Network Models

Sachin Gajjar
sachin.gajjar@nirmauni.ac.in

Reading Material for this topic

- DATA COMMUNICATIONS AND NETWORKING, Fourth Edition by Behrouz A. Forouzan, Tata McGraw-Hill
  - Chapter 2, Topic 2.1 to 2.5

Networking Standards

- Standards: documented agreements containing technical specifications or other precise criteria on how particular products or services should be designed or performed
  - Guidelines to manufacturers, vendors, government agencies, other service providers to ensure interconnectivity in marketplace and in international communications.
  - Many different organizations to oversee computer industry's standards eg. ISO, IEEE, EIA, ANSI

Data communication standards categories:

- De facto
  - not been approved by any organization but been adopted as standards through widespread usage
  - often established by manufacturers who seek to define functionality of a new product or technology.
  - Parallel port of PC
- De jure
  - standards that have been legislated by an officially recognized body
  - IEEE 802.11

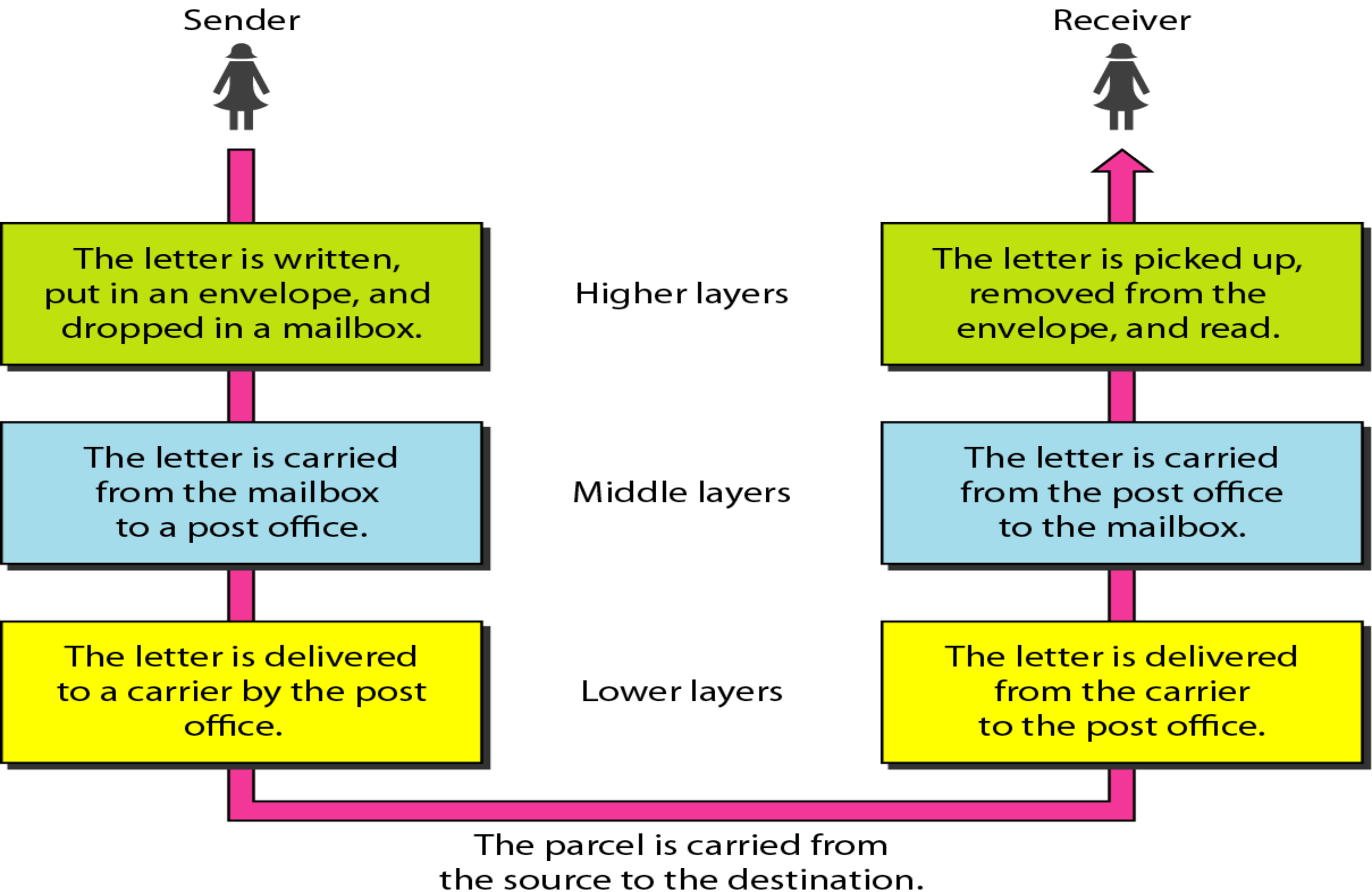
Protocols

- Set of rules that govern data communication
- Syntax (How)
  - structure or format of the data
  - first 8 bits of data= sender address, second 8 bits = receiver address, rest=message
- Semantics (What)
  - meaning of each section of bits
  - does an address identify route to be taken or final destination of the message, address = broadcast, multicast, individual
- Timing (When)
  - how fast
  - sender produces data at 100 Mbps, receiver can process data at 1 Mbps, some data will be lost at receiver
  - when data should be sent

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.***

Figure 2.1 Tasks involved in sending a letter



2-2 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.***

Note

ISO is the organization.
OSI is the model.

Figure 2.2 *Seven layers of the OSI model*

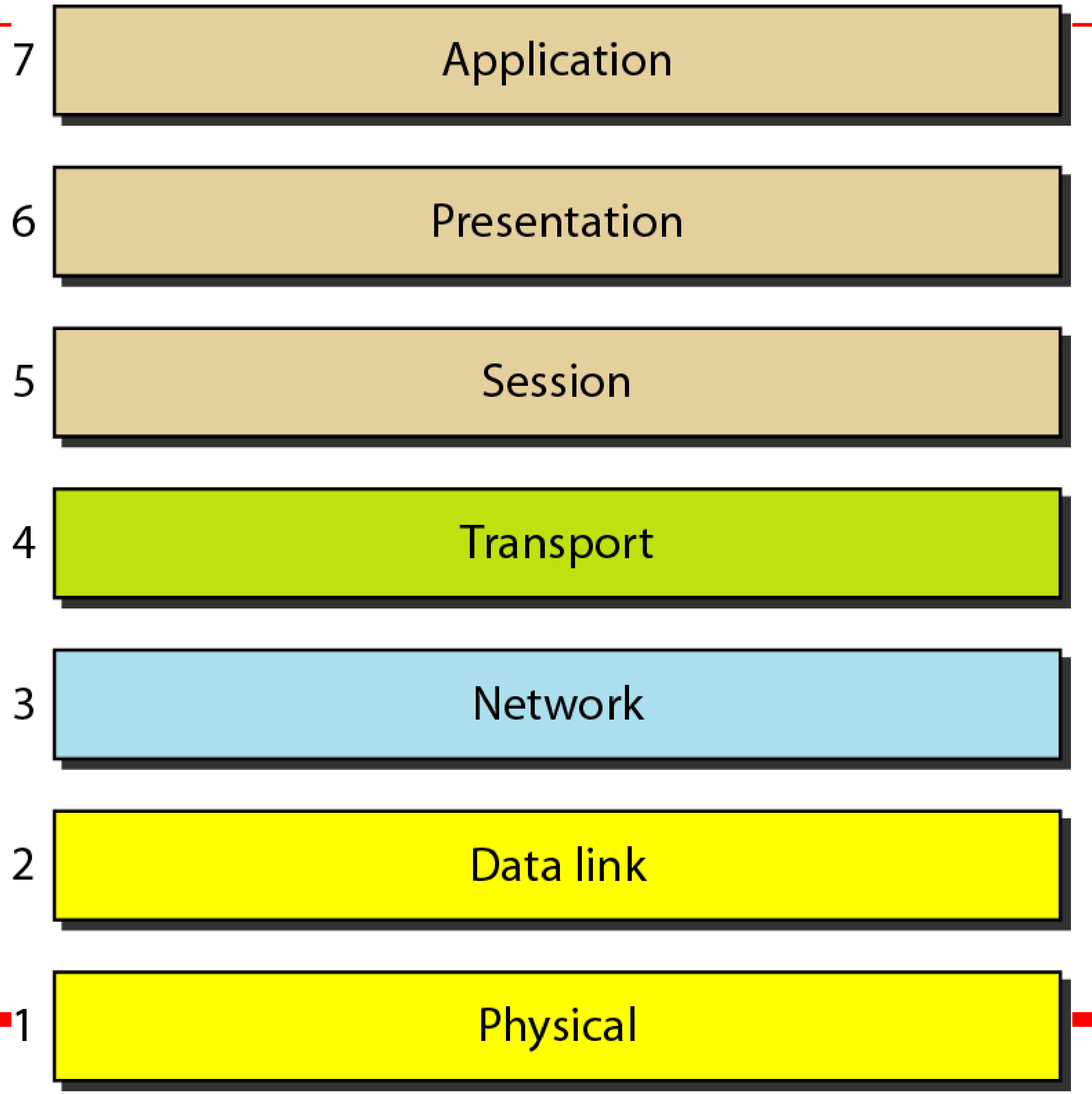
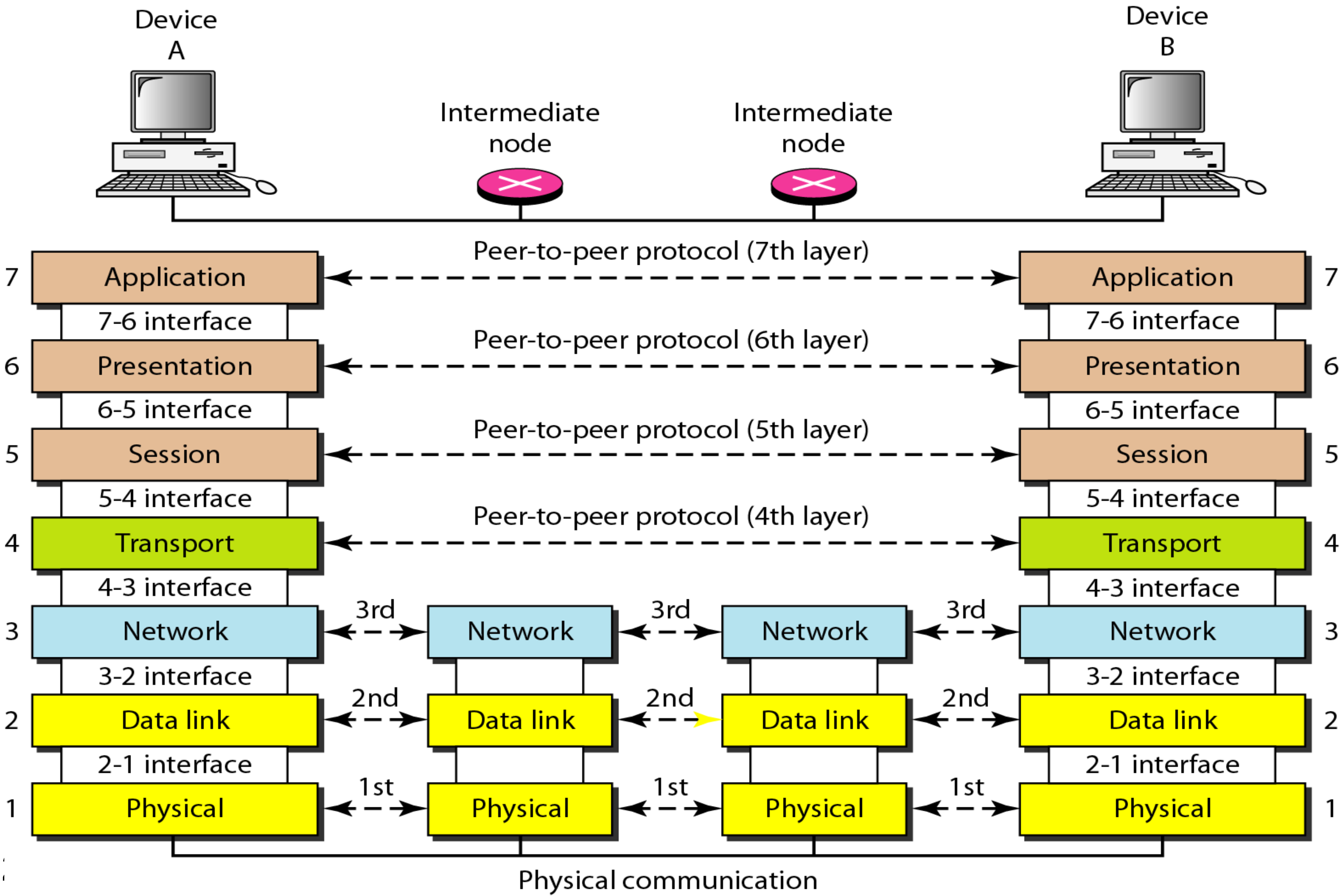


Figure 2.3 *The interaction between layers in the OSI model*



OSI Model – Layers

In developing the model, the designers distilled the process of transmitting data to its most fundamental elements. Eg. bits, signals, connectors, cables, medium access

Networking functions which had related uses were identified and collected those functions into discrete groups that became the layers. Eg. Physical layer – cables, connectors, signals

Each layer defines a family of functions distinct from those of the other layers.

Most importantly, the OSI model allows complete interoperability between otherwise incompatible systems eg. PC connecting to RPi

Layers…..

- **Within a single machine, each layer calls upon the services of the layer just below it.**
- **Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4.**

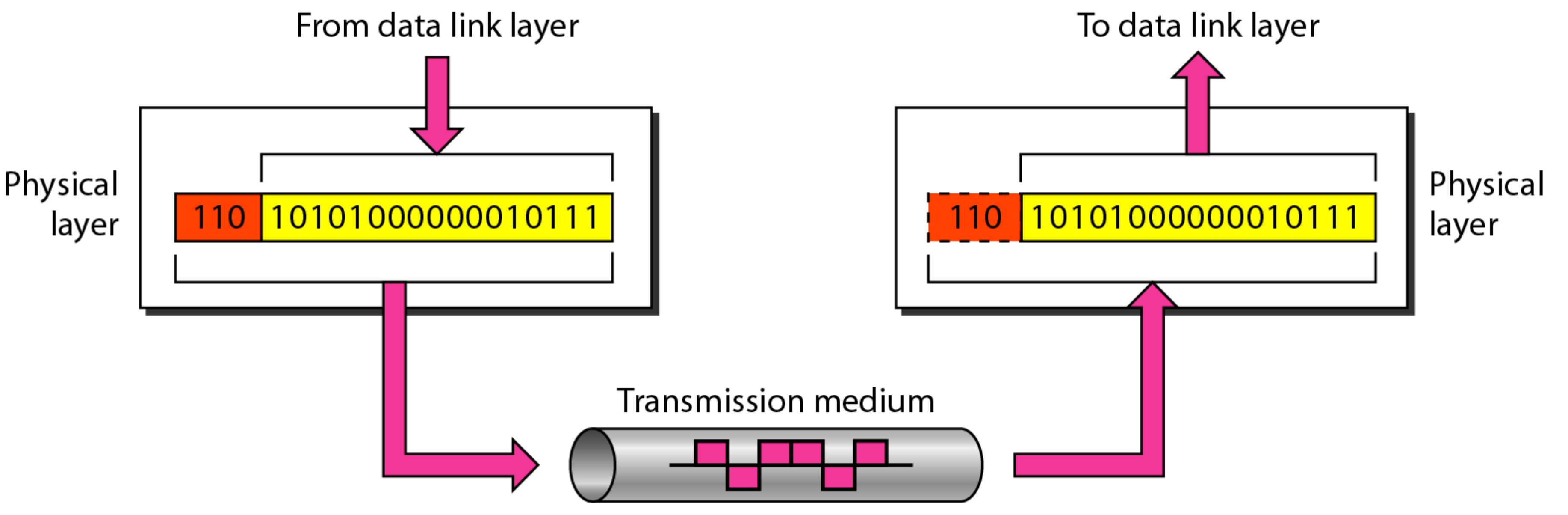
- **Between machines, layer *x* on one machine communicates with layer *x* on another machine.**

- **This communication is governed by an agreed-upon series of rules and conventions called protocols.**

FUNCTIONS of LAYERS IN THE OSI MODEL

Next we describe the functions of each layer in the OSI model.

Figure 2.5 *Physical layer*



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

Physical layer

- **Physical characteristics of the interfaces and medium: defines characteristics of interfaces between the devices and Transmission medium (connectors). Also define the type of the Transmission medium**

- **Representation of bits: To be transmitted, bits must be encoded into signals – electrical or optical. It defines the type of encoding**

- **Data rate: The transmission rate is also defined by the physical layer i.e. it defines the duration of a bit, which is how long it lasts**

- **Synchronization of bits: The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized**

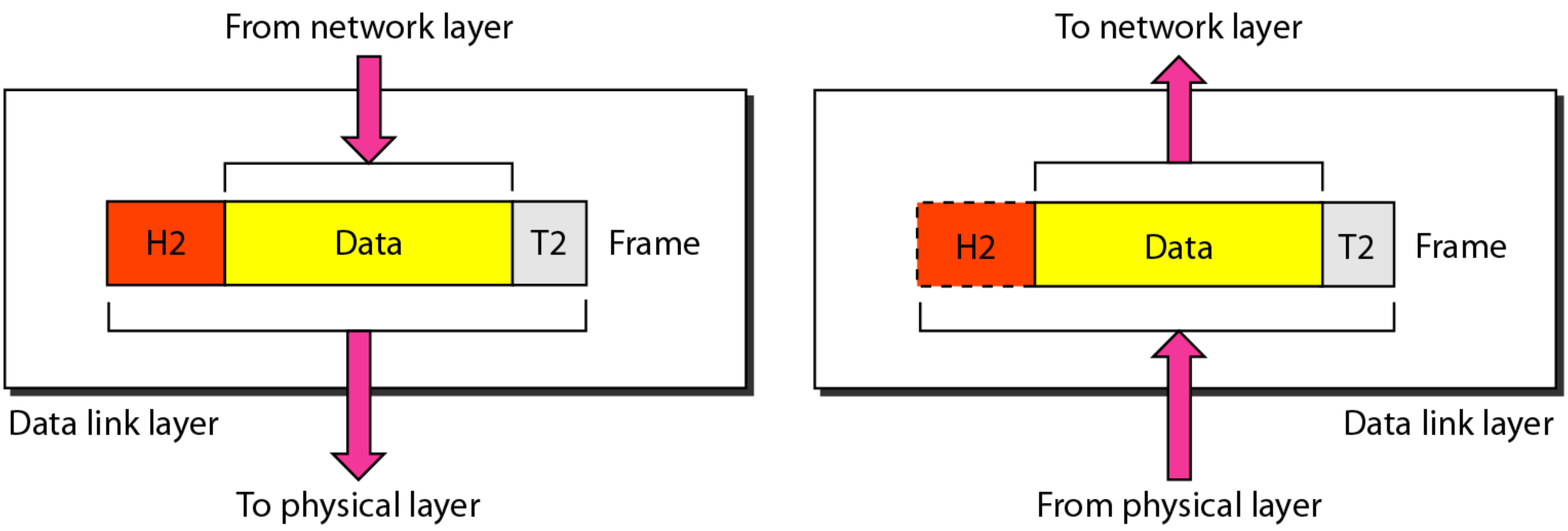
- **Line configuration. concerned with connection of devices to media. point-to-point configuration or multipoint configuration**

Physical Layer

- **Physical topology**: **The physical topology defines how devices are connected to make a network.**

- **Transmission mode: The physical layer also defines the direction of Transmission between two devices: simplex, half-duplex, or full-duplex.**

Figure 2.6 *Data link layer*



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

Data Link Layer Functionality

- **Framing:**
  Divides the stream of bits received from the Network layer into manageable data units called frames.

- **Physical addressing:**
  If frames are to be distributed to different systems on the network, the DLL adds a header to the frame to define the sender and/or receiver of the frame.
  Eg. Etherent address
  If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.

- **Flow control:**
  If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

Data Link Layer…

- **Error control:**
  The DLL 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 added 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 given time.

Figure 2.7 *Hop-to-hop delivery*

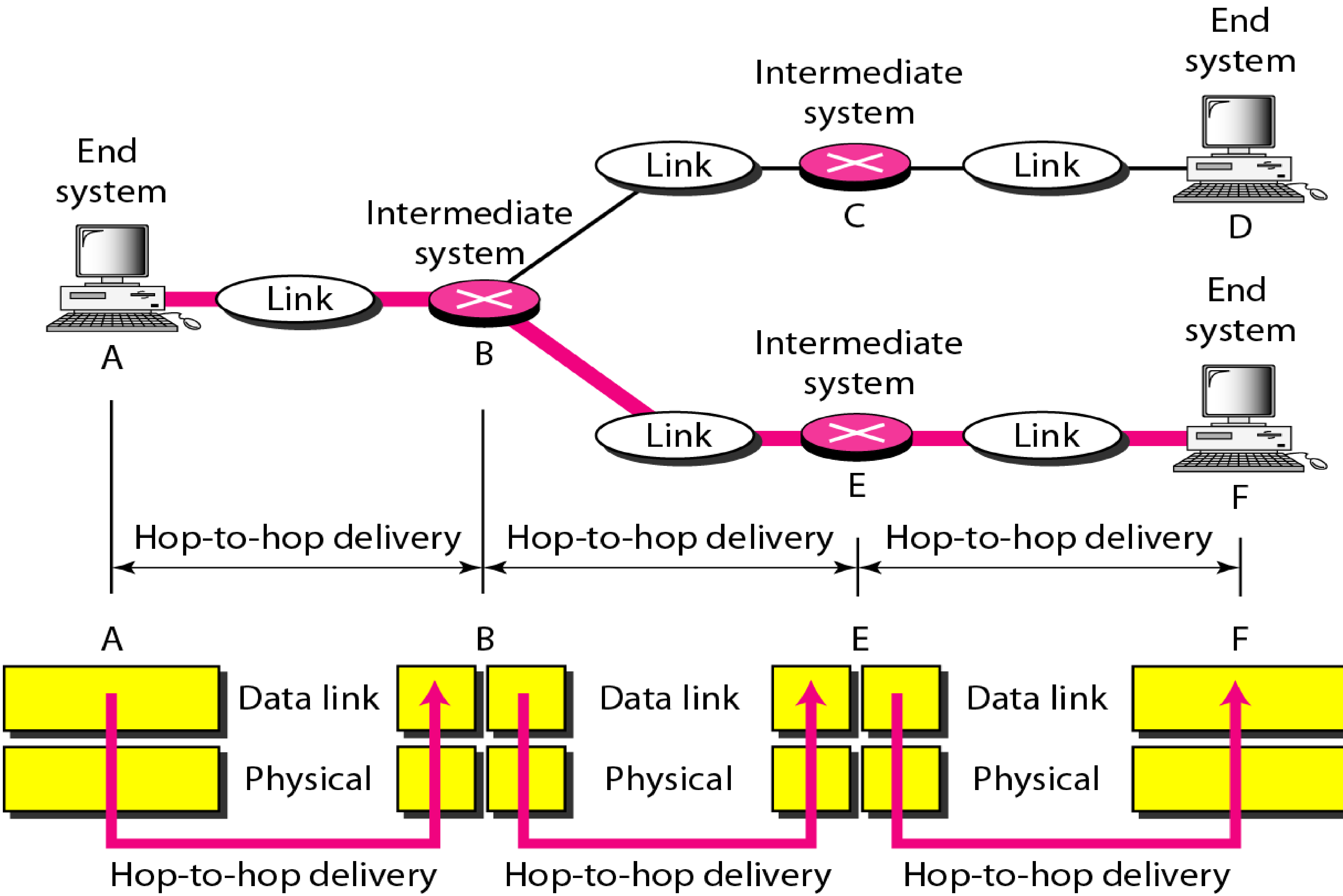
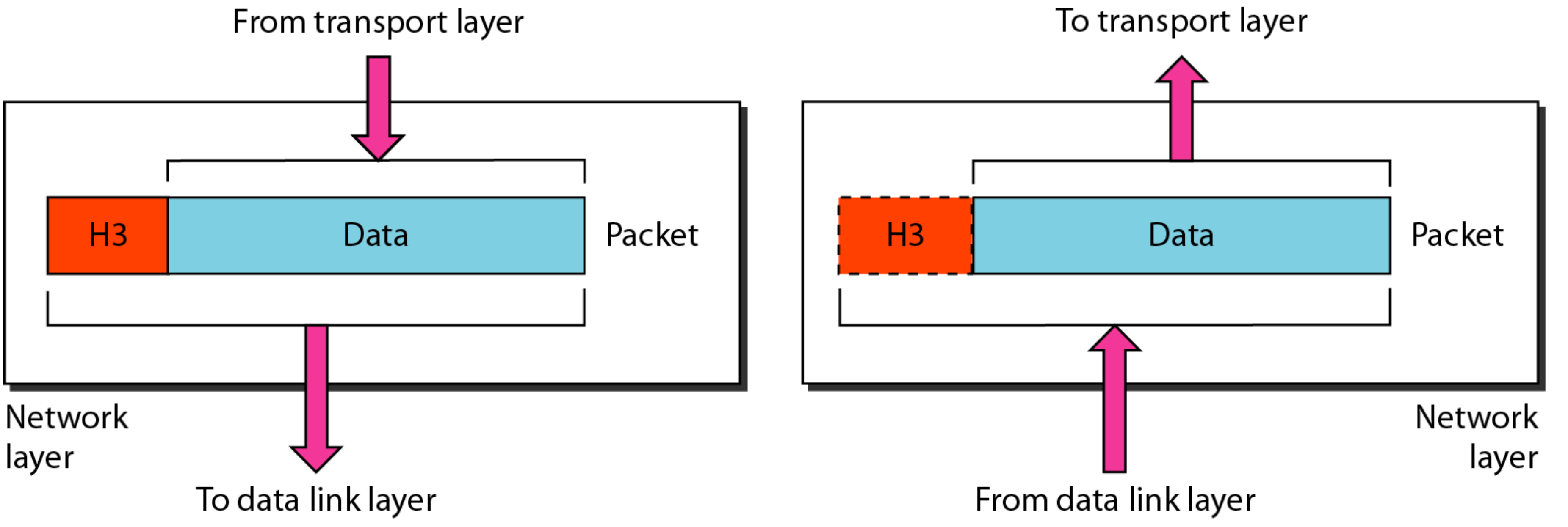


Figure 2.8 *Network layer*



The network layer is responsible for the delivery of individual packets from the source host to the destination host (both are in different networks).

Network Layer Functionality:

- **Logical addressing: The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, it need another addressing system to help distinguish the source and destination systems. The network layer adds logical addresses of the sender and receiver to the packet. Eg. IP Address**

- **Routing:**

  When independent networks or links are connected to create *Internetworks* (network of networks) , the connecting devices (called *routers)* route packets to their final destination. Network layer provides this mechanism

Figure 2.9 *Source-to-destination delivery*

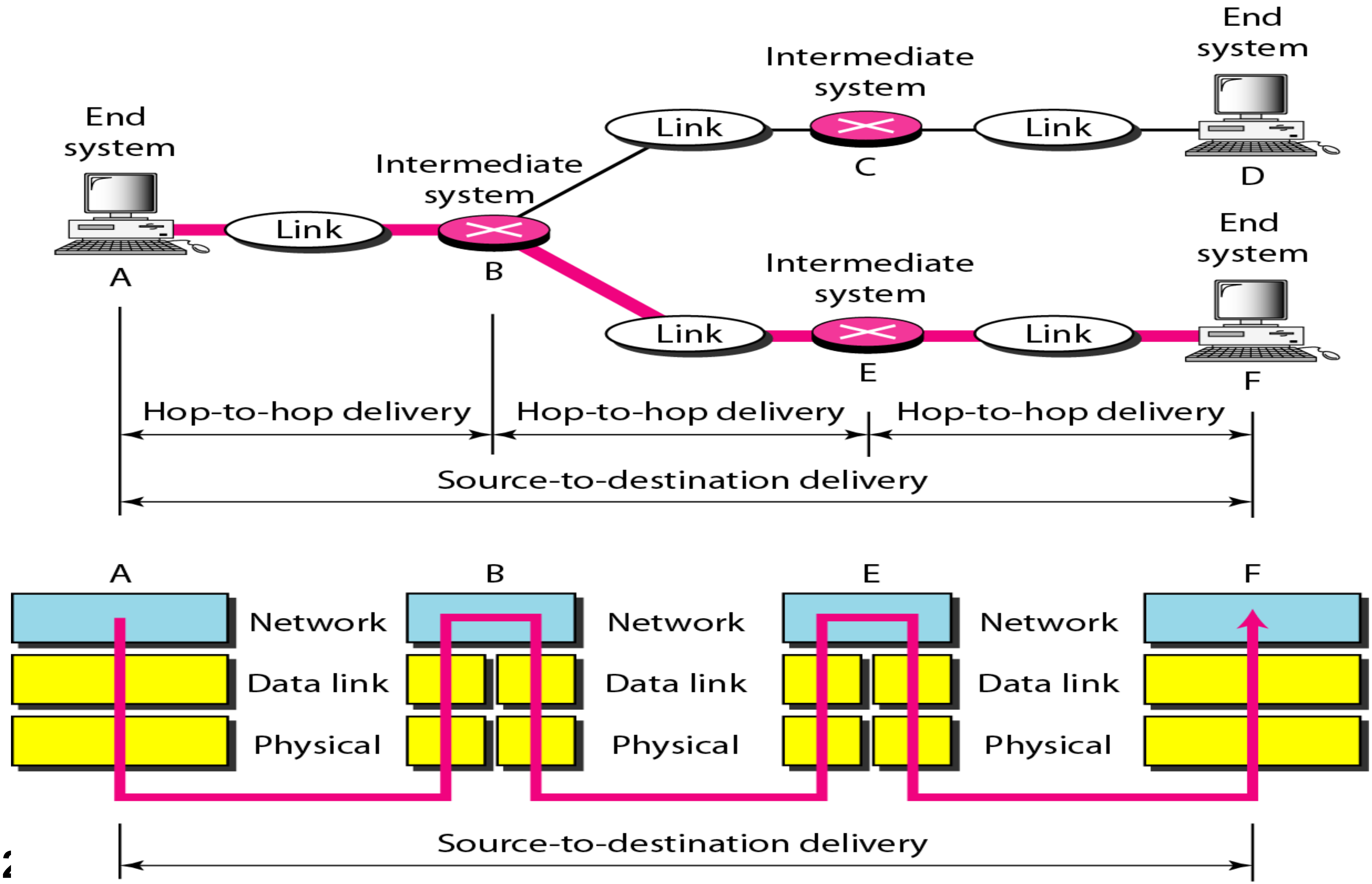
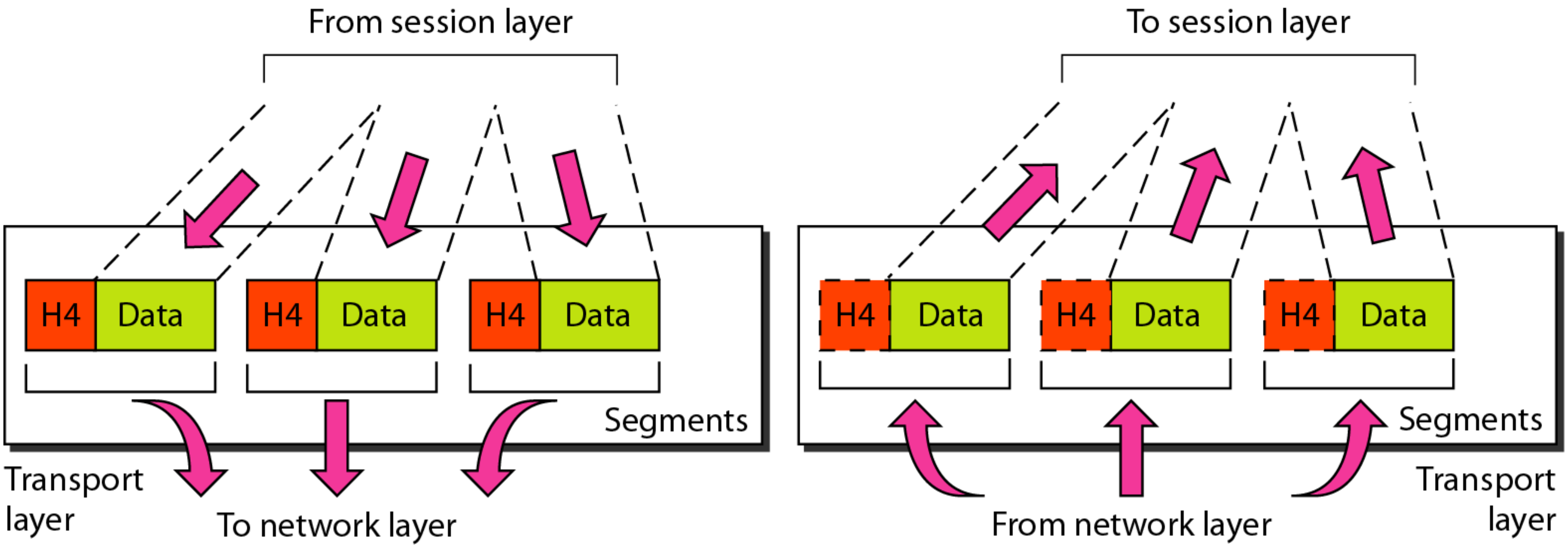
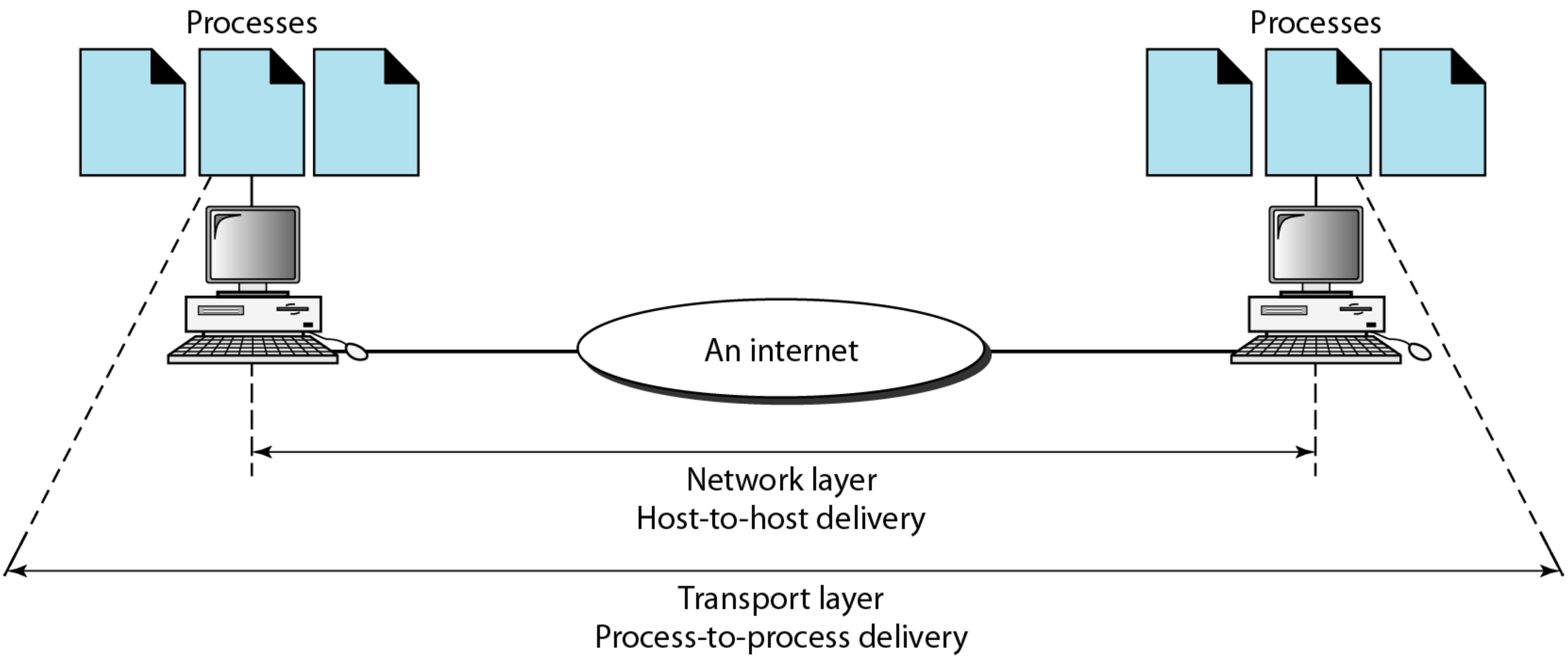


Figure 2.10 *Transport layer*



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

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



Transport Layer Functionality

- **Service-point addressing**: Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other.

  - The transport layer header must therefore include a type of address called a ***service-point address*** **(or port address)**.

  - The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

- **Segmentation and reassembly**: A message is divided into transmittable segments, with each segment containing a sequence number.

These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

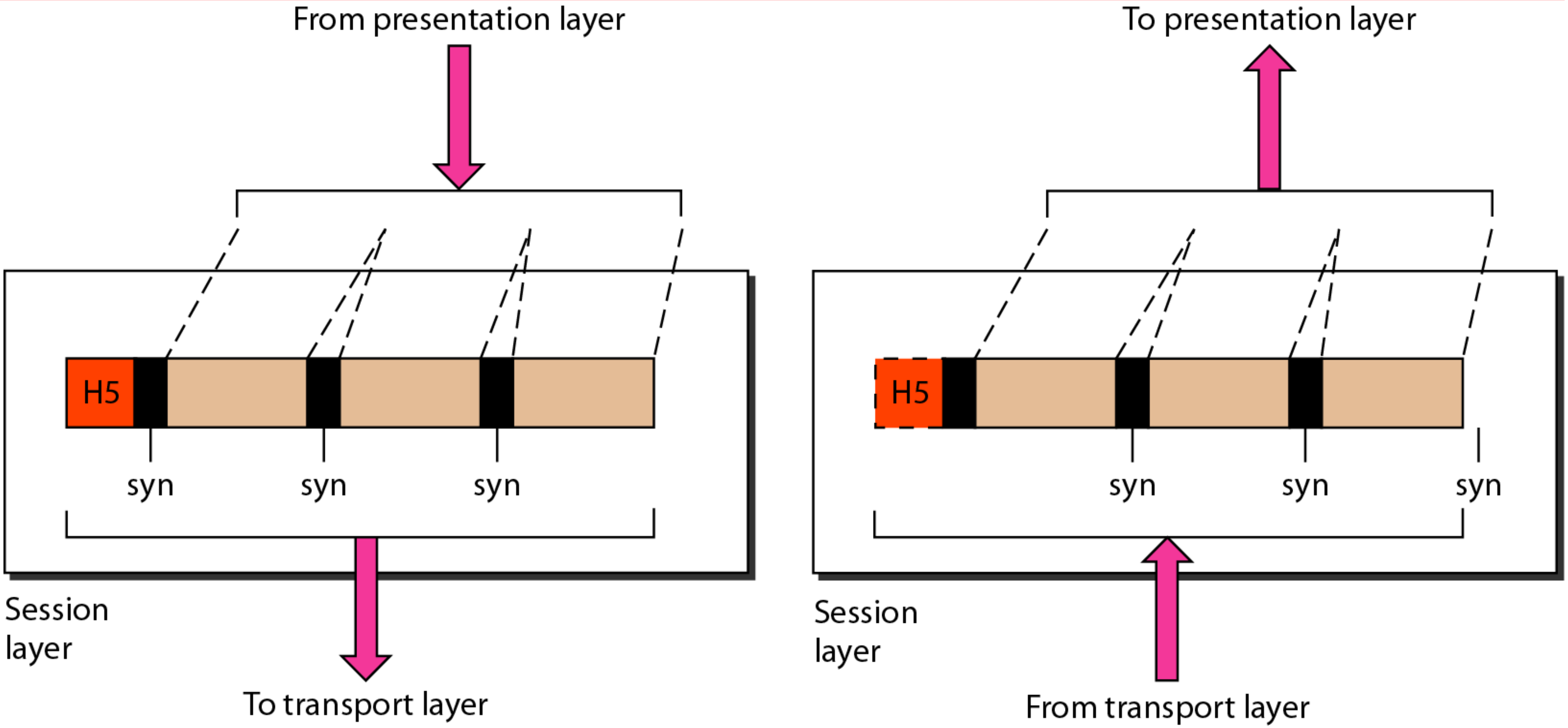
Transport Layer Functionality…

- **Flow control:** **flow control at this layer is performed end to end rather than across a single link.**

- **Error control: error control at this layer is performed process-to process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.**

- **Connection control: The transport layer can be either connectionless or connection-oriented.**

Figure 2.12 *Session layer*



- The session layer is the network *dialog controller*. It establishes, maintains, and Synchronizes the interaction among communicating systems.

The session layer is responsible for dialog control and synchronization.

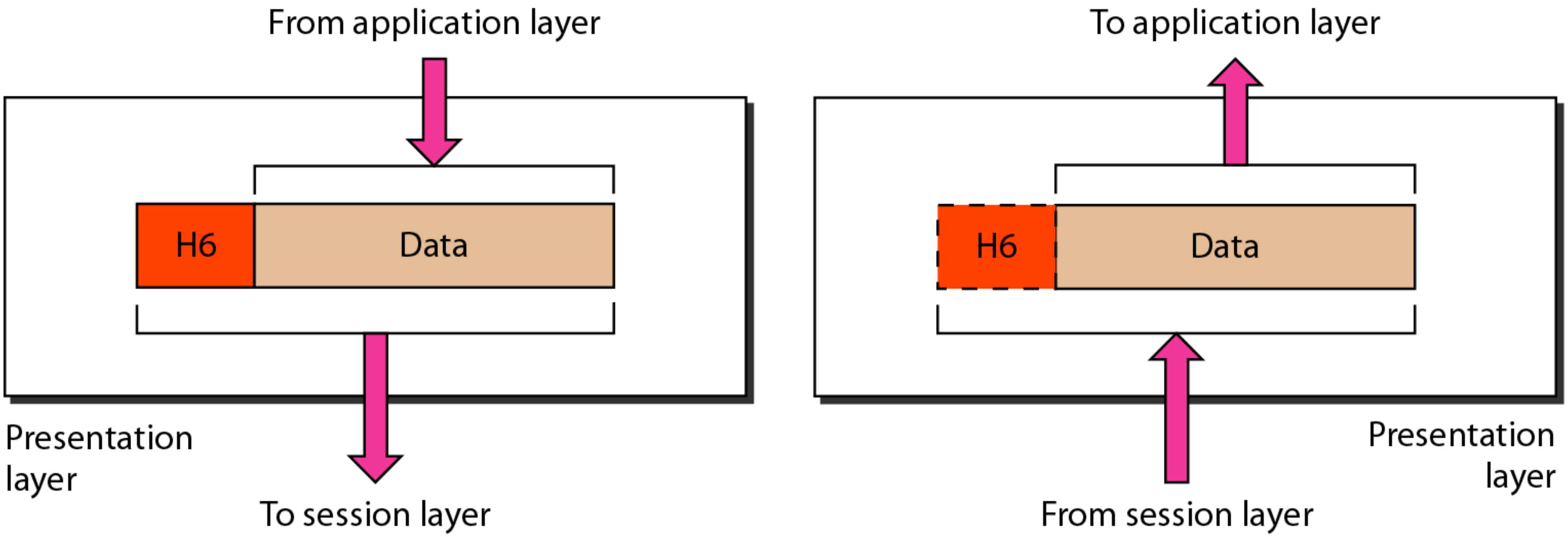
Session Layer Functionality

- **Dialog control: The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half-duplex or full-duplex mode.**

- **Synchronization. The session layer allows a process to add checkpoints, or synchronization points, to a stream of data.**

- ✓ **For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently.**
  In this case, if a crash happens during the transmission of page 425,
  the only pages that need to be resent after system recovery are pages 401 to 425.
  Pages previous to 401 need not be resent.

Figure 2.13 *Presentation layer*



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

Presentation Layer Functionality

- **Translation**:

✓ The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers etc.

✓ The information must be changed to bit streams before being transmitted.

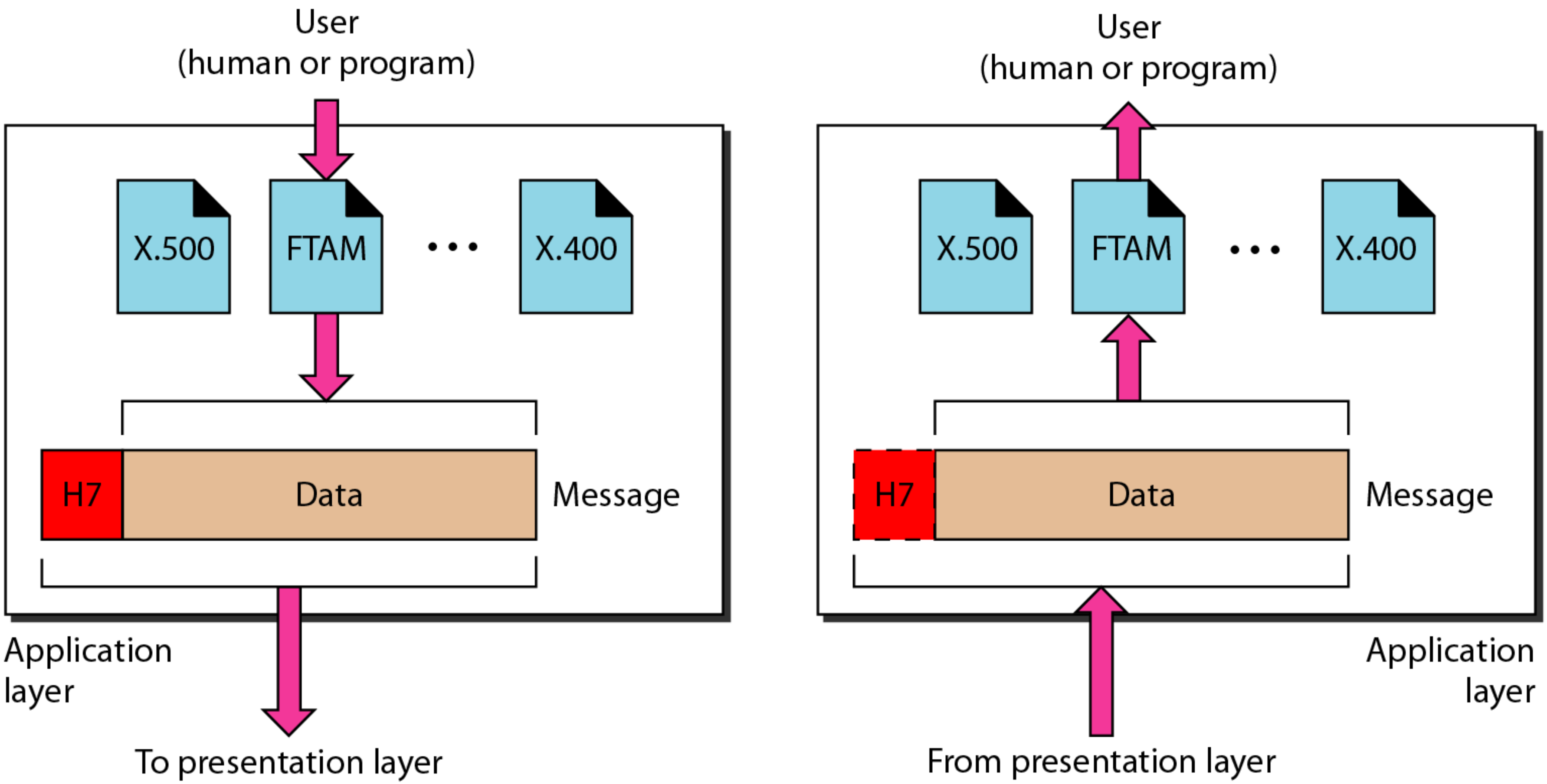
System A using ASCII - > Presentation layer at A ->Common format-> Presentation layer at B->System using UNICODE

Presentation Layer…

- **Encryption**:
  - To ensure privacy.
  - Sender transforms the original information to another form and sends the resulting message out over the network.
  - Decryption reverses the original process to transform the message back to its original form.

- **Compression**:
  - Data compression reduces the number of bits contained in the information.
  - Important in the transmission of multimedia such as text, audio, and video.

Figure 2.14 *Application layer*



❑ **The application layer enables the user, whether human or software, to access the network.**

Application Layer Functionality

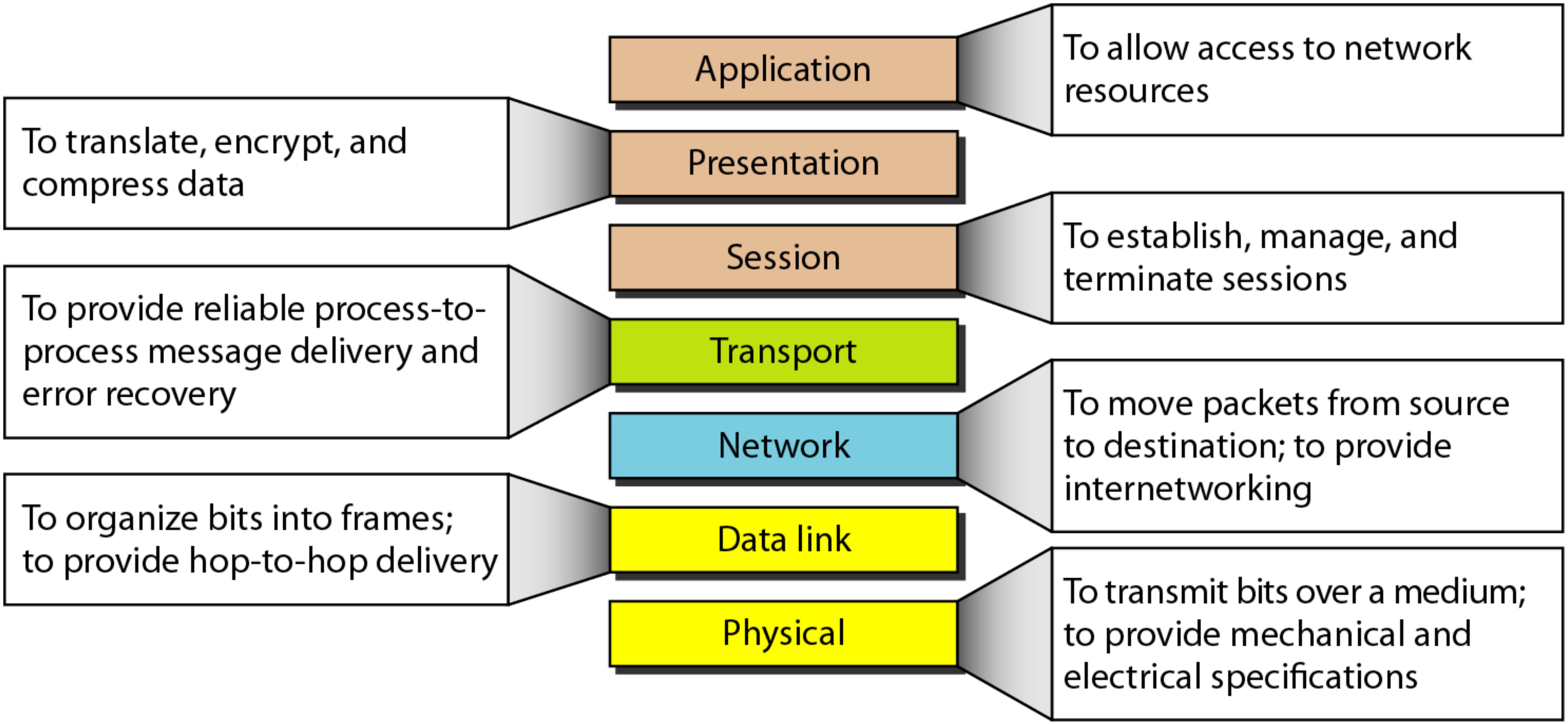
- **Network virtual terminal**: A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.

- **File transfer, access, and management**: 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.

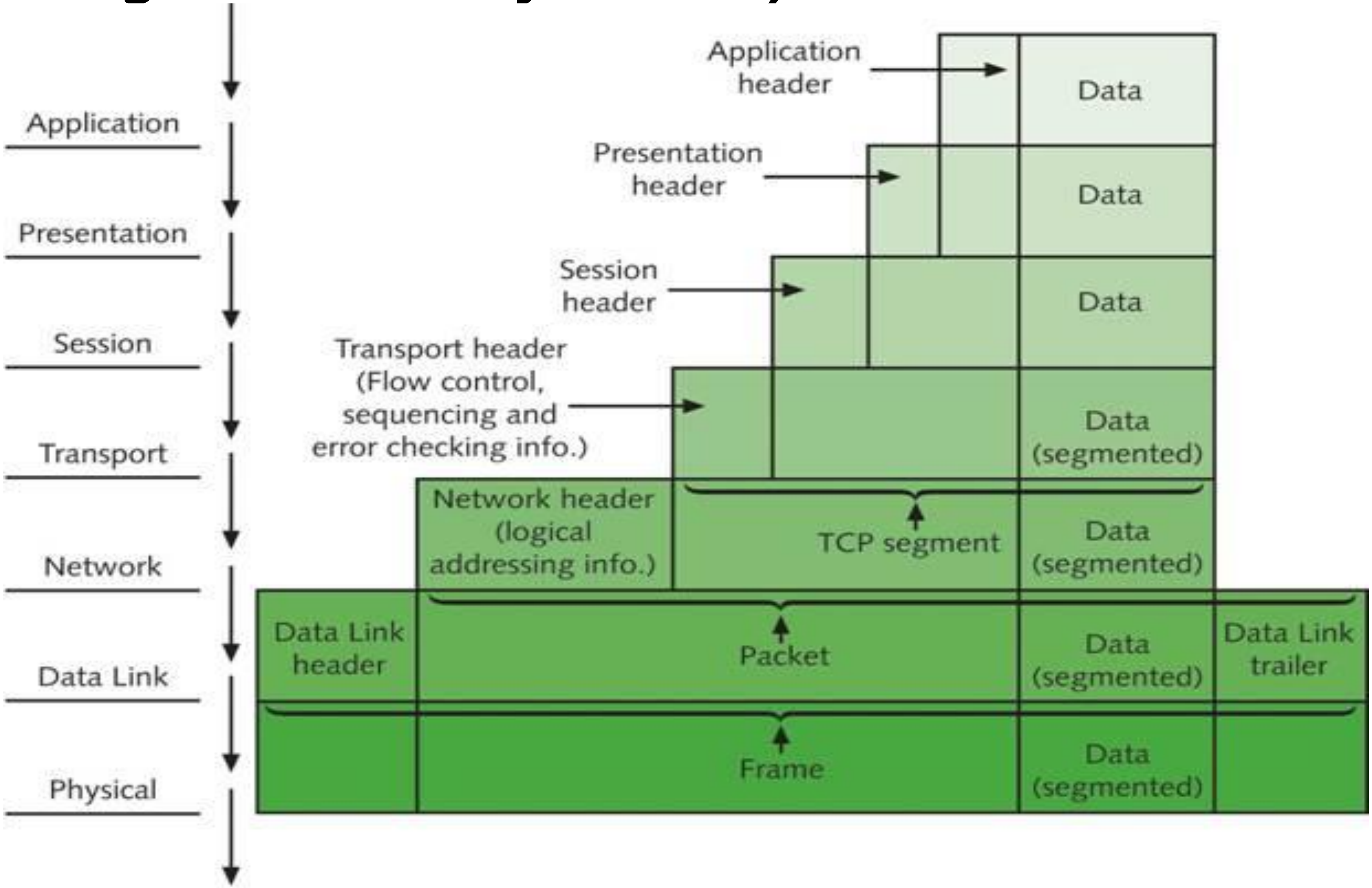
Figure 2.15 *Summary of layers*



OSI Layers, functions and example standards

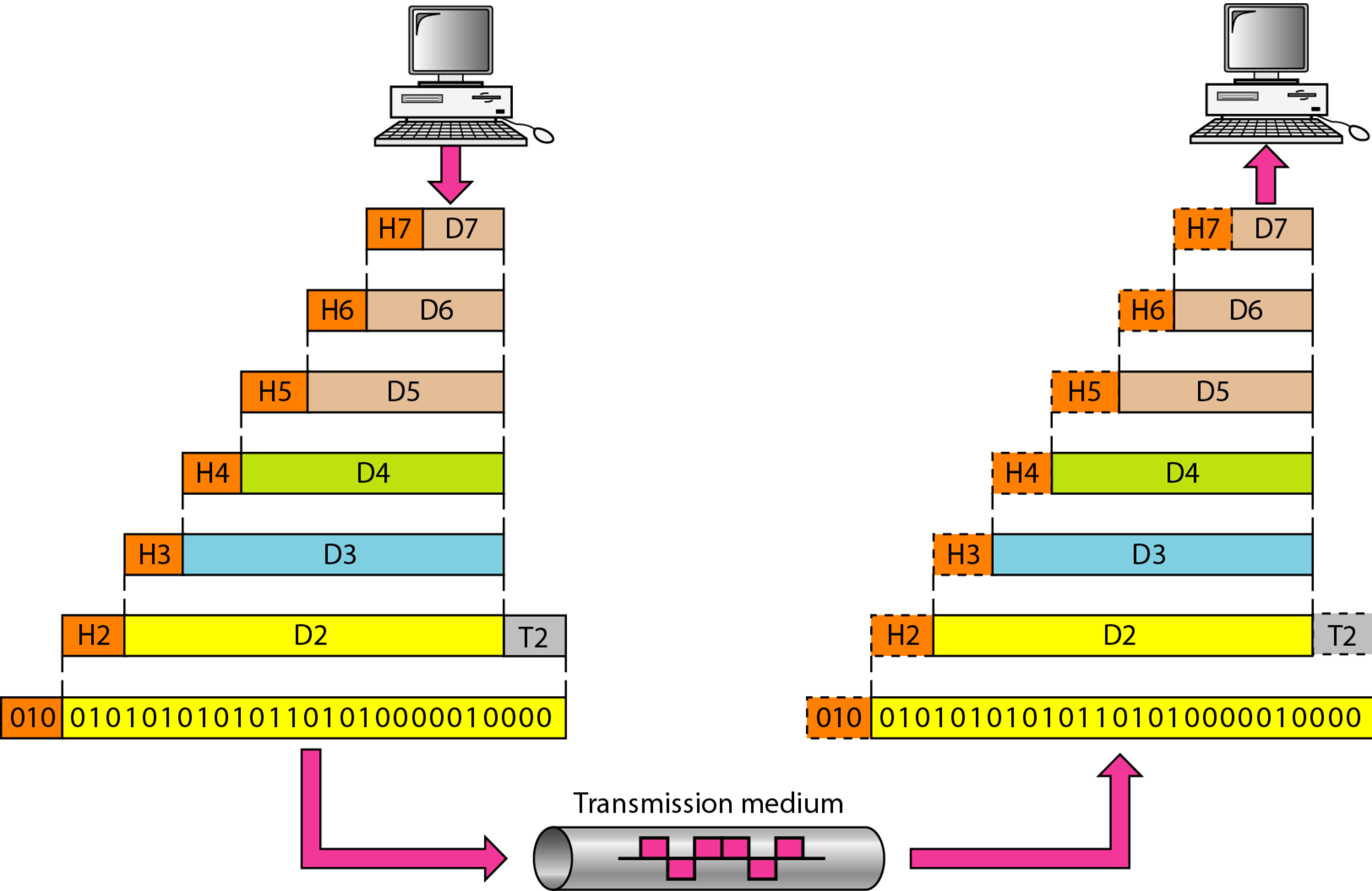
Layer	Name	Location	PDU	Function	Examples
1	Physical	Media	Symbol	Communication over physical medium	Ethernet, FDDI, B8ZS, V.35, V.24, RJ45
2	Data link	Media	Frame	Reliability of communication over physical medium	IEEE 802.5/ 802.2, IEEE 802.3/802.2, PPP, HDLC, Frame Relay, ATM, FDDI
3	Network	Media	Packet	Structuring of data and routing between multiple nodes	DDP, IP, AppleTalk, IPX
4	Transport	Host	Segment	Reliability of communication over networks or between hosts	SPX, TCP, UDP
5	Session	Host	Data	Establishment, management, and termination of remote sessions	NetBios names, NFS, RPC, SQL
6	Presentation	Host	Data	Syntactic conversion of data and encryption	Encryption, ASCII, MIDI, PICT, JPEG, EBCDIC, TIFF, GIF, MPEG
7	Application	Host	Data	User identification, authentication, privacy, and quality of service	SNMP, Telnet, WWW browsers, HTTP, NFS, FTP

Organization of the Layers



At each layer, a header, or possibly a trailer, can be added to the data unit. Commonly, the trailer is added only at layer 2.

Figure 2.4 *An exchange using the OSI model*



Why Layering?

- Layering simplifies design, implementation, and testing by partitioning overall communications process into parts
- Protocol in each layer can be designed separately from those in other layers
- Protocol makes “calls” for services from layer below
- Layering provides flexibility for modifying and evolving protocols and services without having to change layers below
- Functions for each layer is predefined, so debugging becomes easy
- For programming modular languages like C can be used

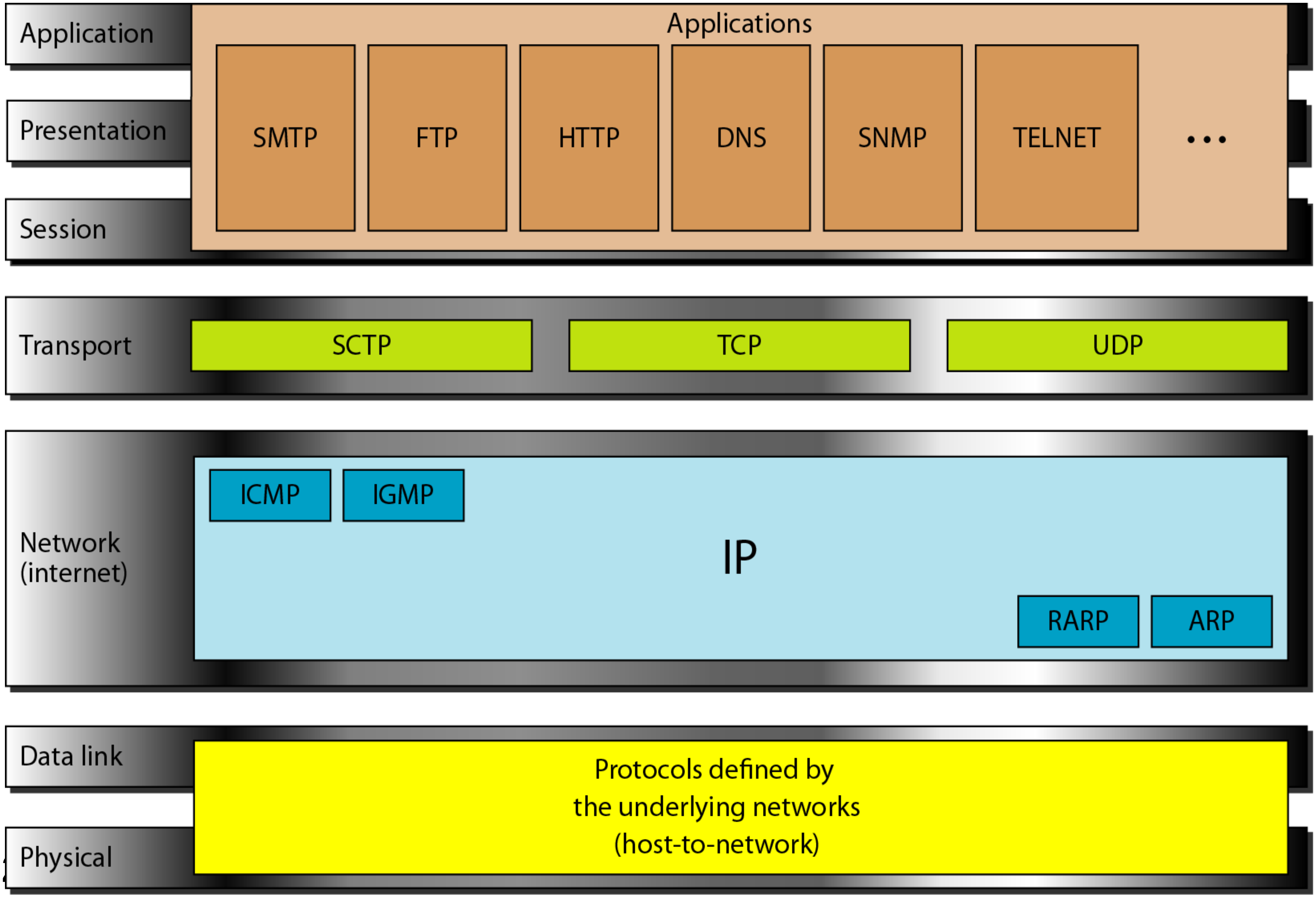
2-4 TCP/IP PROTOCOL SUITE

TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.

First four layer provide physical standards, network interfaces, internetworking and transport functions that corresponds to the first four layer of the OSI model.

The topmost three layers in OSI model are represented in TCP/IP by a single Application Layer.

Figure 2.16 *TCP/IP and OSI model*



Physical and Data Link Layers

- At the physical and data link layers, *TCP/IP* does not define any specific protocol. It supports all the standard and proprietary protocols.
- A network in a *TCP/IP* internetwork can be a local-area network or a wide-area network

- ***Network Layer***
- At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol.
- IP, in turn, uses four supporting protocols: address resolution protocol (ARP) (IP to Ethernet add translation), Internet control message protocol (ICMP), and Internet group management protocol (IGMP).
- Traditionally, this layer was built upon IPv4 (32 bits add), which is gradually shifting to IPv6 (128 bits add.), enabling the accommodation of a much more significant number of addresses and security measures.

Transport Layer

- UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process.
- **SCTP provides support for newer applications such as voice over the Internet.**

Feature	UDP	TCP
Name	User datagram protocol	Transmission control protocol
Type of service	Connectionless	Connection-oriented
Reliability	Low	High
Time-criticality	High	Low
Packet sequencing	No sequencing required	High level of sequencing involved
Speed of transfer	High	Relatively low
Error checking	Present, but it simply discards errorenous packets	Present; Errorenous packets are re-transmitted from the source
Error recovery	Absent	Present
Acknowledgment	Absent	Present; Done by means of ACK frames
Handshake	None	Done by SYN, SYN-ACK, ACK frames
Weight	Lightweight protocol	Heavyweight protocol
Usage	SNMP, TFTP, RIP, VoIP, DNS, DHCP	HTTP, HTTPs, FTP, SMTP, Telnet

Application Layer

- **The *application layer* in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model.**

- **Many protocols are defined at this layer such as TELNET, SNMP, DNS, HTTP, FTP, SMTP**

Sr No	OSI Model	TCP/IP Model
1.	Clearly makes distinction between three central concepts – Services, Interfaces and Protocols	Does not do it
2.	Protocols are better hidden and can be replaced relatively easily as the technology changes.	Protocol changes are not easy.
3.	The OSI reference model was devised before the corresponding protocol were invented. The model was not biased towards one particular set of protocols	In TCP/IP, protocols came first and model was really a description of the existing protocols.
4.	Has 7 Layers	Has 4 Layers
5.	Supports both connectionless and connection oriented communication in the network layer but only connection-oriented communication in the transport layer	It supports only connectionless mode in network layer but both modes in the transport layer

Relationship between Layers

- Two houses, one in Kashmir and the other in Kanyakumari, with each house being home to a dozen kids
- The kids in Kashmir household are cousins of kids in the Kanyakumari households
- Each kid in both household writes a letter to each cousin every week, with each letter delivered by the traditional postal service in a separate envelope
- Thus, each household sends 144 (12 x 12) letters to the other household every week (These kids would save a lot of money if they had e-mail!)

Relationship between Layers

- In each of the households there is one kid -- Jay in Kashmir house and Veeru in the Kanyakumari house responsible for mail collection and mail distribution
- Each week Jay visits all his brothers and sisters, collects the mail, and gives the mail to a postal-service mail person who makes daily visits to the house
- When letters arrive to Kanyakumari house, Veeru also has the job of distributing the mail to his brothers and sisters.
- Jay has a similar job in Kashmir

Relationship between Layers

- Postal service moves mail from house to house, not from person to person.
- Jay and Veeru provide logical communication between the cousins – they pick up mail from and deliver mail to, their brothers and sisters.
- From the cousins' perspective, they *are the mail service, even* though they are only a part (the end system part) of the end-to-end delivery process.
- This household example is an analogy for explaining how the transport layer relates to the network layer

Analogy

- *hosts, End systems = houses*
- *processes = cousins*
- *application messages = letters in envelope*
- *network layer protocol = postal service (including mail persons)*
- *transport layer protocol = Jay and Veeru*
- *Physical layer protocol = postal vans*

Analogy Contd.

- Jay and Veeru (Transport protocols) do all their work within their respective homes (hosts)
- They are not involved, in sorting mail in any intermediate mail center or in moving mail from a mail center to another
- Within hosts, transport protocol moves messages from application processes to the network edge (i.e., the network layer) and vice versa
- It doesn't have any say about how the messages are moved within the network core

Analogy Contd.

- Suppose that Jay and Veeru go on vacation
- another cousin pair -- say, Sonu and Monu -- substitute for them and do same services
- Unfortunately , they do not do the collection and delivery in same way as Jay and Veeru
- Being younger kids, Sonu and Monu occasionally lose letters (which are sometimes chewed up by the family dog).

Analogy Contd.

- Thus, the cousin-pair Sonu and Monu do not provide the same set of services (i.e., the same service model) as their brothers
- Similarly a computer network may make available multiple transport protocols, with each protocol offering a different service model to applications (UDP, TCP)

Analogy Contd.

- Possible services that Jay and Veeru (Transport layer protocol) can provide are constrained by the possible services that the postal service (Network layer protocol) provides
- Eg. If postal service (network layer protocol) doesn't provide a max. bound on how long (Delay, BW) it can take to deliver mail between the two houses (end systems)
- Then there is no way that Jay and Veeru (transport layer protocol) can guarantee a maximum delay for mail delivery between any of the cousin pairs (processes)

Figure 2.17 *Addresses in TCP/IP*

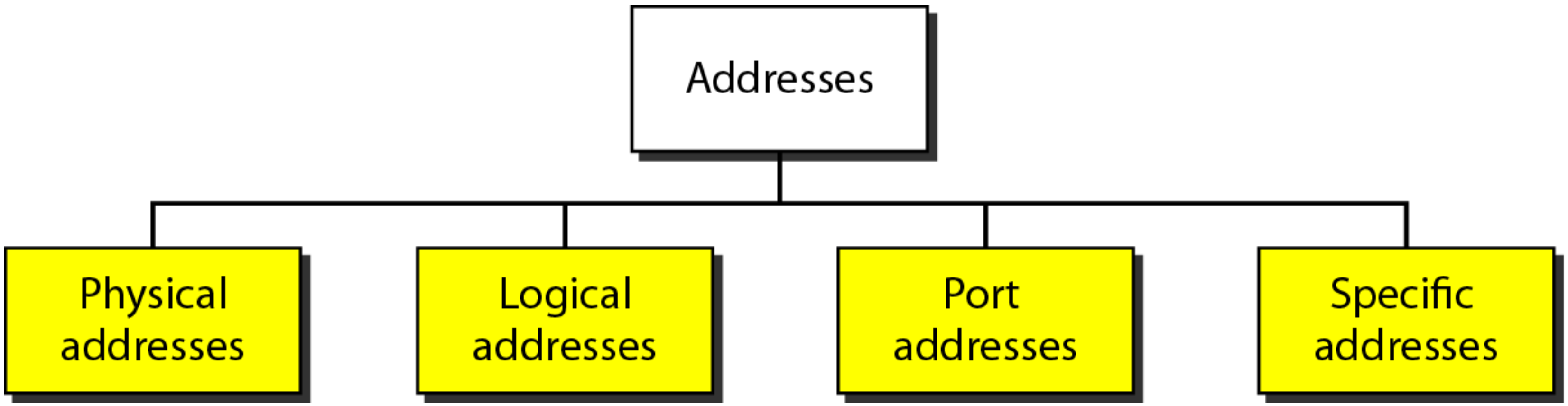
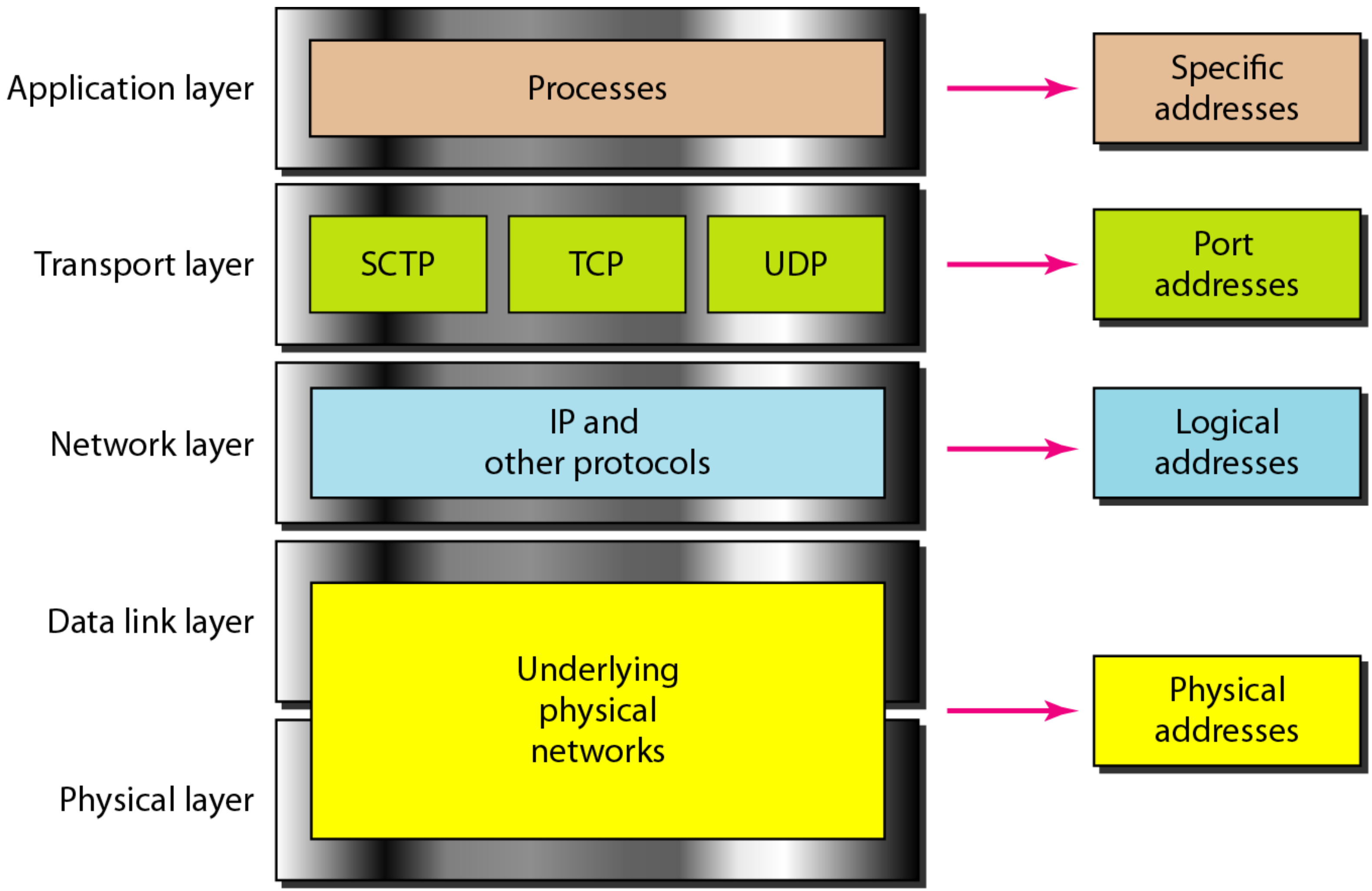


Figure 2.18 *Relationship of layers and addresses in TCP/IP*

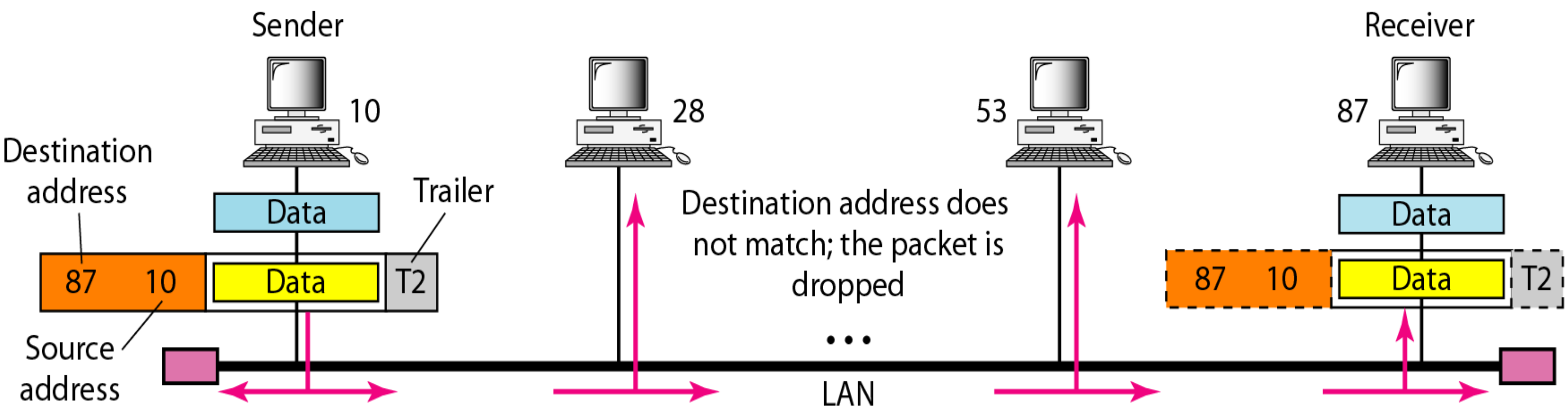


Physical Address

- Also known as link/MAC/Data Link Layer Addresses, is address of a node as defined by its LAN
- It is the lowest-level address.
- Size and format of these addresses vary depending on the network
- Ethernet uses a 6-byte (48-bit) physical address imprinted on network interface controller (NIC)
  - 07:01:02:01 :2C:4B-A 6-byte (12 hexadecimal digits) physical address
  - first 24 bits are organizational identifiers
  - last 24 bits are NIC identifiers

These addresses are unique globally.

Example 2.1



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).

Logical Addresses

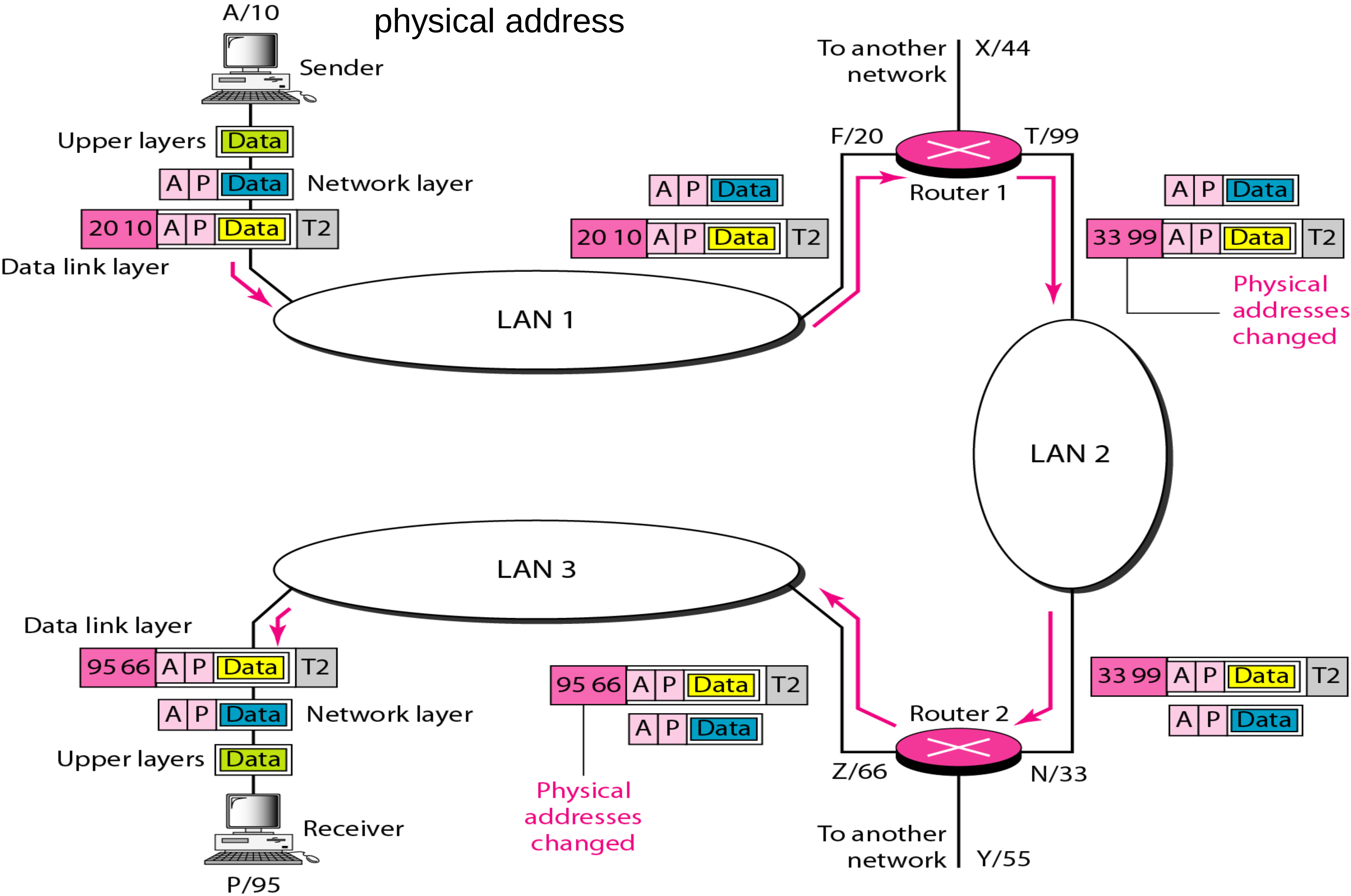
- Network layer addressing/ IP-based addressing
- Necessary for universal communications that are independent of underlying physical networks.
- Physical addresses are not adequate in an internetwork environment where different networks can have different address formats.
- A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network.
- No two publicly addressed and visible hosts on the Internet can have the same IP address.
- Traditionally, IP addresses were IPv4 (32 bits add), which is gradually shifting to IPv6 (128 bits add.), enabling the accommodation of more significant number of addresses

Note

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

IP addresses

A=Sender - logical address
P=Receiver - logical address
physical address



Port Addresses

- Nodes can run multiple processes at the same time
- For these processes to receive data simultaneously, labelling of the different processes is required
- In other words, they need addresses.
- A port address in TCP-IP is 16 bits in length.

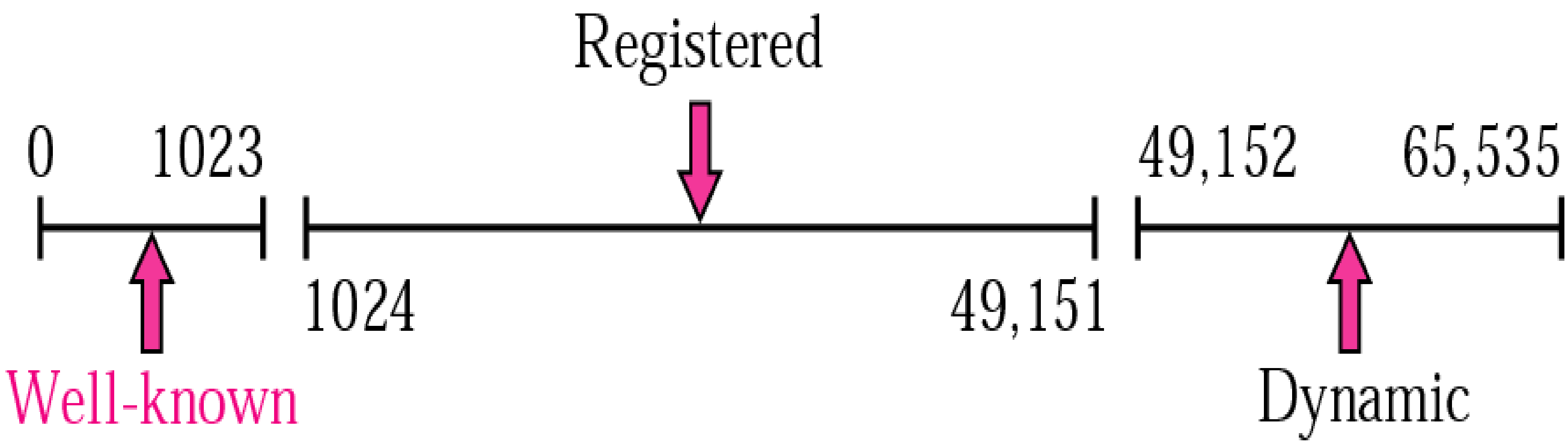
Internet Port Addressing

IANA (Internet Assigned Number Authority) has divided the port numbers

Well known – for server with some exceptions

Registered – to be registered with IANA to prevent duplication

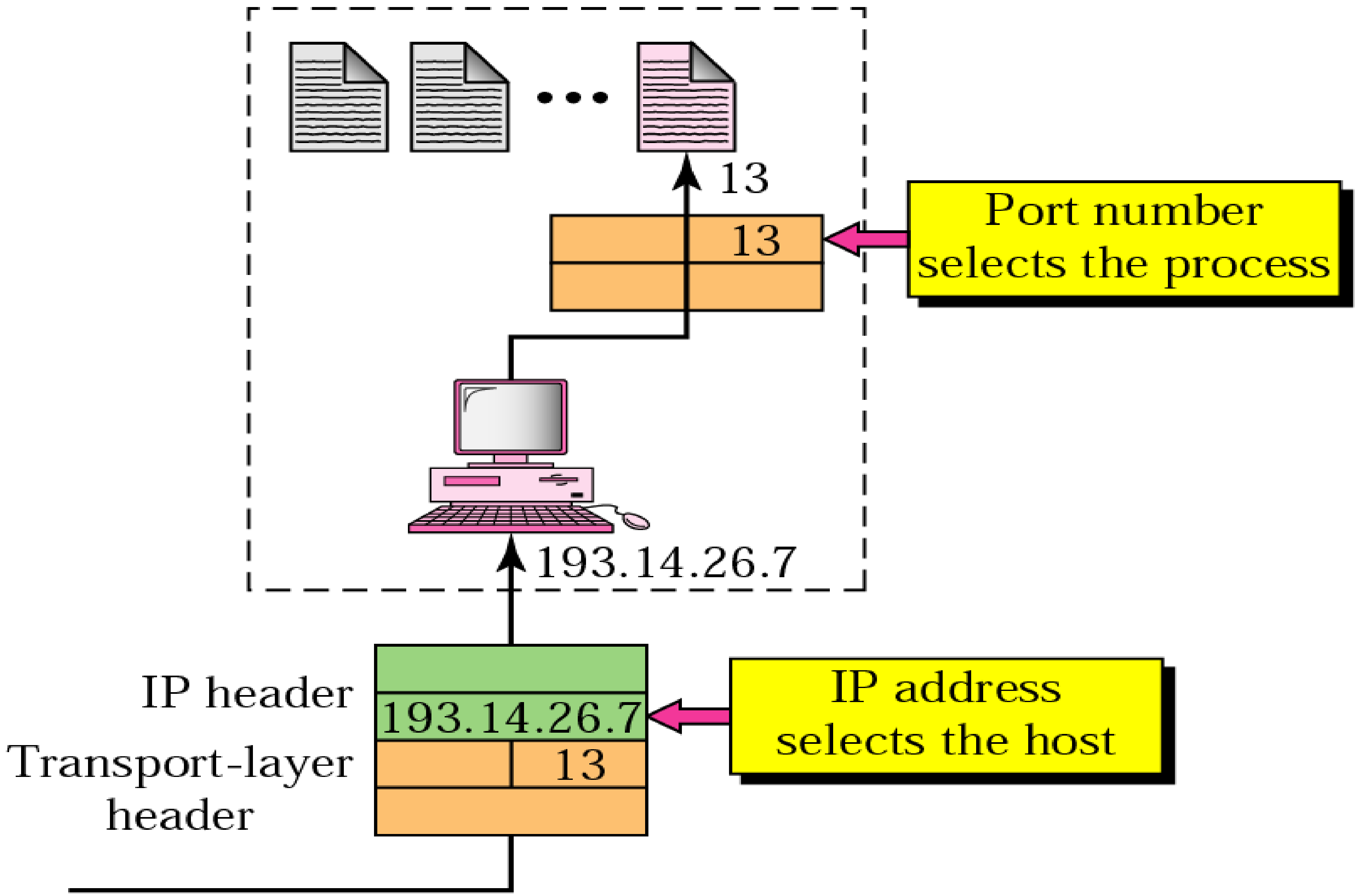
Dynamic – ephemeral, used by any process



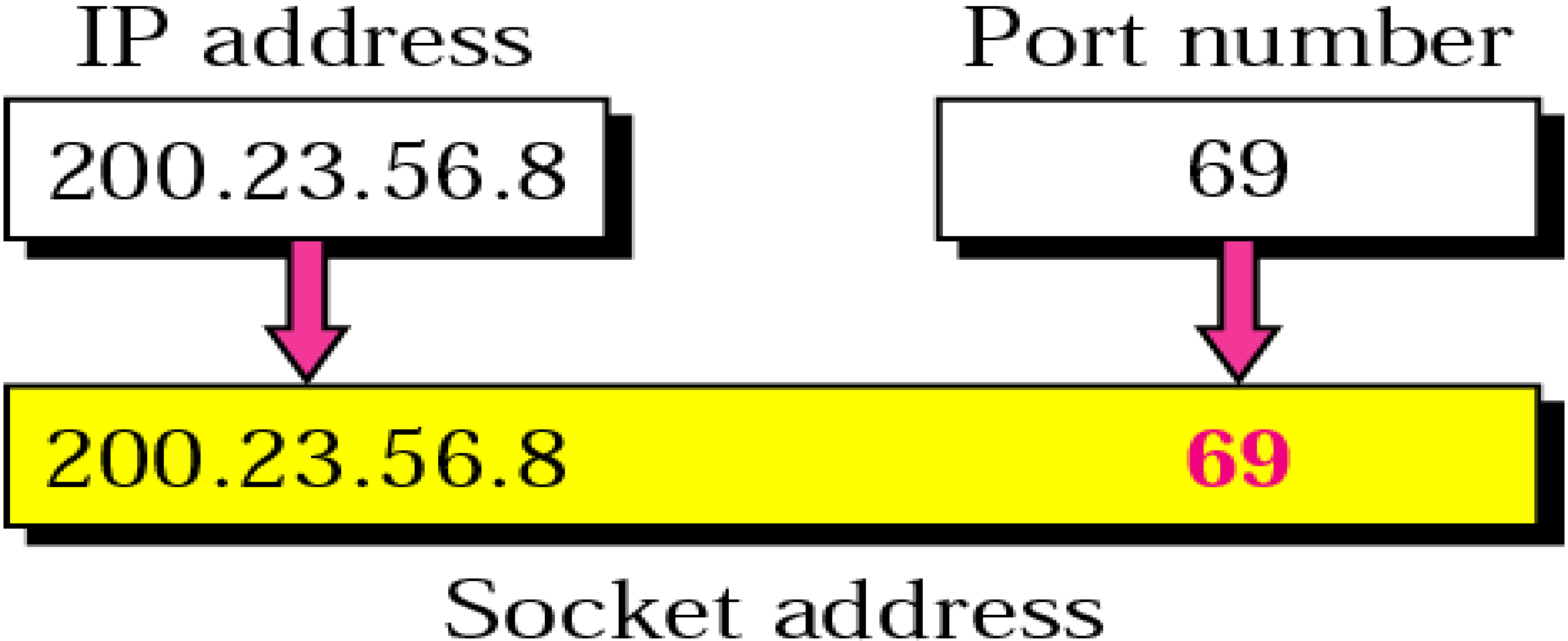
Well known Ports

Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FTP, Data	File Transfer Protocol (data connection)
21	FTP, Control	File Transfer Protocol (control connection)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

IP Address vs Port Address



Socket Addresses



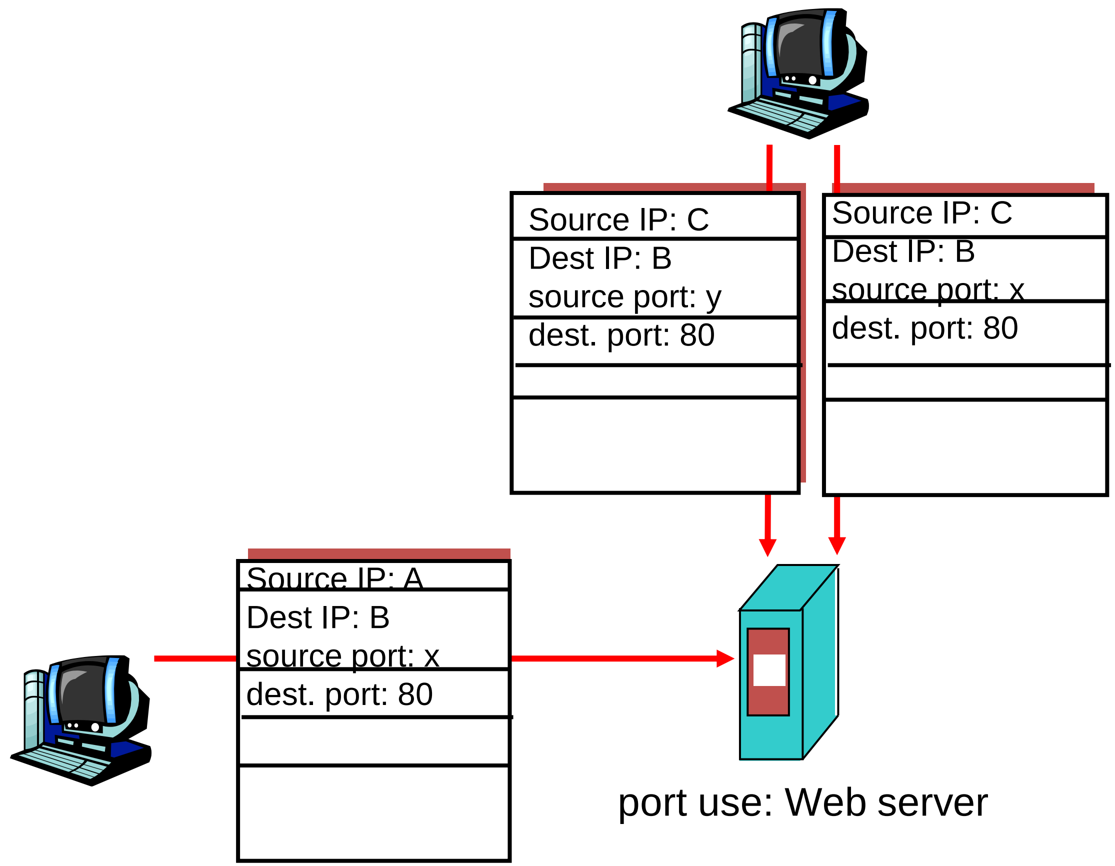
Client/Server Paradigm

- Server - more computational capability, more memory, wall powered, gives services
- Client – less computational capability, less memory, battery operated, asks for services
- Process on local host, client, needs services from a process on remote host, server
- Both processes (client, server) have same name
- To get the day and time from a remote machine, we need a Daytime client/ Daytime server process

Multiplexing/Demultiplexing

A: 10.1.19.22
B: 10.1.19.23
C: 10.1.19.24

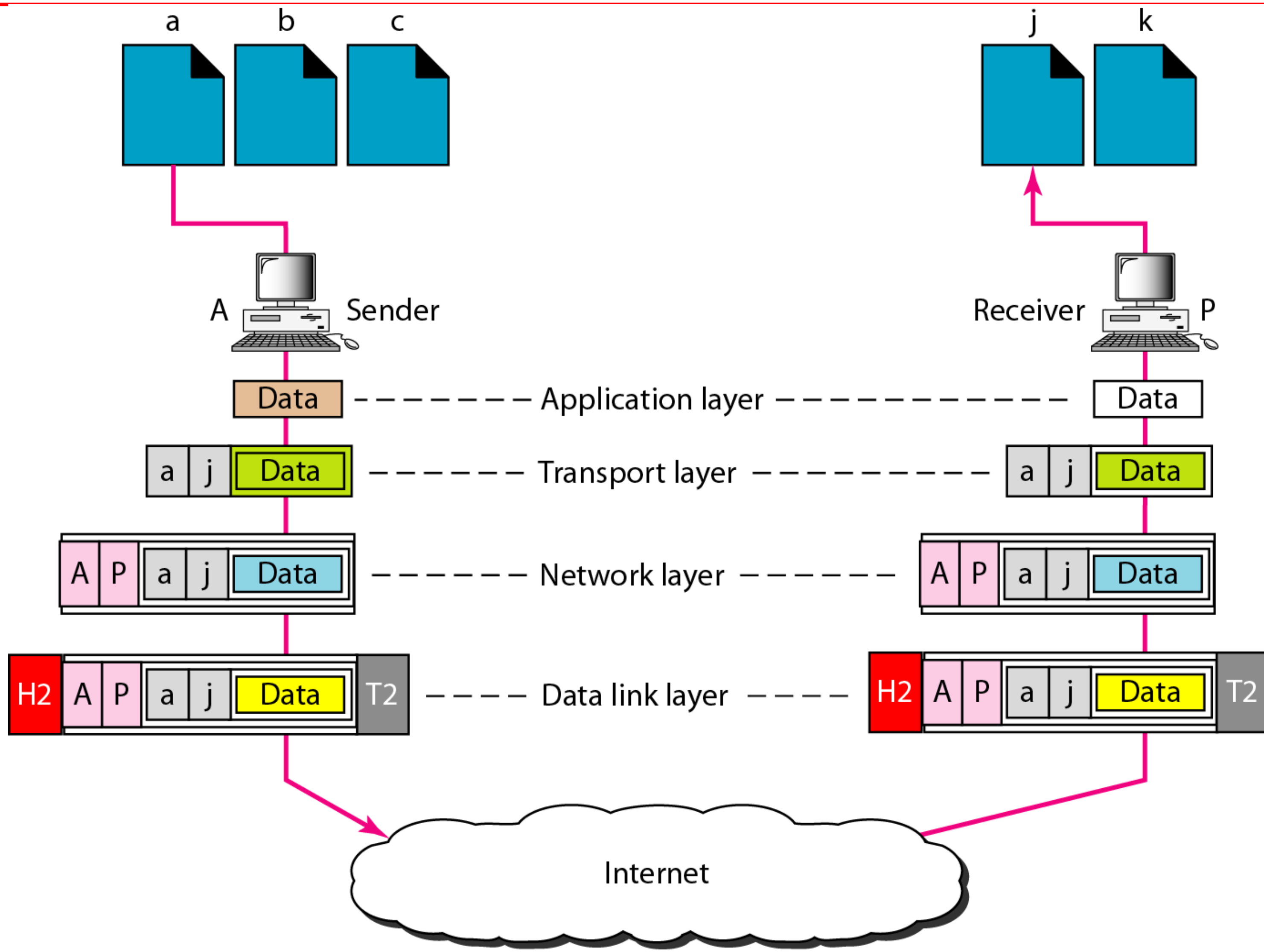
x,y = anything between
49,152 to 65,535



Specific Addresses

- Some applications have user-friendly addresses that are designed for that specific address
  - Universal Resource Locator (URL) *www.mhhe.com*
  - Email address

Figure 2.21 *Port addresses*



Thank You!