1-4 PROTOCOLS AND STANDARDS

Jargon terms: ***Protocols and Standards***

- ***Protocol*** ***is synonymous with rule***
- ***Standards*** ***are agreed-upon rules***

Topics discussed in this section:

Protocols
Standards
Standards Organizations
Internet Standards
Connection oriented and connectionless services

Protocols

- Set of rules that govern data communication
  - Defines what is communicated, how it is communicated and when it is communicated
- Key elements- Syntax, Semantics and Timing
- Syntax- structure or format of data; order in which data is presented
  - E.g. first 48 bits sender address, next 48 bits receiver address and remaining bits the message/user data
- Semantics- meaning of each section of bits
  - How a bit pattern is to be interpreted and what action be taken
- Timing- refers to what data to be sent and how fast be sent
  - Useful for matching the sending rate of sender with the capability of receiver

Standards

- Provide guidelines to manufacturers, vendors, government agencies, and other service providers
- Essential for guaranteeing national and international interoperability (of technology and processes)
- Developed through cooperation of standards creation committees, forums and regulatory agencies
- Two categories: De facto and De jure
  - De facto (by fact)- standards not been approved by a standardisation body but have been adopted through widespread use
  - De jure (by regulation)- standards that have been legislated by an officially recognized body (e.g. IEEE)

Standards Organizations

- ISO: International Organization for Standardization
- ITU-T: International Telecommunication Union-Telecommunication Standards Sector
- ANSI: American National Standards Institute
- IEEE: Institute of Electrical and Electronics Engineers
- EIA: Electronic Industries Association

- Special Interest Groups/ Forums- representatives from various corporations
  - work with universities and users, test and evaluate new technologies
- Regulatory Agencies - Govt. agencies to protect public interest (e.g. TRAI, FCC)
  - Regulate radio, TV, wire/cable communication

Connection Oriented and Connectionless Services

- Connection Oriented Services
  - Requires prior session connection between sender and receiver
  - Sets up virtual links between the end systems through a network
  - Reliable network service
  - Suitable for Long messages
  - High overhead, thus greater BW demand
  - Example: Telephone call

Connection Oriented and Connectionless Services

- Connection Less Services
  - No prior connection between sender and receiver required
  - Less overhead
  - Suitable for Short messages, real-time traffic
  - No reliability
  - Does not maintain state information
  - Example: email, SMS

Reliable and Unreliable Services

- Reliable Services
  - Assured delivery of message from sender to receiver
  - Requires acknowledgement from the receiver about receipt of message
  - Large Overhead; unsuitable for real-time applications like Voice/video i.e multimedia
  - Example: TCP

Reliable and Unreliable Services

- Unreliable Services
  - Time-bound delivery of message; No guarantee
  - Less Overhead; suitable for real-time applications like Voice/video i.e multimedia
  - Example: UDP

Data Communications and Networking Fourth Edition

Forouzan

Network Models

Slide Source: B. A. Forauzan, Data Communications and Networking, McGraw-Hill Online Learning Centre
http://highered.mheducation.com/sites/0072967757/information_center_view0/index.html

NETWORK MODELS

- Network- combination of hardware and software that sends data from one location to another
  - Hardware- physical equipment that carries signal
  - Software- consists instruction sets that make network services possible

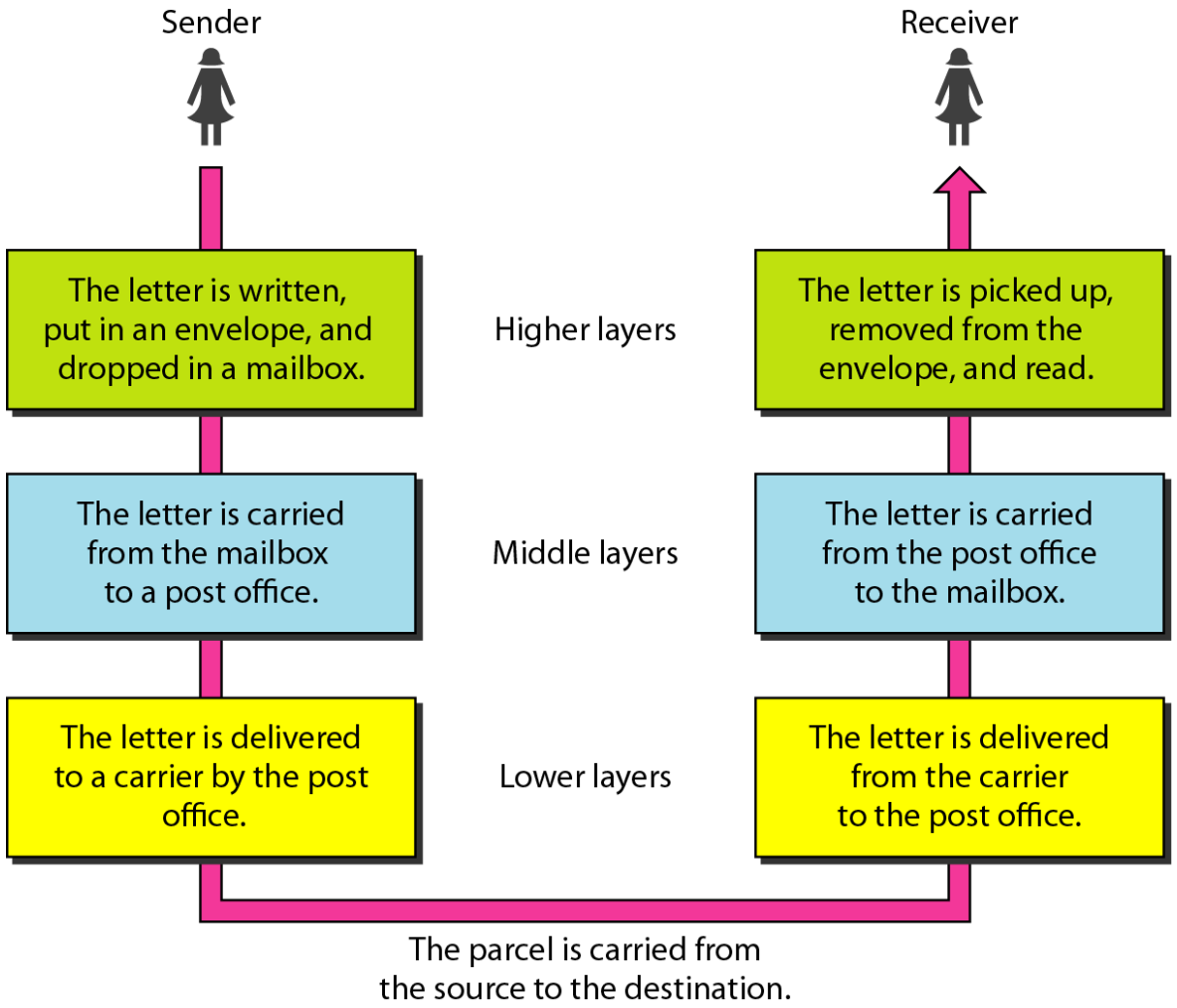
2-1 LAYERED TASKS

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 2.1 Tasks involved in sending a letter



2-2 THE OSI MODEL

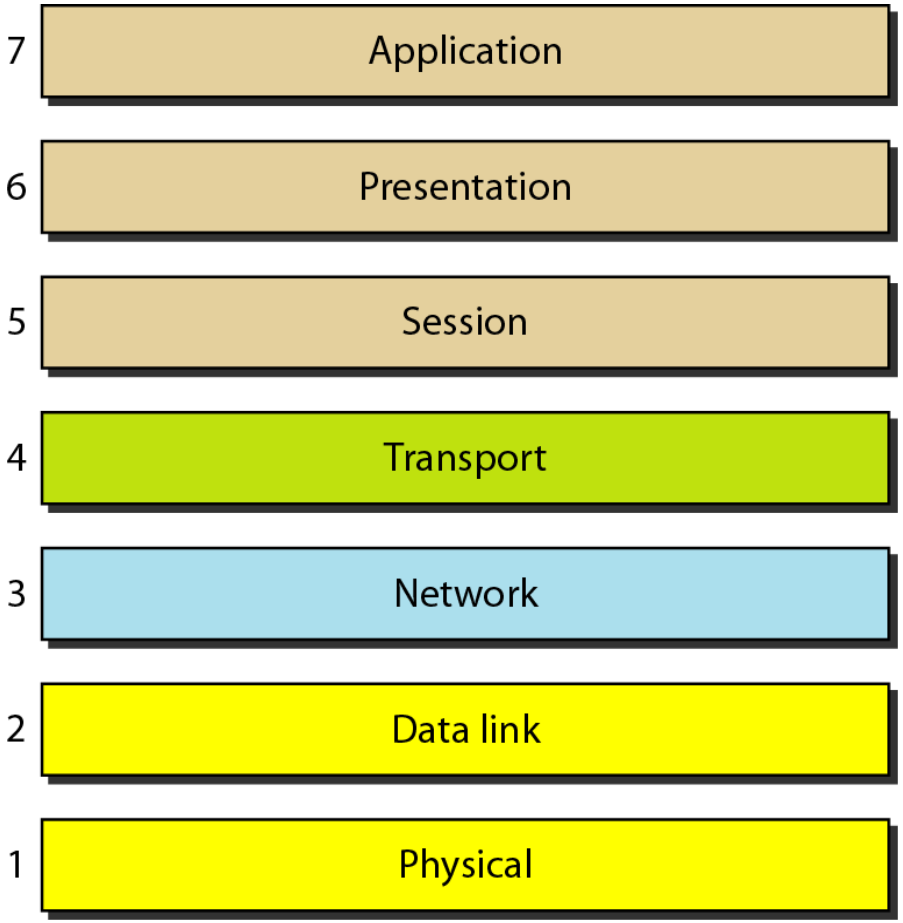
- ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model; introduced in the late 1970s
  - To Facilitate communication between different systems without requiring changes to the underlying hardware and software
- Layered framework for the design of network systems that allows communication between all types of computer systems

- Composed of 7 separate but related layers (ordered)

Note

ISO is the organization.
OSI is the model.

Figure 2.2 *Seven layers of the OSI model*



OSI MODEL …

- Each layer defines part of the process of moving information across a network
- Networking functions with related uses are collected into discrete groups→ layers
- Allows complete interoperability between incompatible systems
- Subgroups: Network support layers (Physical, Data link and Network layer), User support layers (Application, Presentation and Session); Transport layer -interface between the two
- Within a single machine, each layer calls upon the services of a layer just below it

- Peer Processes: processes on each machine that communicate at a given layer

Figure 2.3 *The interaction between layers in the OSI model*

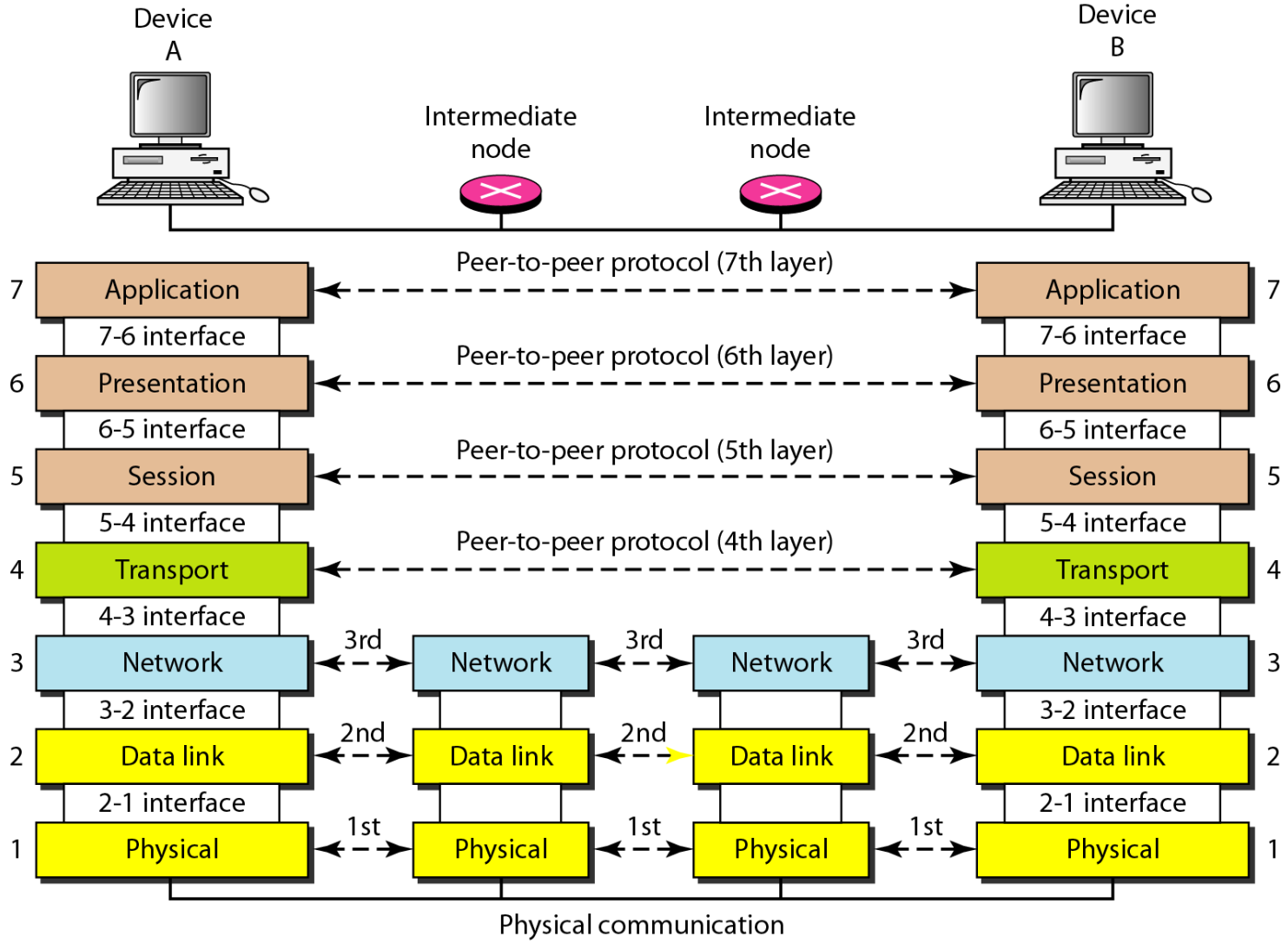
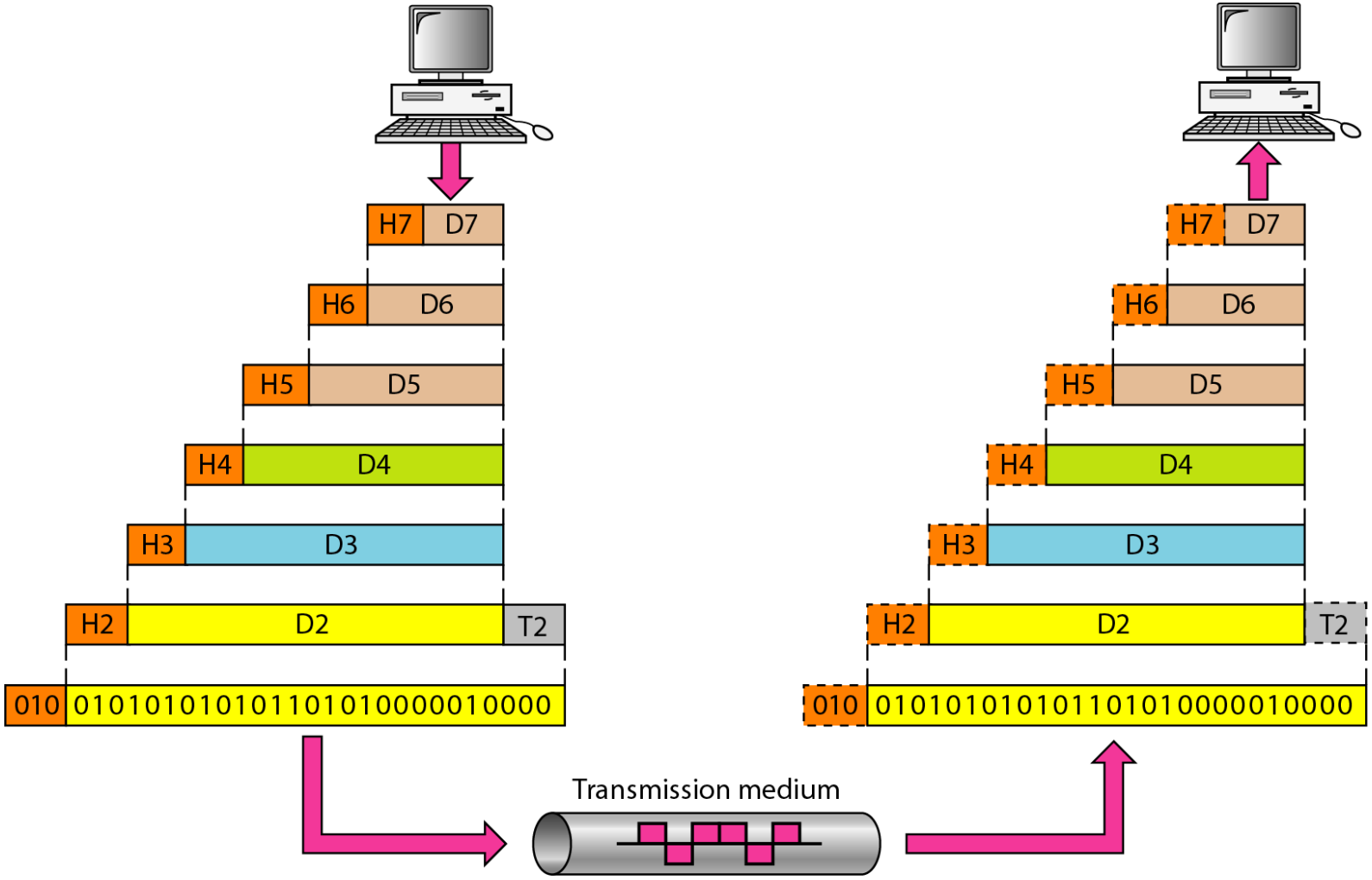


Figure 2.4 *An exchange using the OSI model*



2-3 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

Physical layer

- Coordinates functions required to carry a bit stream over physical medium
  - Electrical specifications of the interface and transmission medium
  - Defines procedures and functions to be performed by physical devices and interfaces

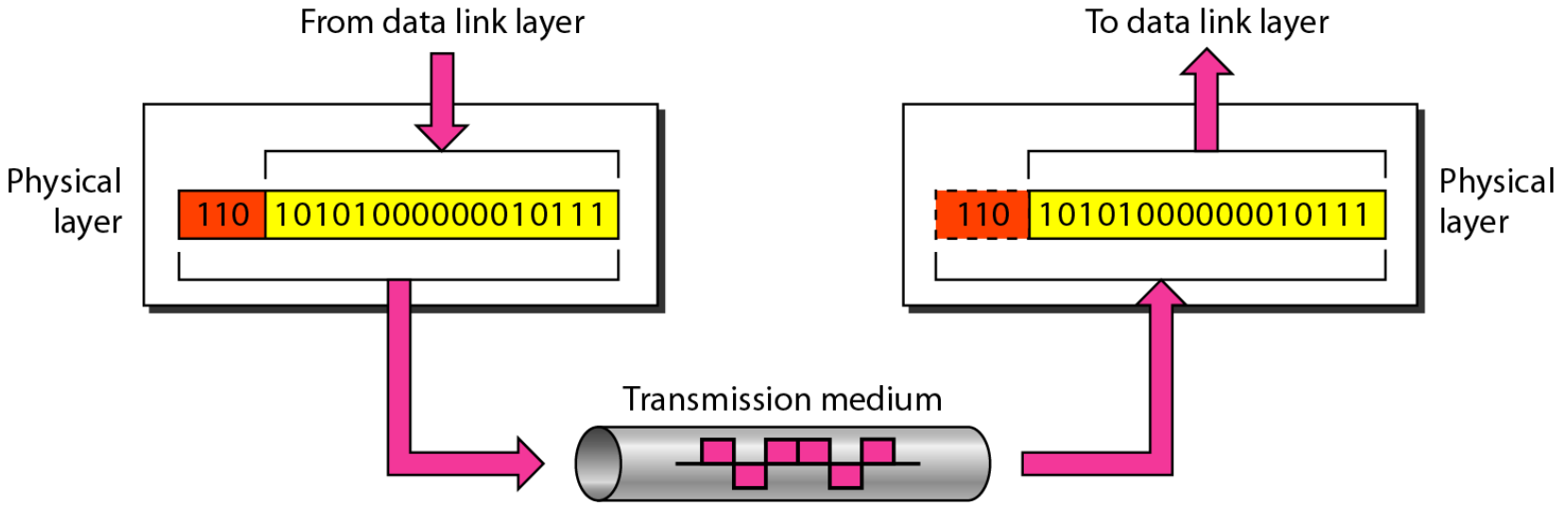
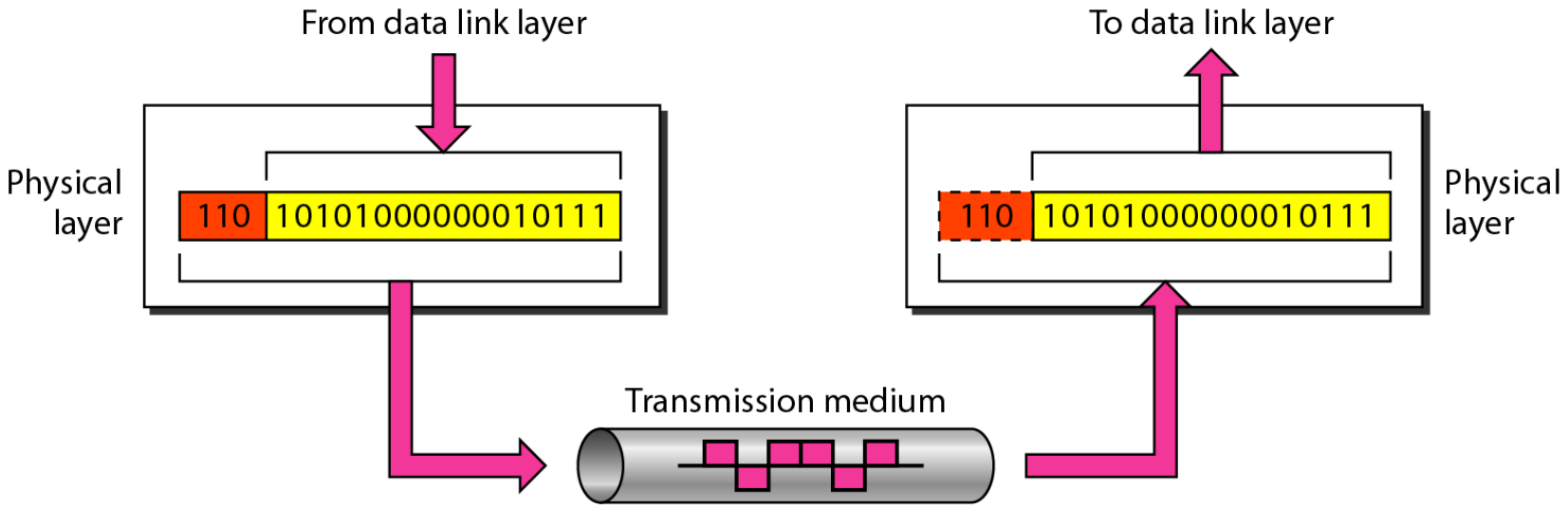


Figure 2.5 *Physical layer*



Physical layer

- Physical layer is also concerned with following:
  - Physical characteristics of interfaces and medium
  - Representation of bits (encoding; 0s and 1s changed to signals)
  - Data rate (bit duration)
  - Synchronization of bits (clock synchronization)
  - Line configuration (point-to-point/ multipoint)
  - Physical topology
  - Transmission mode (simplex/duplex)

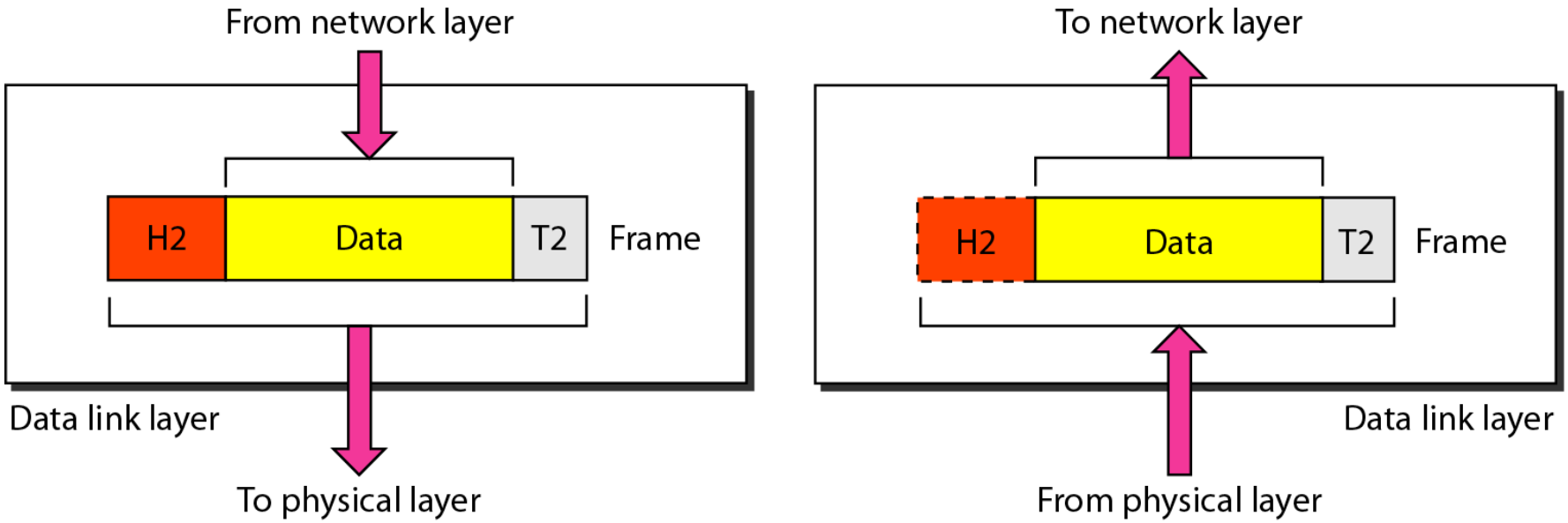
Note

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

Data Link layer

- Data link layer transforms the physical layer from raw transmission facility to a reliable link
  - responsible for moving frames from one hop (node) to the next
- Responsibilities
  - Framing: divides the stream of bits received into manageable data units called Frames
  - Physical Addressing: Address of sender and receiver of frame
  - Error control: adds reliability to the physical layer; detect and retransmit damaged or lost frame
  - Flow control: avoid overwhelming the receiver
  - Access control: defines which device has right to use the shared link/channel

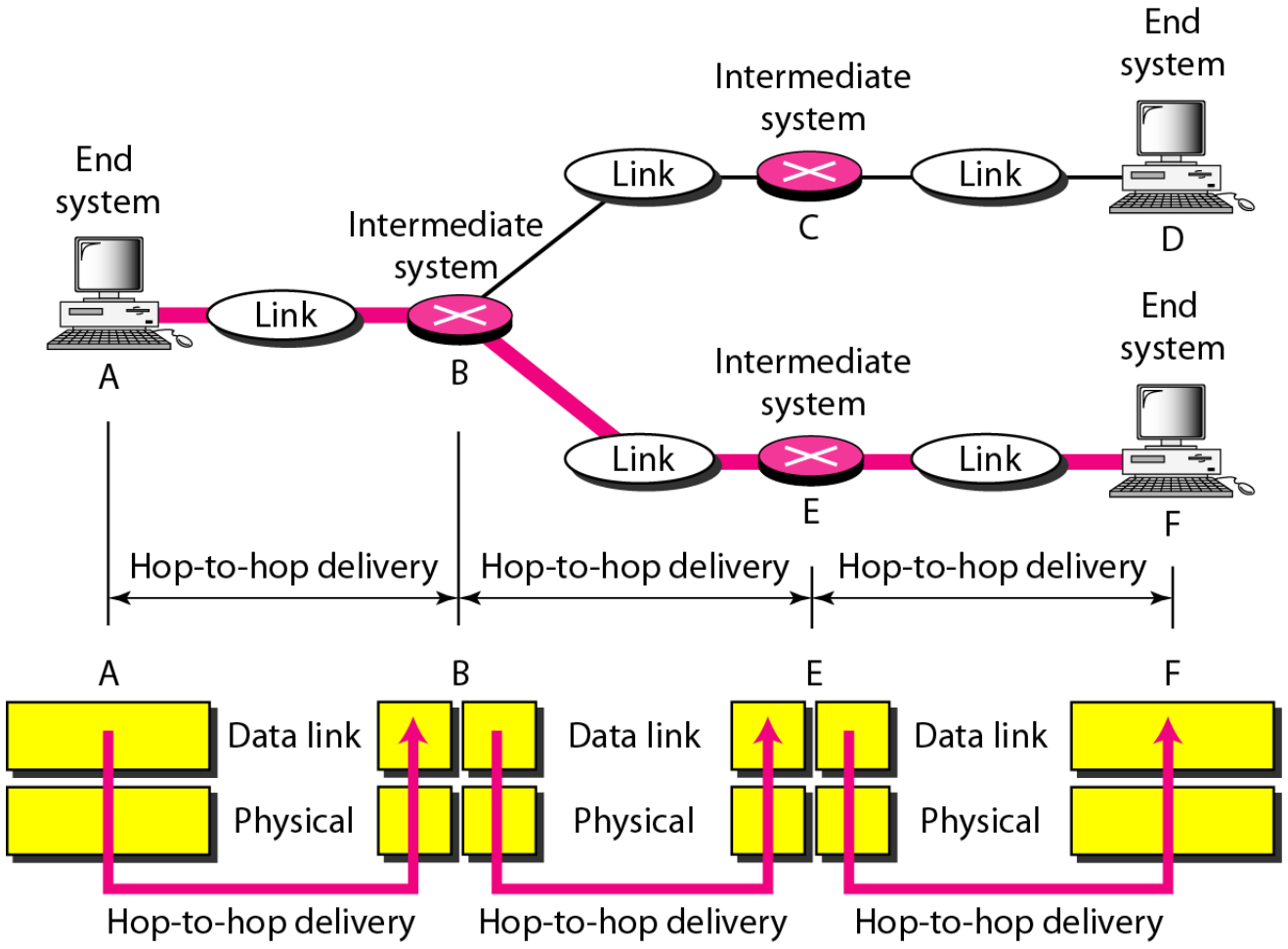
Figure 2.6 *Data link layer*



Note

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

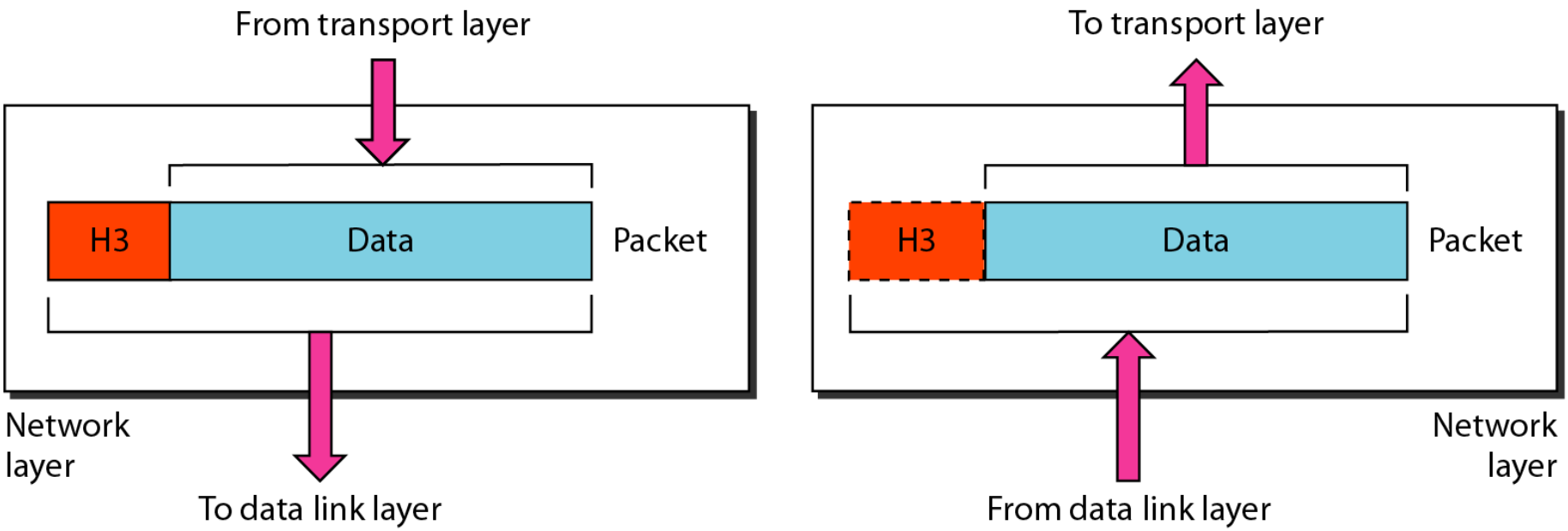
Figure 2.7 *Hop-to-hop delivery*



Network layer

- Responsible for source-to-destination delivery of packets across multiple networks
  - Needed when two systems are connected to different networks, with connecting devices between the networks
- Responsibilities
  - Logical Addressing: physical address cannot be used when packet passes the network boundary
  - Logical addressing used to distinguish source and destination system
  - Routing: Route packets to final destination over a large network or an internetwork of independent networks

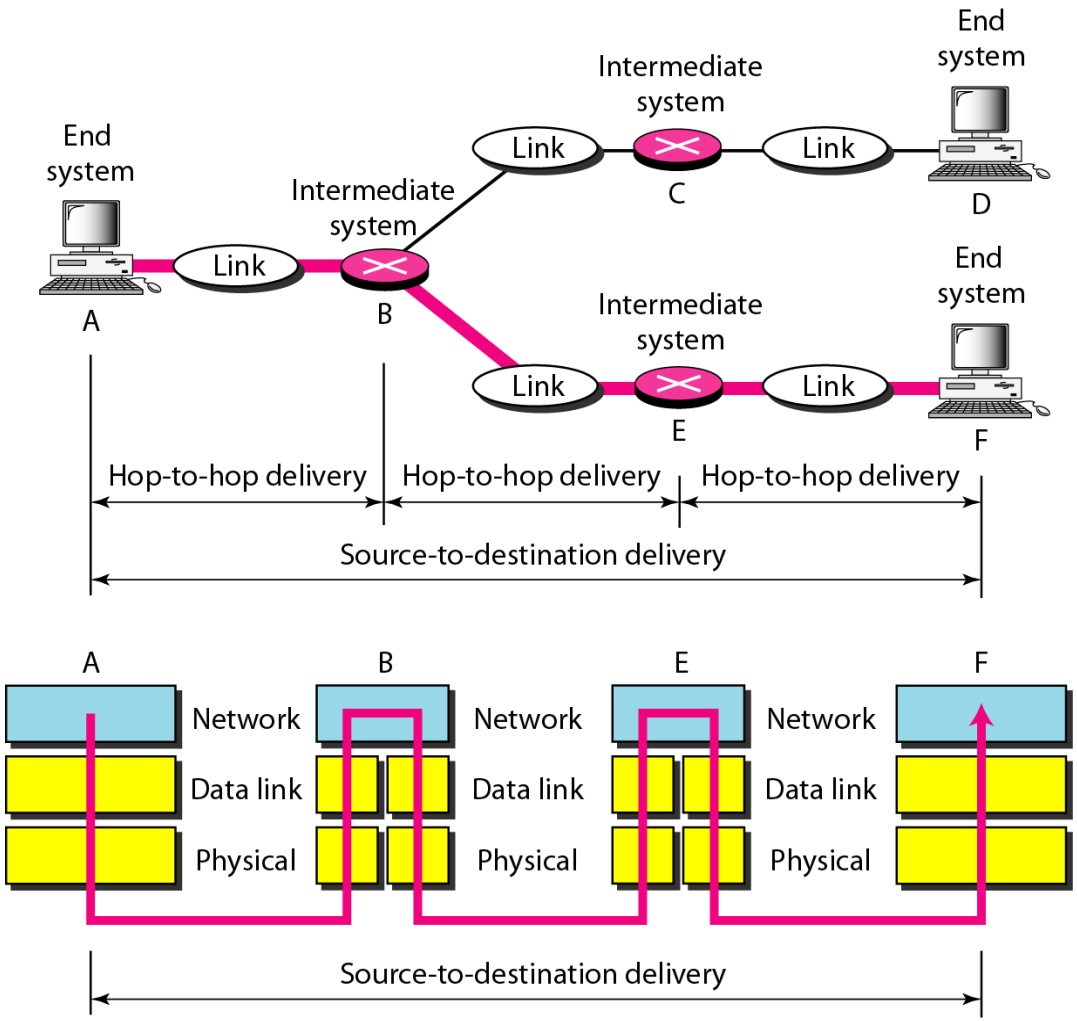
Figure 2.8 *Network layer*



Note

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

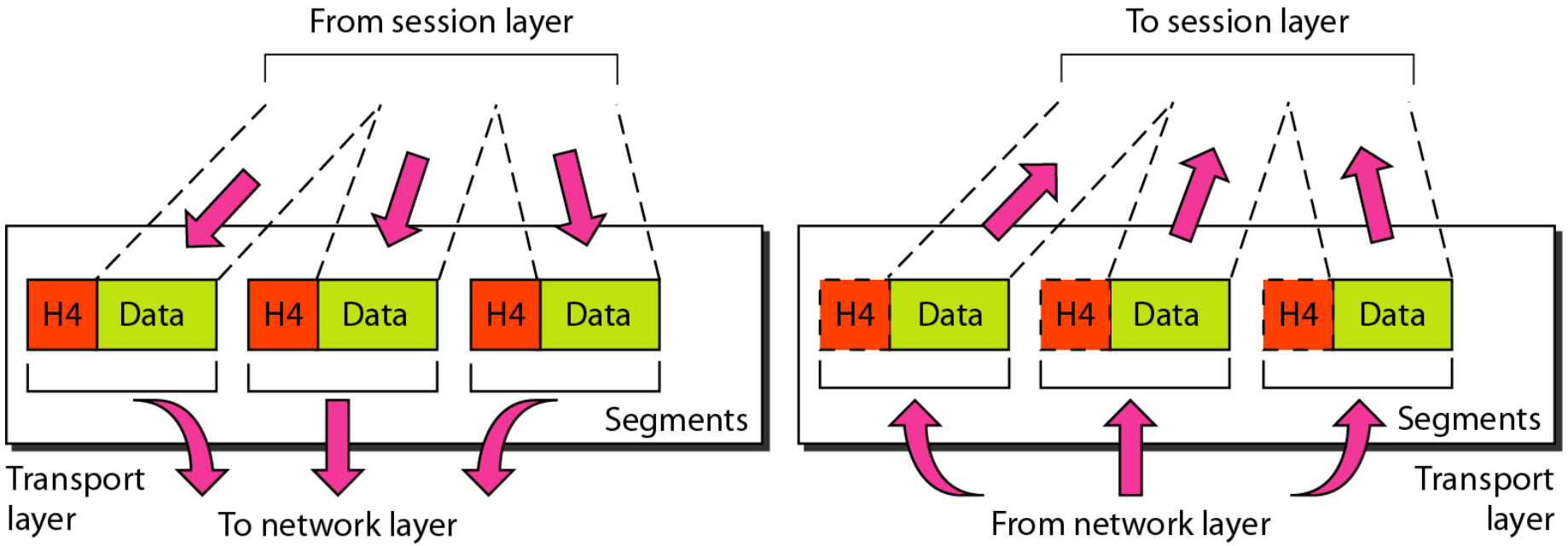
Figure 2.9 *Source-to-destination delivery*



Transport layer

- Responsible for process-to-process delivery of packets
  - Process- an application program running on host
  - Transport layer ensures that whole message arrives intact and in order
- Responsibilities
  - Service-point Addressing: Port addressing
    - *Network layer gets each packet to correct computer, Transport layer gets the entire message to correct process*
  - Segmentation and Reassembly: message divided into transmittable segments; sequence number
  - Connection control
  - Flow control and Error control

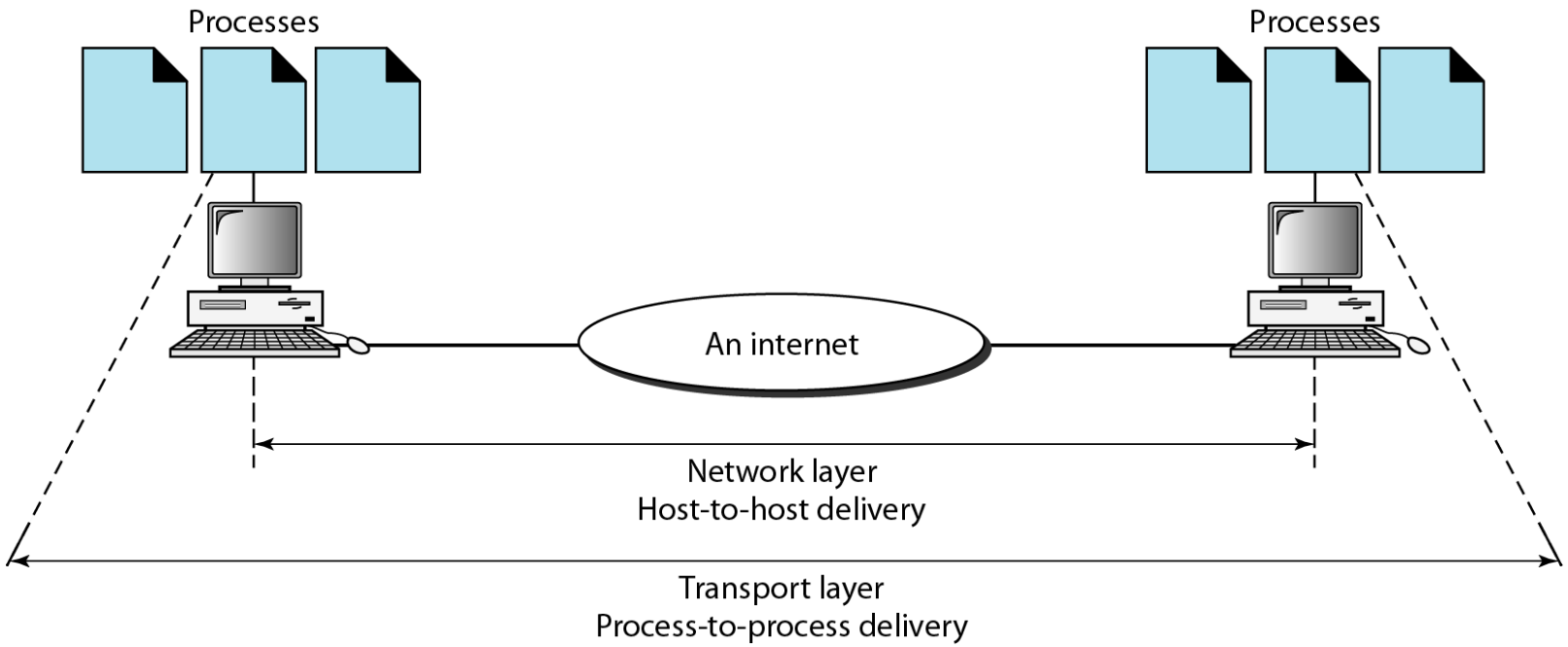
Figure 2.10 *Transport layer*



Note

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

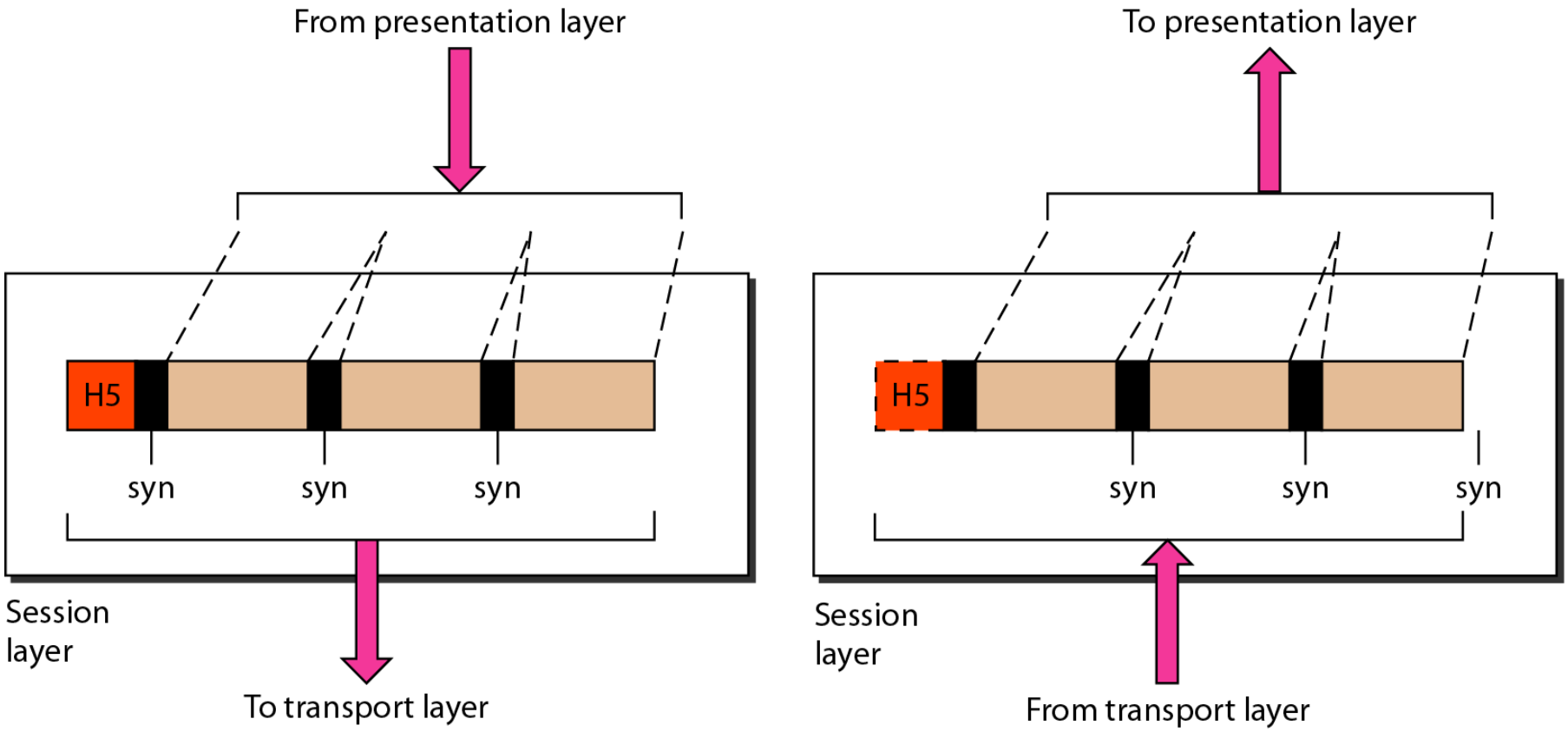
Figure 2.11 *Reliable process-to-process delivery of a message*



Session Layer

- Is the network *dialog controller; session manager*
  - Establishes, maintains and synchronizes the interaction among communicating systems
- Responsibilities
  - Dialog control: allows dialog between two systems; communication can take place in half-duplex or full-duplex
  - Synchronization: Check points/synchronization points added to stream of data
  - e.g large file of 1000 pages; checkpoint every 100 page

Figure 2.12 *Session layer*



Note

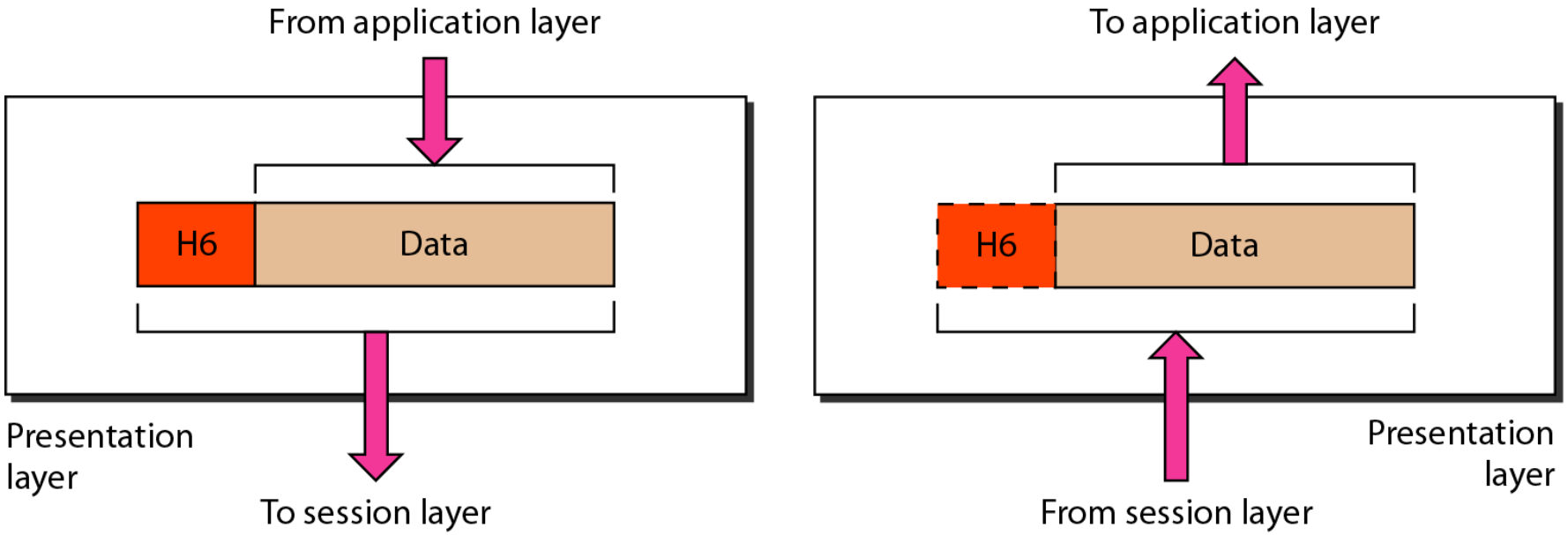
The session layer is responsible for dialog control and synchronization.

Presentation Layer

- Concerned with syntax and semantics of the information exchanged

- Responsibilities
  - Translation: changes the information from machine dependent format to machine independent format
  - Compression: reduce the amount of bits/data in the information
  - Encryption: ensure privacy

Figure 2.13 *Presentation layer*



Note

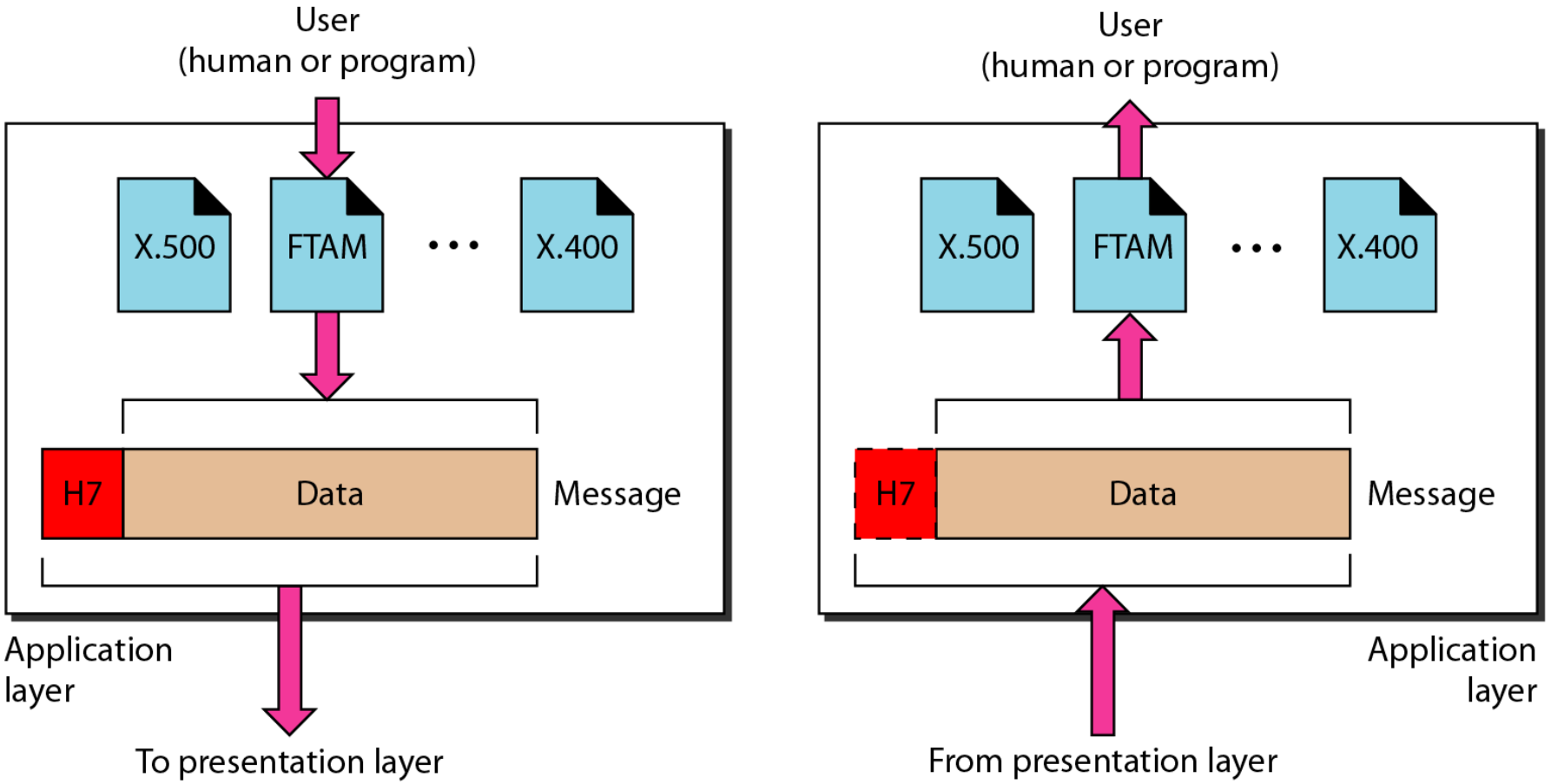
The presentation layer is responsible for translation, compression, and encryption.

Application Layer

- Enables users to access the network; provides user interfaces and support for services
  - Responsible for providing services to the user

- Services provided-
  - Network virtual terminal: allows user to log on to remote host
  - File transfer, access and management: allows user to access files on remote host
  - Mail services: e-mail forwarding and storage
  - Directory services: provides database sources and access for global information about various objects and services

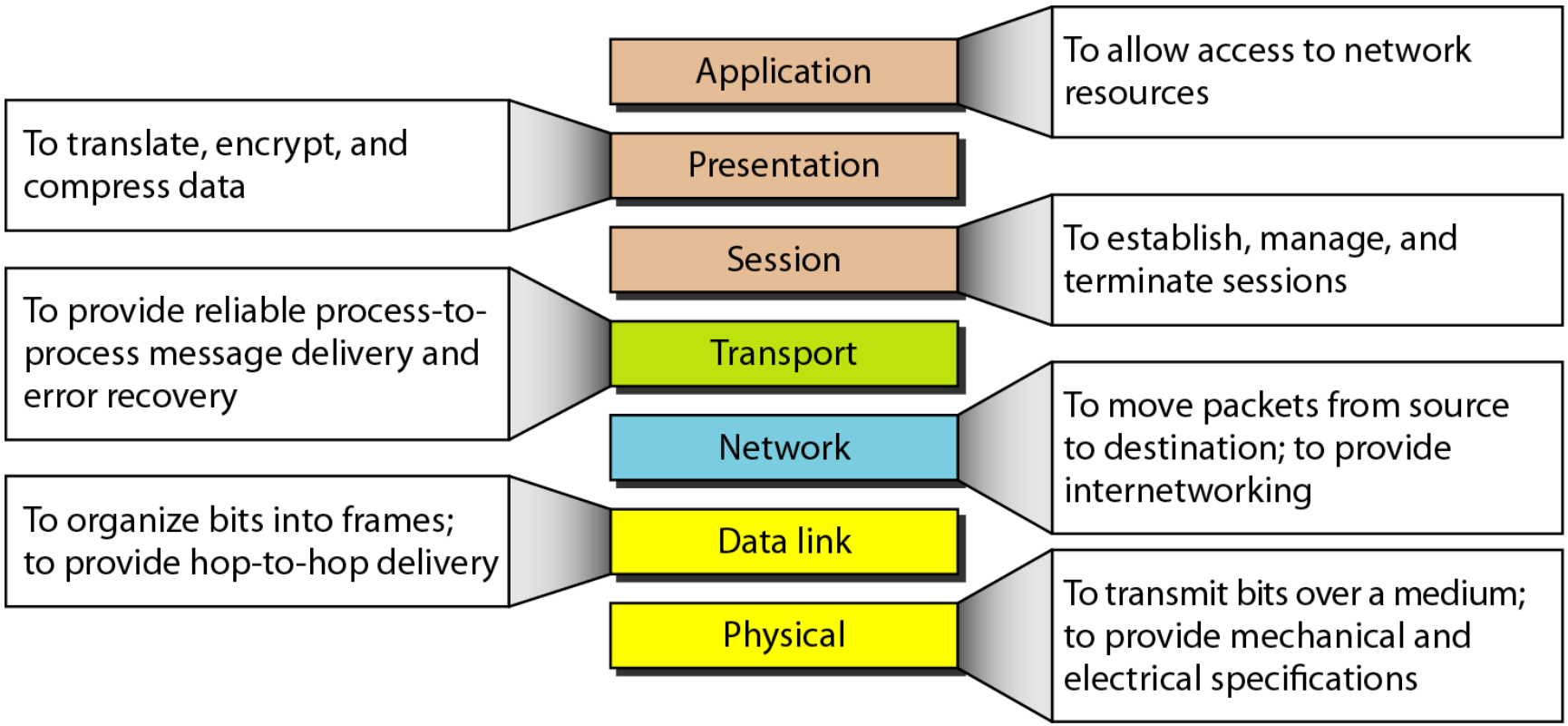
Figure 2.14 *Application layer*



Note

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

Figure 2.15 *Summary of layers*



2-4 TCP/IP PROTOCOL SUITE

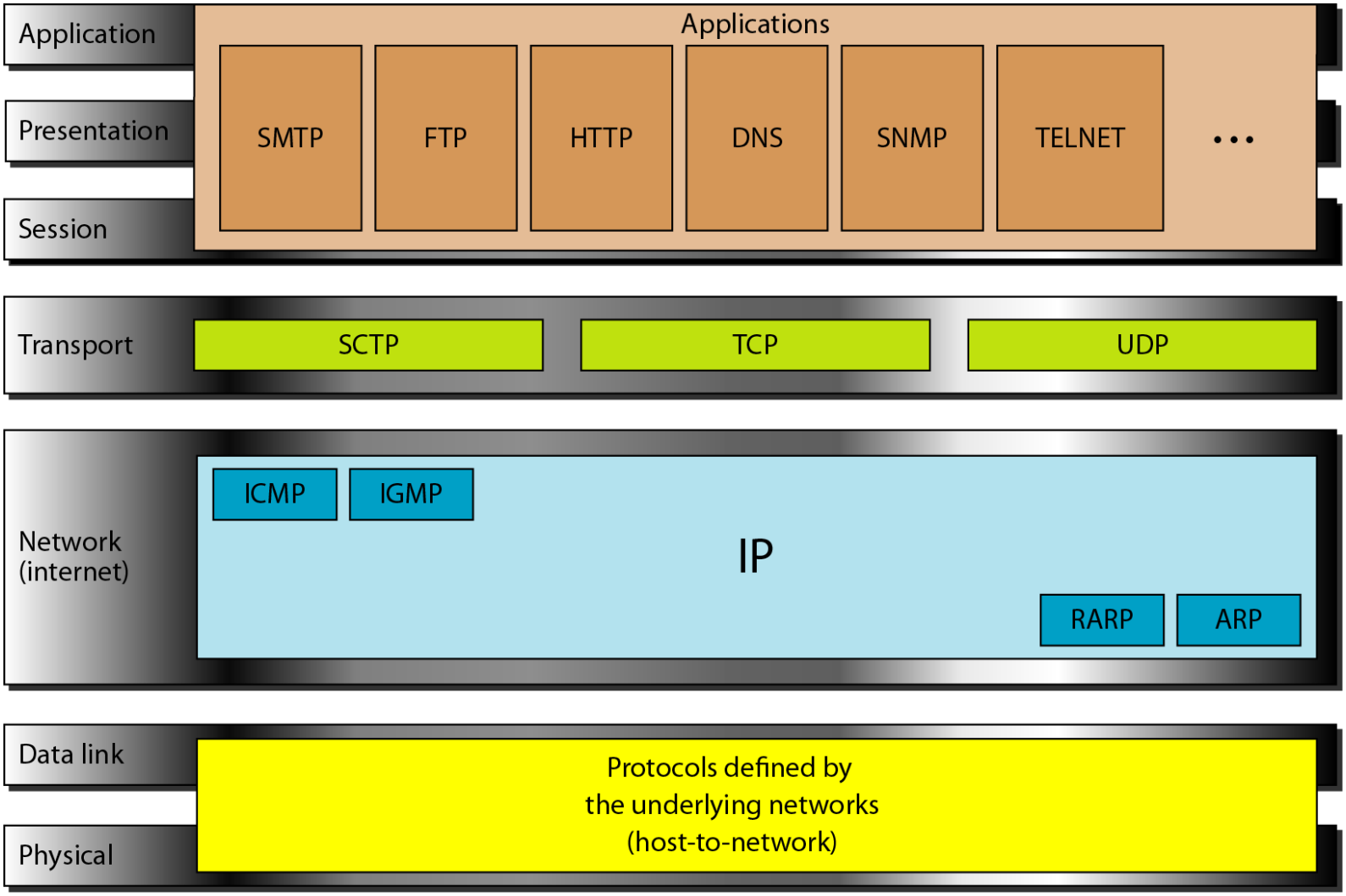
The layers in the TCP/IP protocol suite do not exactly match those in the OSI model.

The original TCP/IP protocol suite had four layers: host-to-network, internet, transport, and application. 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

Figure 2.16 *TCP/IP and OSI model*



2-5 ADDRESSING

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

Topics discussed in this section:

Physical Addresses
Logical Addresses
Port Addresses
Specific Addresses

Figure 2.17 *Addresses in TCP/IP*

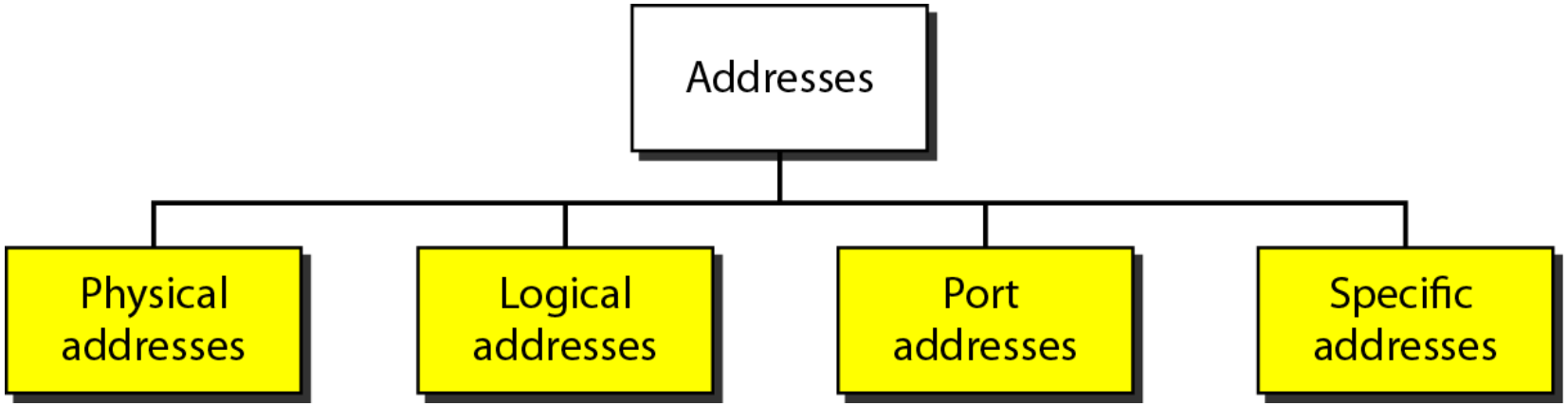
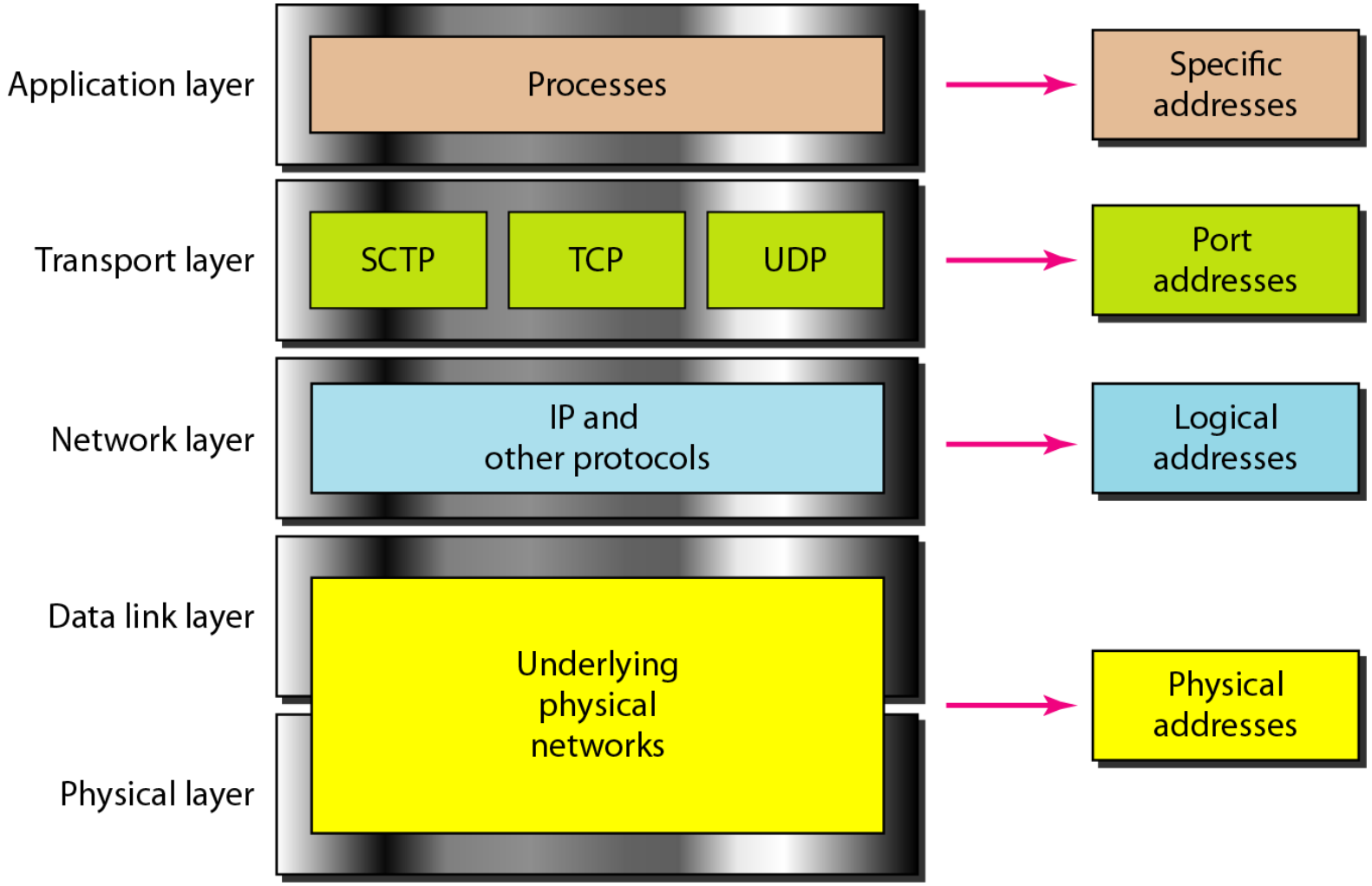


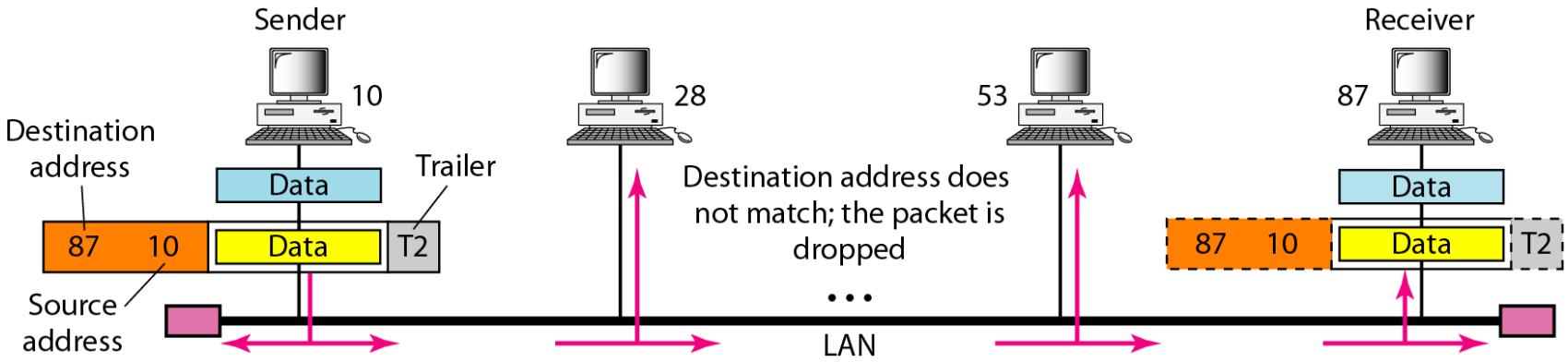
Figure 2.18 *Relationship of layers and addresses in TCP/IP*



Example 2.1

In Figure 2.19 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.

Figure 2.19 *Physical addresses*



Example 2.2

As we will see in Chapter 13, 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:

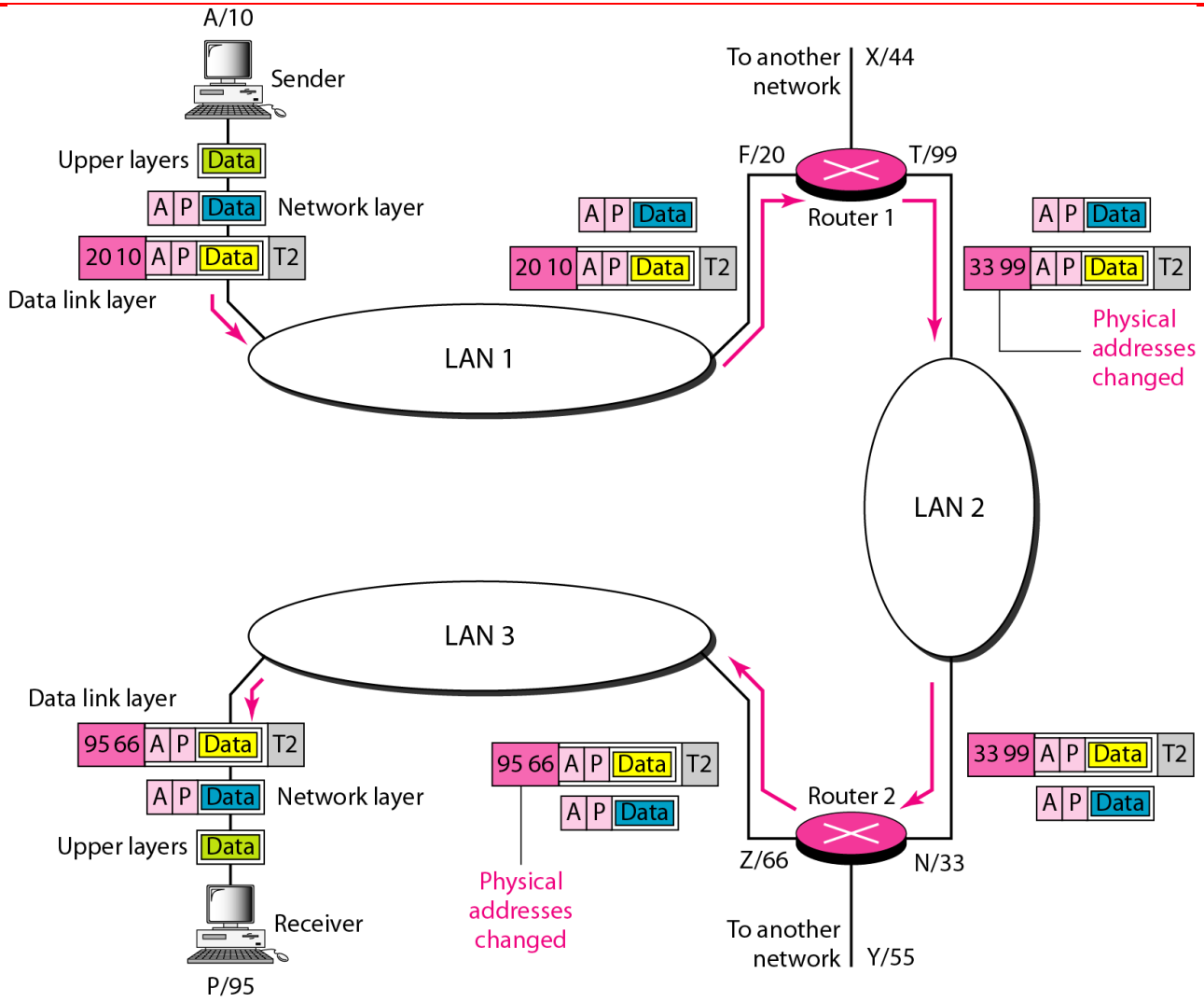
07:01:02:01:2C:4B

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

Example 2.3

Figure 2.20 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.

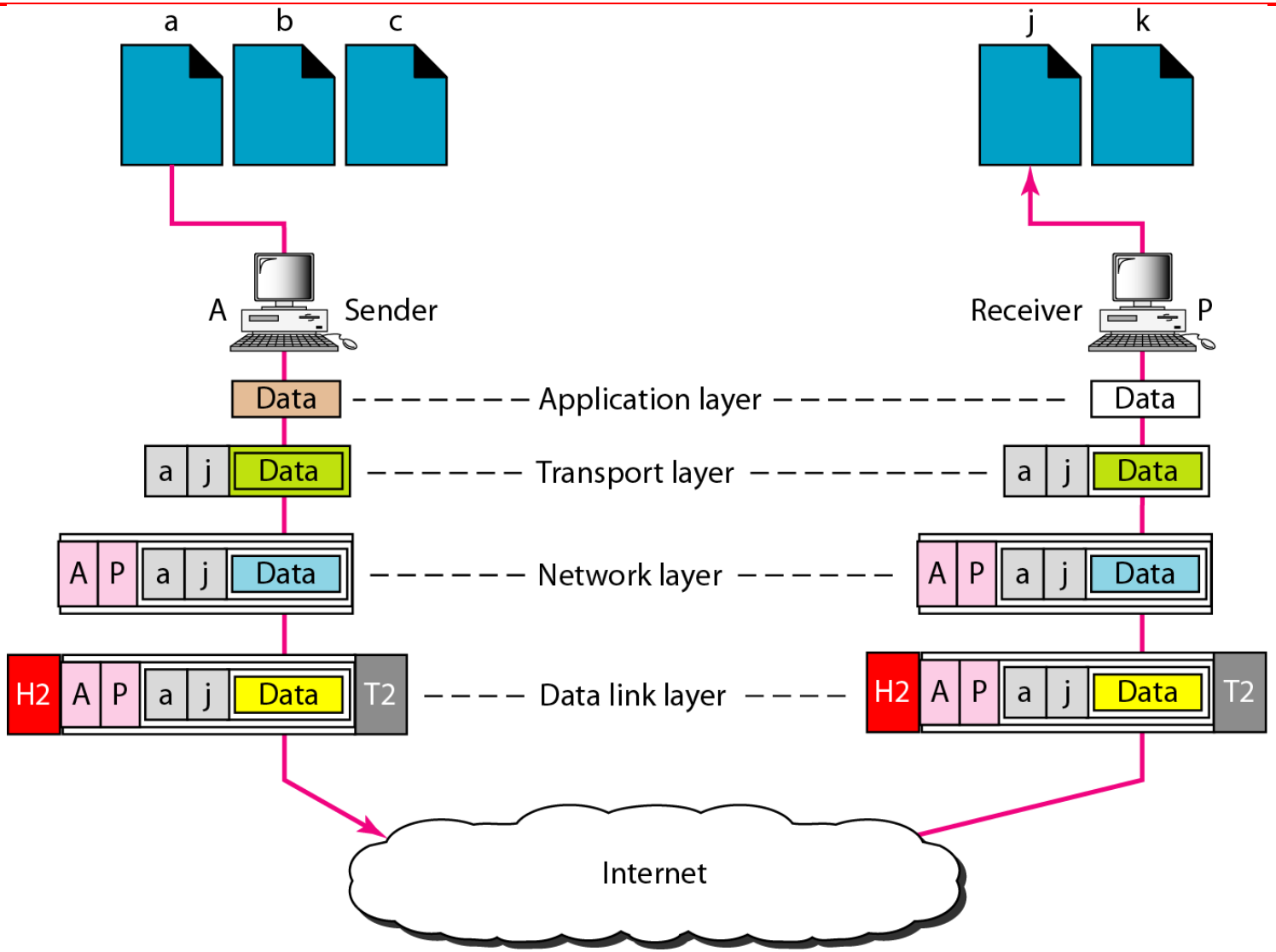
Figure 2.20 *IP addresses*



Example 2.4

Figure 2.21 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 2.21 *Port addresses*



Note

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

Example 2.5

As we will see in Chapter 23, 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.

Note

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