Protocols

Communication between two people or two devices needs to follow some protocol. A **protocol is a set of rules that governs communication**.

- For example, in a face-to-face communication between two persons, there is a set of implicit rules in each culture that define how two persons should start the communication, how to continue the communication, and how to end the communication.

- A protocol defines what is communicated, how it is communicated and when it is communicated. The key elements of a protocol are **syntax, semantics, and timing**.

Syntax. Syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

Semantics. Semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?

Timing. Timing refers to two characteristics: when data should be sent and how fast it can be sent. For example, if a sender produces data at 100 megabits per second (100 Mbps) but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and data will be largely lost.

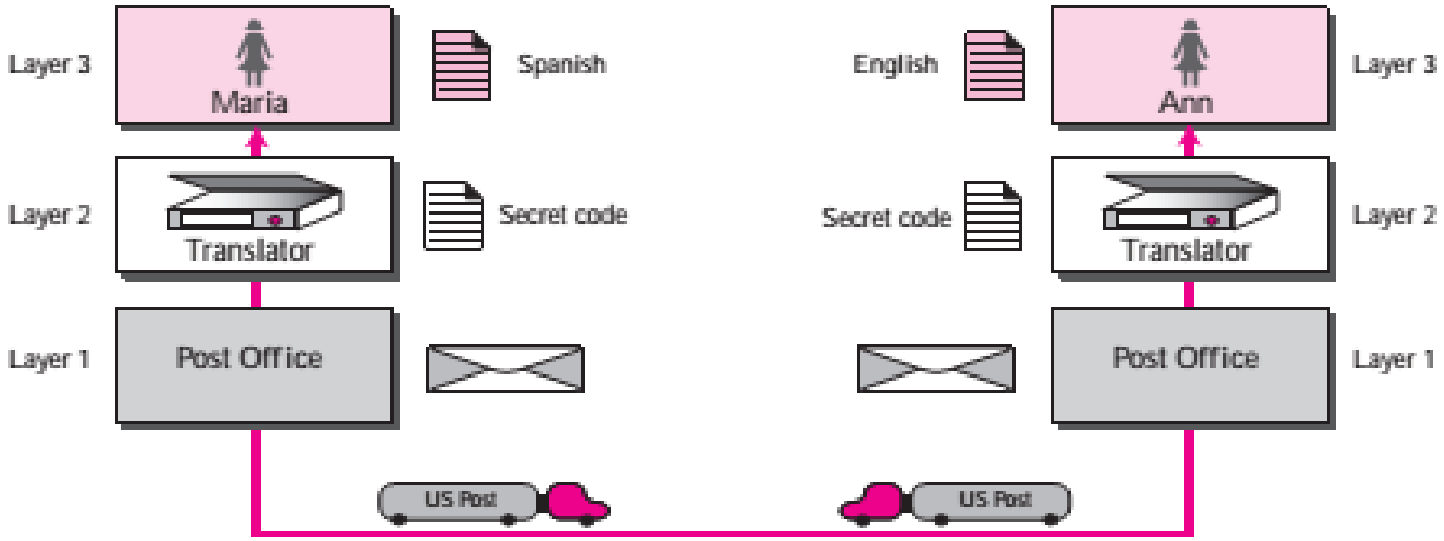
The OSI Model and TCP/IP Protocol Suite

CONTENTS

- THE OSI MODEL
- LAYERS IN THE OSI MODEL
- TCP/IP PROTOCOL SUITE
- ADDRESSING
- TCP/IP VERSIONS

Simple Commuication

Not so Simple



2.1

THE OSI MODEL

- An open system is a set of protocols that allows any 2 different systems to communicate regardless of their underlying architecture.

Note

ISO is the organization.
OSI is the model.

Figure 2-1

OSI Model

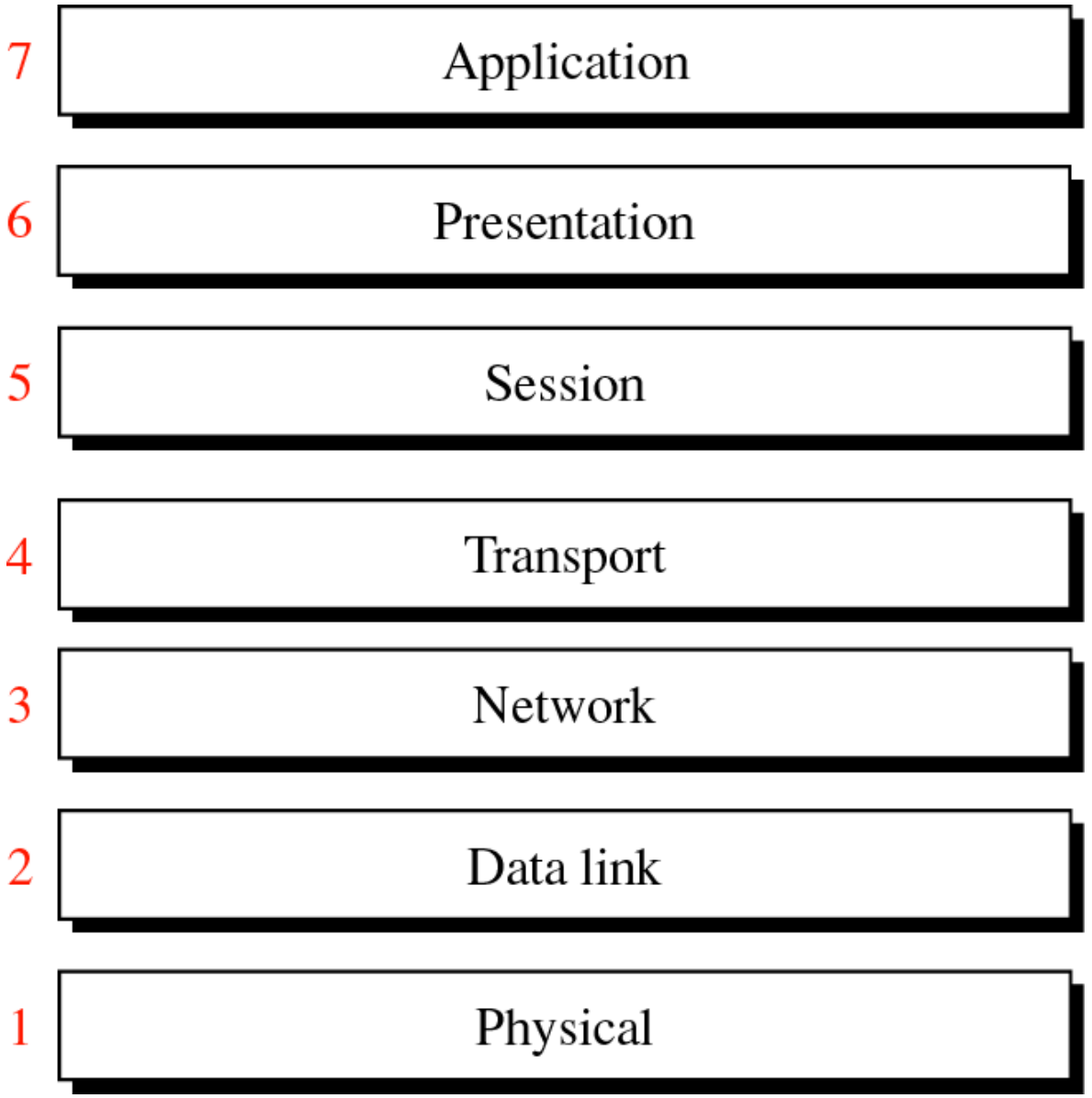
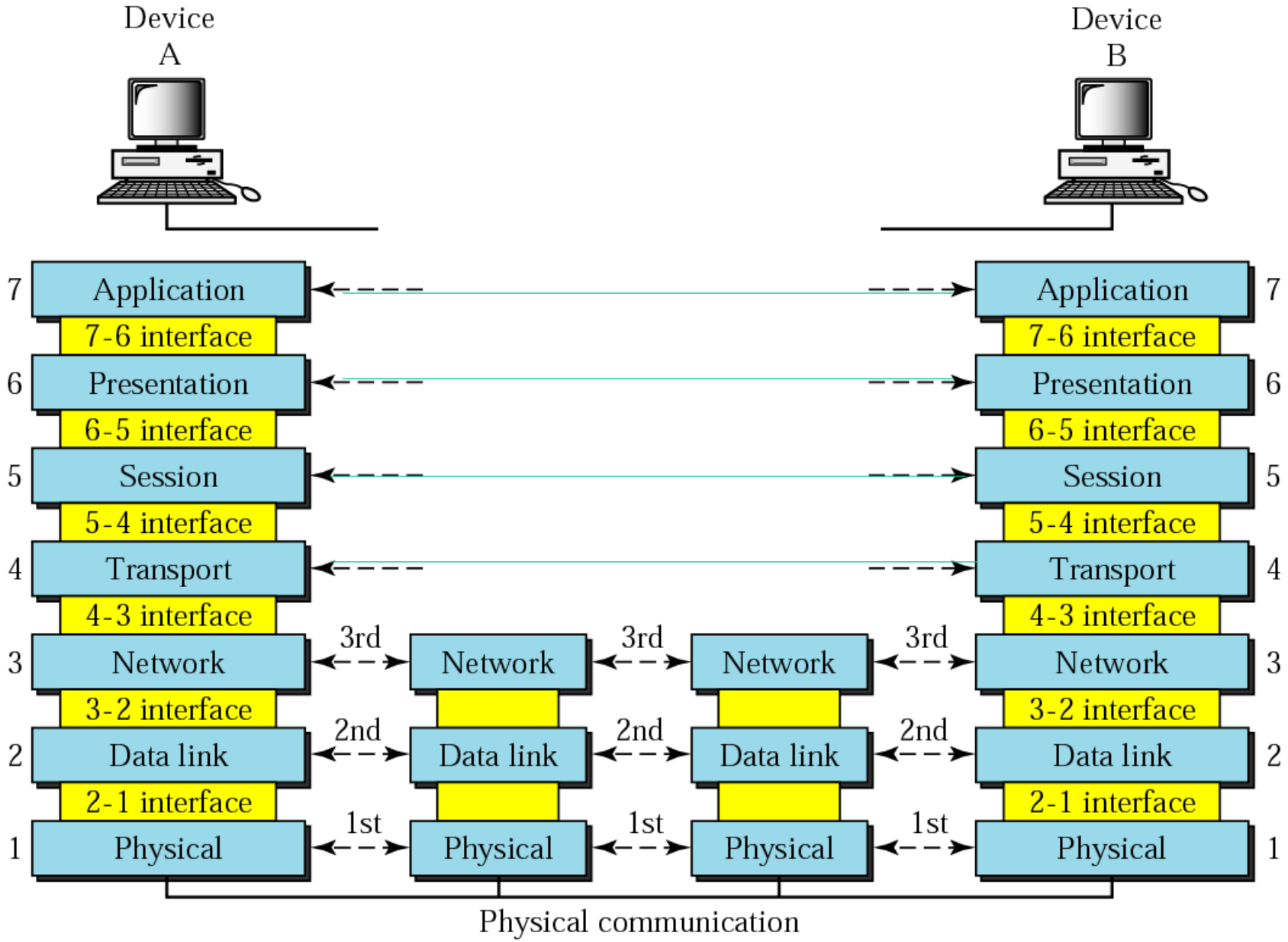


Figure 2-2

OSI layers



- Each layer defines a family of functions distinct from those of the other layers.
- Each layer calls upon the services of the layer just below it.

Layer 2 → layer3 → layer4

Organization of the Layers

- Three subgroups
- Layers 1, 2, and 3
- Network support layers
- Deal with the physical aspects of moving data from one device to another
- Electrical specifications, physical connections, physical addressing, and transport timing and reliability

- Layers 5, 6, and 7
  -User support layers.
  -Allow interoperability among unrelated software systems.
- Layer 4
  - Links the two subgroups
  - Ensures that what the lower layers have transmitted in a form that the upper layers can use

Encapsulation and De-encapsulation

- Each layer adds information to the original data – Encapsulation

- *protocol data unit (PDU)*

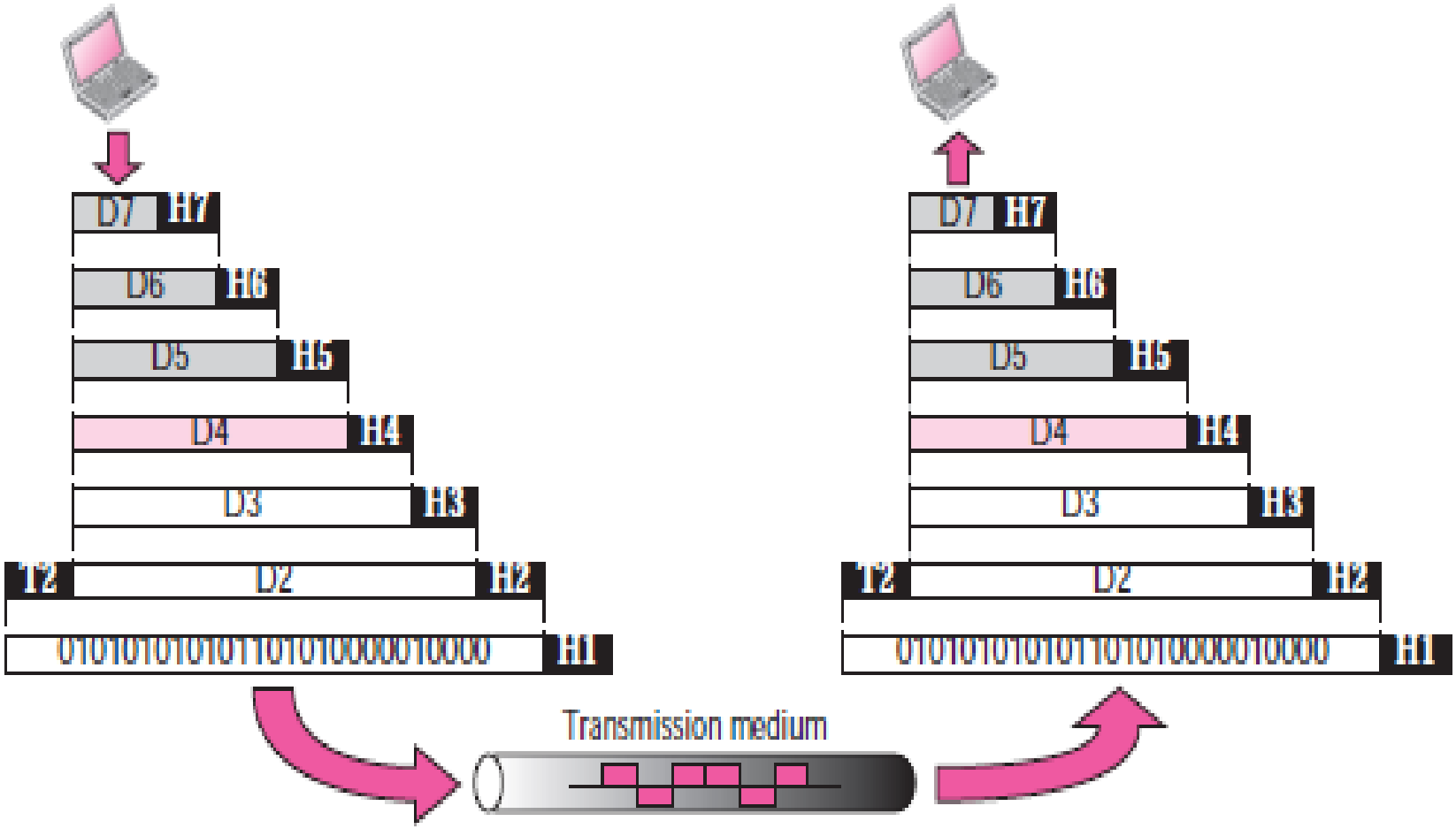
PDU Term	OSI Reference Model Layer
Data	Application, presentation, and session layers
Segment	Transport layer
Packet	Network layer (TCP/IP calls this a *datagram*)
Frame	Data link layer
Bits	Physical layer

- To physical layer - Once the physical layer is reached, the bits of the data link layer frame are converted into a physical layer signal—a voltage, light source, radio wave

- **De-encapsulation-** stripping off the headers and trailers of the PDU

Figure 2-3

An exchange using the OSI model



2.2 LAYERS IN THE OSI MODEL

Physical Layer

- Coordinates the functions required to carry a bit stream over a physical medium.
- Deals with Mechanical and electrical specifications of the interface and transmission media.
- Also defines procedures and functions that physical devices and interfaces have to perform for transmission to occur.

Physical layer is concerned with the foll:

- Physical characteristics of interfaces and media.
- Representation of bits. - encoding (how 0s and 1s are changed to signals).
- Data rate.
- Synchronization of bits
- Line configuration.- P2P, Multipoint

- Physical topology.
- Transmission mode

- **Physical characteristics of interfaces and media.** The physical layer defines the characteristics of the interface between the devices and the transmission media. It also defines the type of transmission media
- **Representation of bits.** The physical layer data consists of a stream of **bits** (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals—electrical or optical. The physical layer defines the type of **encoding** (how 0s and 1s are changed to signals).
- **Data rate.** The **transmission rate**—the number of bits sent each second—is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.
- **Synchronization of bits.** The sender and receiver must not only use the same bit rate but must also be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.
- **Line configuration.** The physical layer is concerned with the connection of devices to the media. In a **point-to-point configuration**, two devices are connected together through a dedicated link. In a **multipoint configuration**, a link is shared between several devices.
- **Physical topology.** The physical topology defines how devices are connected to make a network. Devices can be connected using a **mesh topology** (every device connected to every other device), a **star topology** (devices are connected through a central device), a **ring topology** (each device is connected to the next, forming a ring), or a **bus topology** (every device on a common link).
- **Transmission mode.** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In the **simplex mode**, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the **half-duplex mode**, two devices can send and receive, but not at the same time. In a **full-duplex** (or simply duplex) **mode**, two devices can send and receive at the same time.

Data Link Layer

- Transforms the physical layer, a raw transmission facility, to a reliable link.
- Makes the physical layer appear error-free to the upper layer.

Other responsibilities:

- Framing.
- Physical addressing.
- Flow control.
- Error control.
- Access control.

- **Framing.** The data link layer 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 data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the connecting device that connects the network to the next one.

- **Flow control.** If the rate at which the data is absorbed by the receiver is less than the rate produced at 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. It also uses a mechanism to recognize duplicate 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.

Note:

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

Network Layer

- Source-to-destination delivery of a packet across networks.
- Logical addressing.
- Routing.

- **Logical addressing.** The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
- **Routing.** When independent networks or links are connected together to create **internetworks** (network of networks) or a large network, the connecting devices (called *routers* or *switches*) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

Transport Layer

- The transport layer is responsible for process-to-process delivery of the entire message.
- Service-point addressing (port addressing).
- Segmentation and reassembly – sequence numbers
- Connection control.- Connection Oriented & connectionless
- Flow control.
- Error control.

Transport Layer

The **transport layer** is responsible for **process-to-process delivery** of the entire message. A process is an application program running on the host. Whereas the network layer oversees **source-to-destination delivery** of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

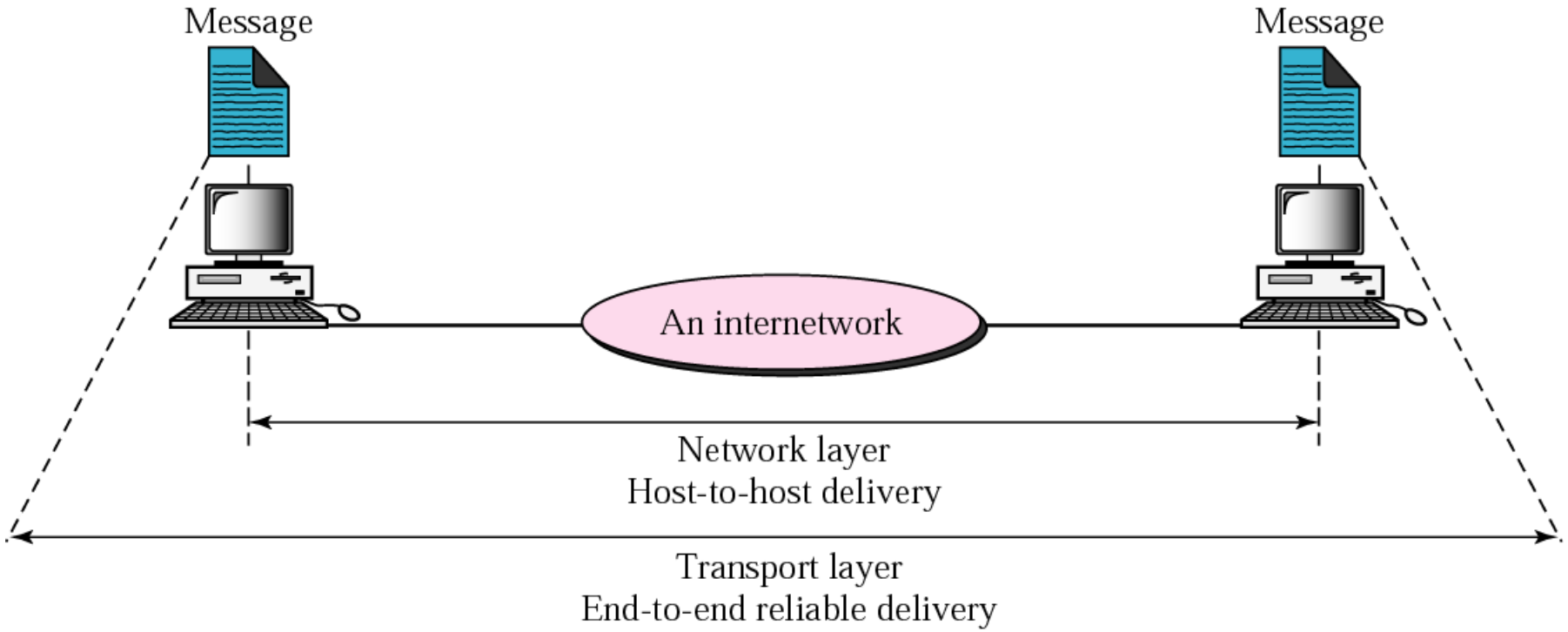
Service-point addressing. Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. 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.
- **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.** Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- **Error control.** Like the data link layer, the transport layer is responsible for error control. However, 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.

Figure 2-10

Reliable end-to-end delivery of a message



Session Layer

- Session layer is the network dialog controller.

  -establishes, maintains, and synchronizes the interaction between communicating systems.

- Dialog control

  - half duplex or full-duplex

- Synchronization.

  Check Points [2000 pages as group of 100]

- **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 (one way at a time) or full-duplex (two ways at a time) mode.

- **Synchronization.** The session layer allows a process to add checkpoints (**synchronization points**) into a stream of data. For example, if a system is sending a file of 2,000 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 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

Presentation Layer

- Concerned with Syntax and semantics of the info exchanged between 2 systems.
-
  - **Translation.** The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information should be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

- **Encryption.** To carry sensitive information a system must be able to assure privacy. Encryption means that the 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. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

Application layer

The **application layer** enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information servic

Application Layer

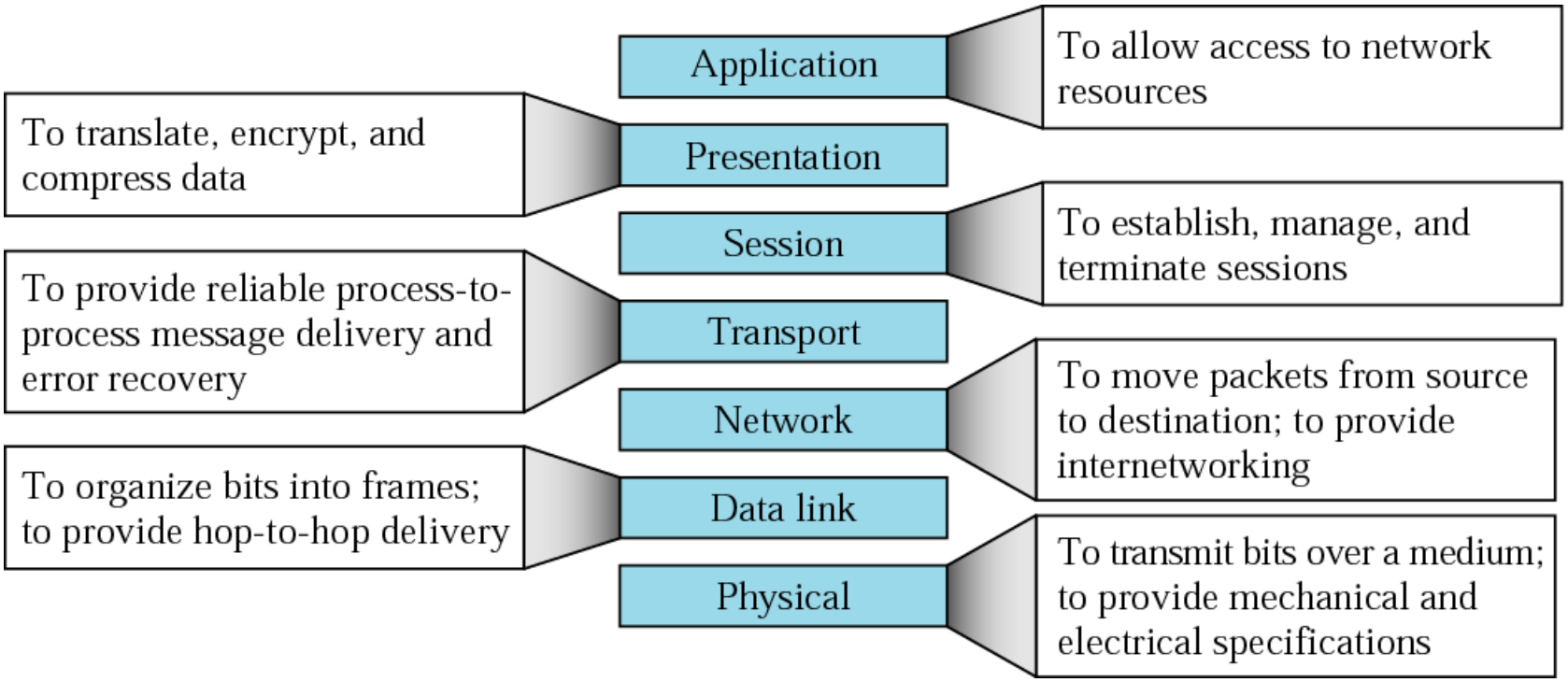
- Network virtual terminal.
- File transfer, access, and management (FTAM).
- E-mail services.
- Directory services.

- **Network virtual terminal.** A network virtual terminal is a software version of a physical terminal and 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 you to log on.
- **File transfer, access, and management (FTAM).** 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

- **E-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 2-14

Summary of layers



BOOTP, DHCP, DNS, FTP, HTTP, HTTPS, IMAP4, PING, POP3, NSLOOKUP, NTP, SFTP, SMTP, Telnet, TFTP	Application Layer Protocols
MIME, SSL, TLS	Presentation Layer Protocols
RTP, SIP	Session Layer Protocols
TCP, UDP	Transport Layer Protocols

ARP, ICMP, IGMP, IP, IPSec, RARP	Network Layer Protocols

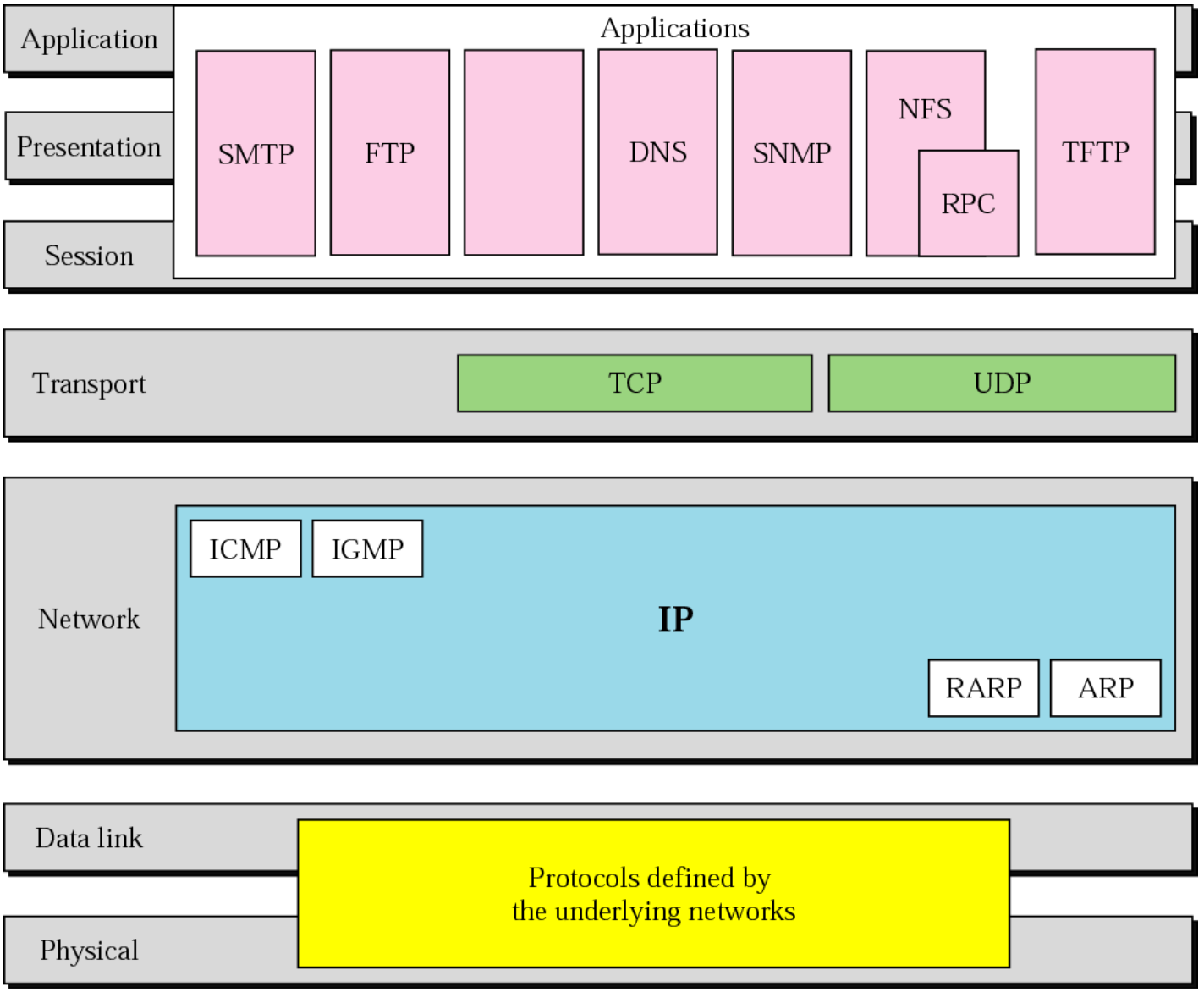
L2TP, PPP, PPTP, SLIP	Data Link Layer Protocols

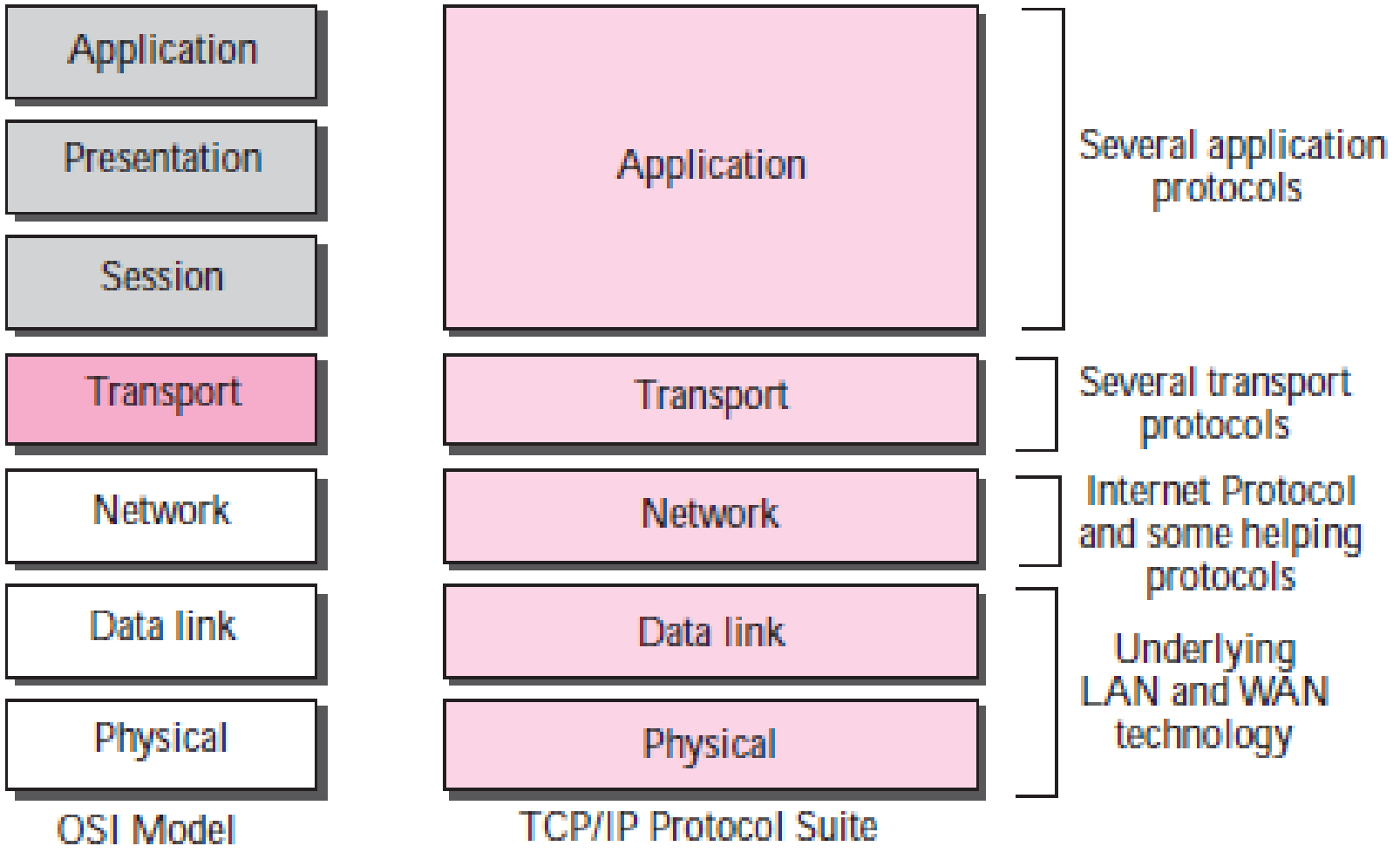
IEEE 802.3 (Ethernet) 802.5 (Token Ring) 802.11 (Wi-Fi)	Physical Layer Protocols

TCP/IP PROTOCOL SUITE

Figure 2-15

TCP/IP and OSI model





Two reasons were mentioned for this decision. First, TCP/IP has more than one transport-layer protocol. Some of the functionalities of the session layer are available in some of the transport layer protocols. Second, the application layer is not only one piece of software. Many applications can be developed at this layer. If some of the functionalities mentioned in the session and presentation are needed for a particular application, it can be included in the development of that piece of software.

TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality, but the modules are not necessarily interdependent. Whereas the OSI model specifies which functions belong to each of its layers, the layers of the TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched, depending on the needs of the system. The term *hierarchical* means that each upper level protocol is supported by one or more lower level protocols.

2.4

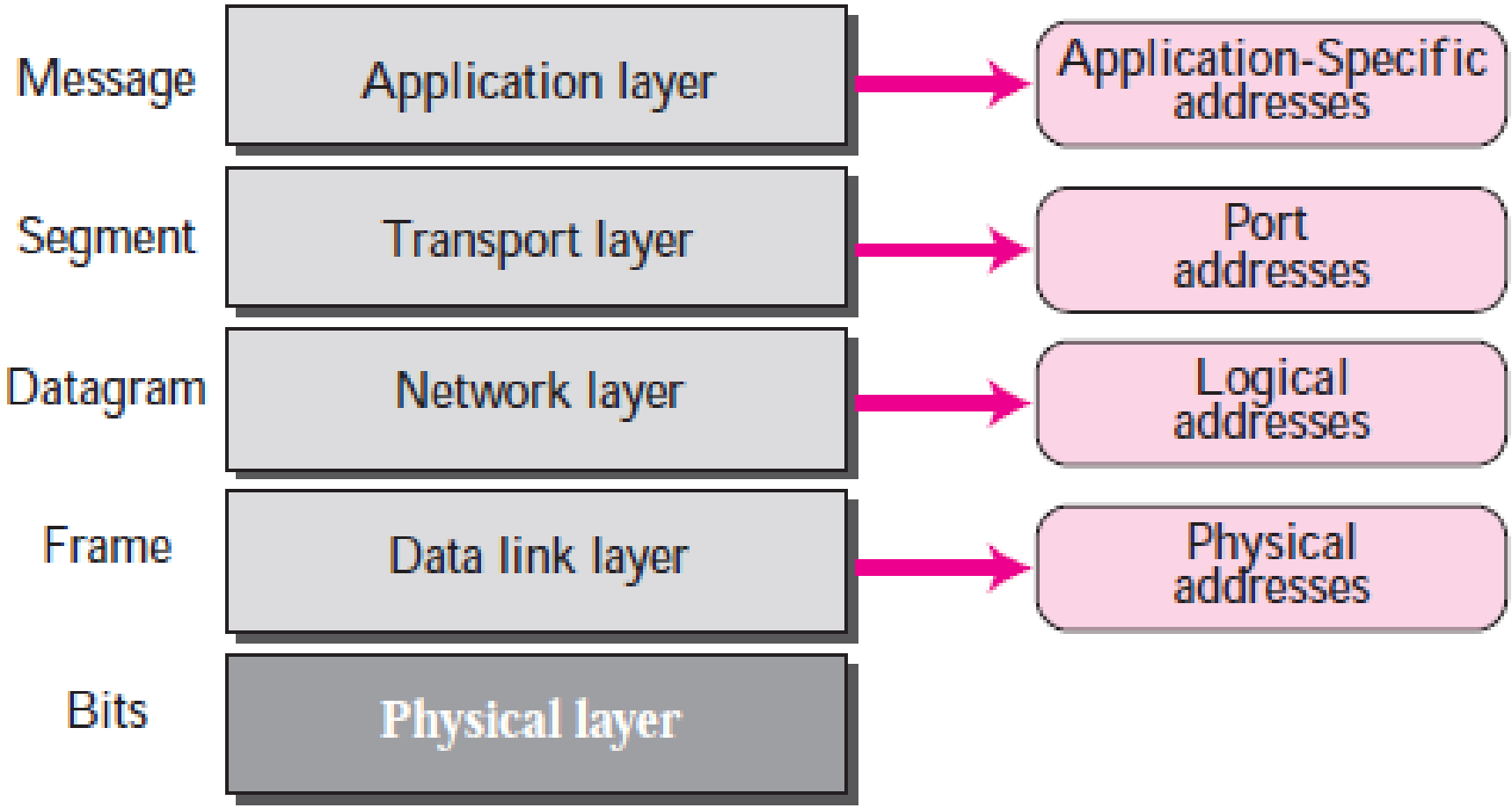
ADDRESSING

Figure 2-16

Addresses in TCP/IP

Addresses in tcp/ip

- Physical addresses (link address)
- Logical address
- Port address

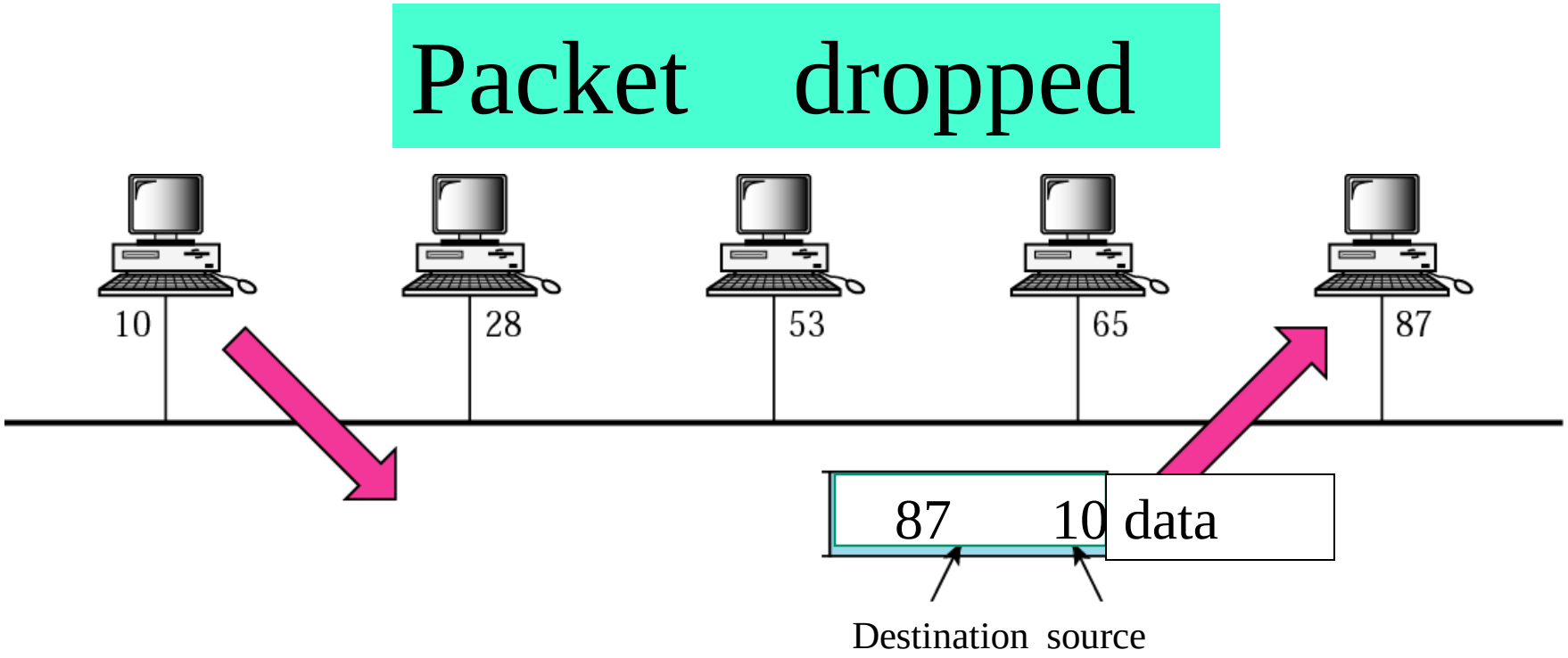


Example 1

Figure 2.18 shows an example of physical addresses.

Figure 2-18

Physical addresses



Example 2

Most local area networks use a 48-bit (6 bytes) physical address written as 12 hexadecimal digits, with every 2 bytes separated by a hyphen as shown below:

07-01-02-01-2C-4B

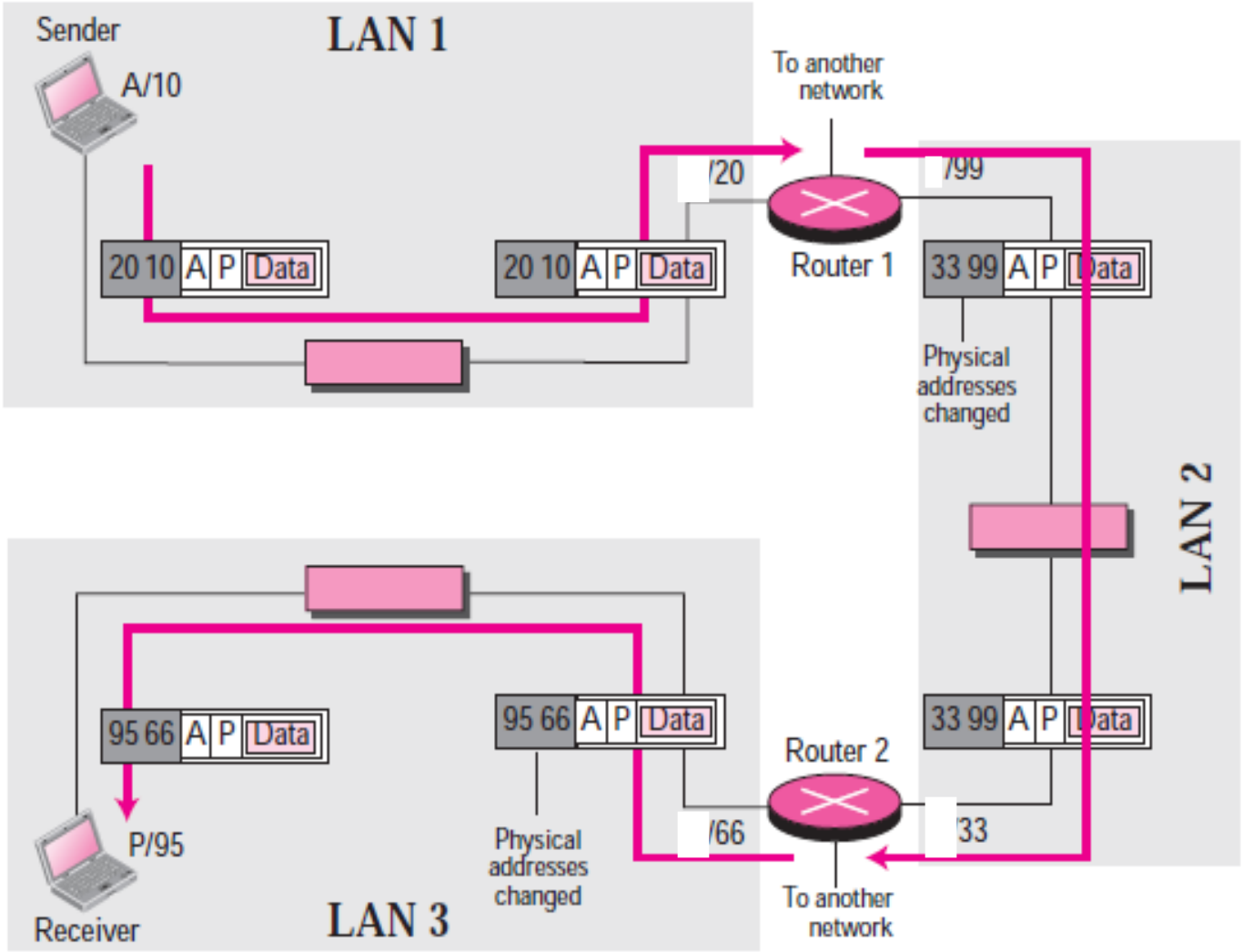
A 6-byte (12 hexadecimal digits) physical address

Example 3

Figure 2.19 shows an example of Internet addresses (32 bit).

Physical address changes from hop to hop but logical address remains the same.

Figure 2.17 *Example 2.5: logical addresses*



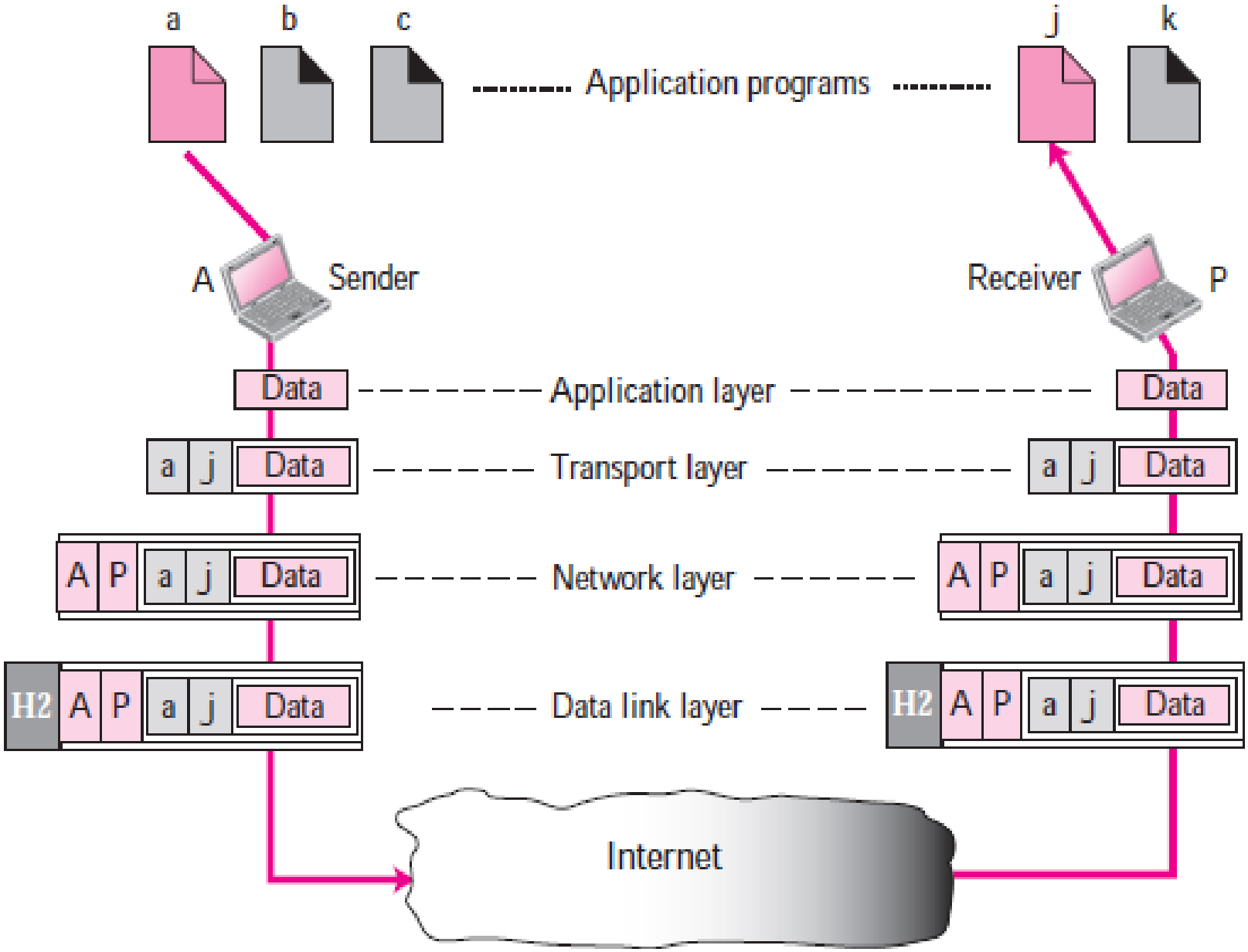
Example 4

As we will see in Chapter 4, an Internet address (in IPv4) is 32 bits in length, normally written as four decimal numbers, with each number representing 1 byte. The numbers are separated by a dot. Below is an example of such an address.

132.24.75.9

Port address

- Today, computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process.
- For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP).
- For these processes to receive data simultaneously, we need a method to label the different processes. In other words, they need addresses. In the TCP/IP architecture, the label assigned to a process is called a port address. A port address in TCP/IP is 16 bits in length.



Example 6

As we will see in Chapters 11 and 12, a port address is a 16-bit address represented by one decimal number as shown below.

753 **A 16-bit port address**

2.5

TCP/IP VERSIONS

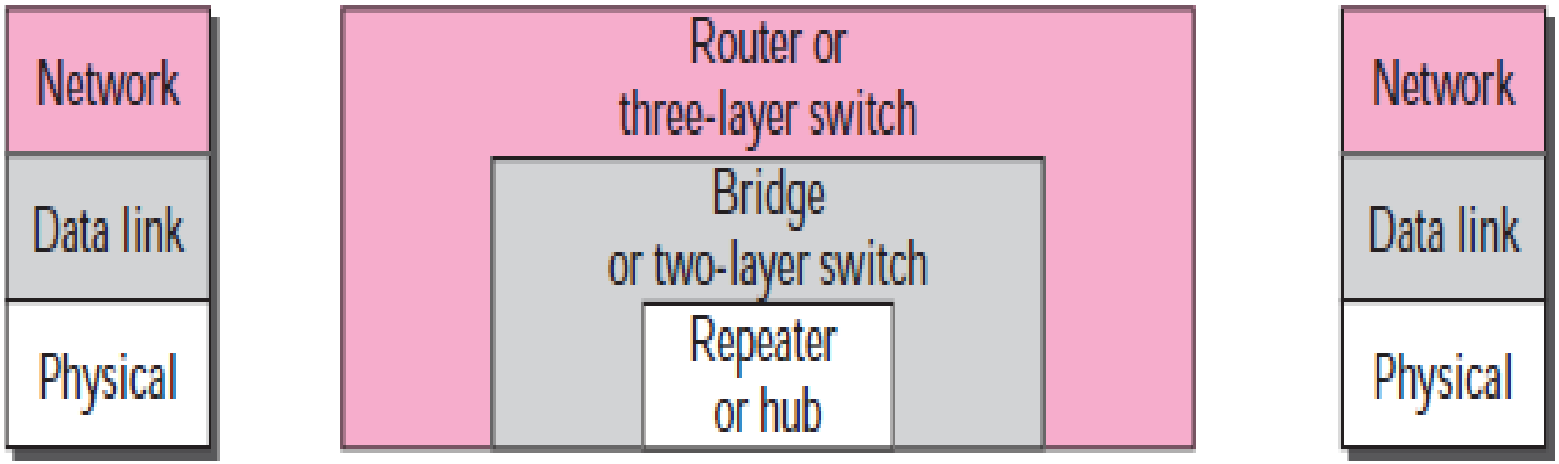
Versions:

- Version 4 (current)

Connecting devices

- We discuss three kinds of connecting devices: **repeaters or hubs, bridges or two-layer** switches, **and routers or three-layer switches**. Repeaters and hubs operate in the first layer of the Internet model. Bridges and two-layer switches operate in the first two layers. Routers and three-layer switches operate in the first three layers.

Figure 3.40 *Connecting devices*



Connecting devices

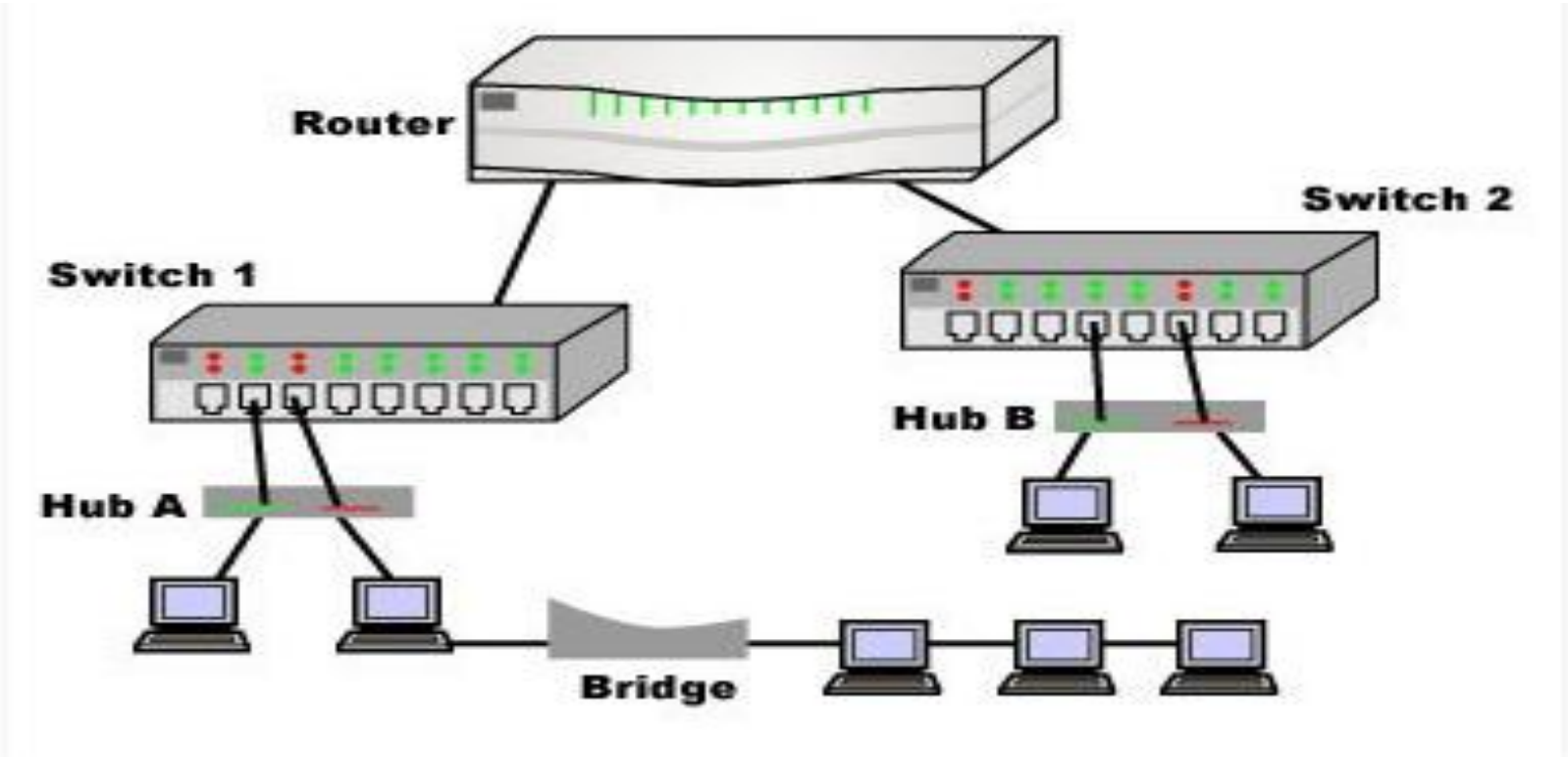
- **1. Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do no amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

- **2. Hub** – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

- **3. Bridge** – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

- **4. Switch** – A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

- **5. Routers** – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



- **6. Gateway** – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

vlans

- A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

- **Static and Dynamic VLANs**
- Network administrators often refer to static VLANs as “port-based VLANs.” A static VLAN requires an administrator to assign individual ports on the network switch to a virtual network. No matter what device is plugged into that port, it becomes a member of that same pre-assigned virtual network.

- Dynamic VLAN configuration allows an administrator to define network membership according to characteristics of the devices themselves rather than their switch port location.
- For example, a dynamic VLAN can be defined with a list of physical addresses (MACaddresses) or network account names.

- **Setting up a VLAN**
- At a high level, network administrators set up new VLANs as follows:
- Choose a valid VLAN number
- Choose a private IP address range for devices on that VLAN to use

- Configure the switch device with either static or dynamic settings. Static configurations require the administrator to assign a VLAN number to each switch port while dynamic configurations require assigning a list of MAC addresses or user names to a VLAN number.
- Configure routing between VLANs as needed. Configuring two or more VLANs to communicate with each other requires the use of either a VLAN-aware router.