1.4 Reference Models(1.4.1 The OSI Reference 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 n/w communications is the **OSI (Open System Interconnection)** Model.
- An open system is a model that allows any **two different systems to communicate regardless of their underlying architecture.**
- **Purpose**: The main purpose of the OSI model is to open communication between different systems without requiring changes to the logic of the underlying hardware and software.
- It was revised in 1995.
- The OSI model has seven layers. (Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, Application Layer)

OSI Model

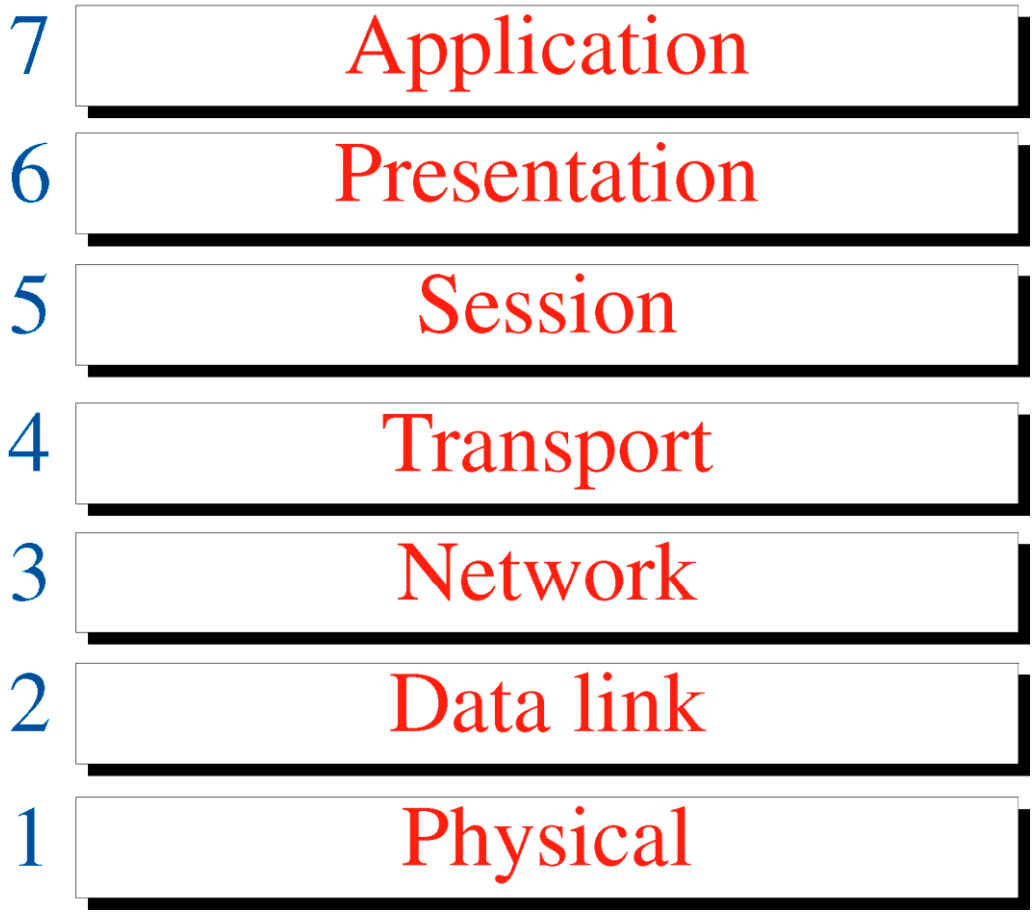
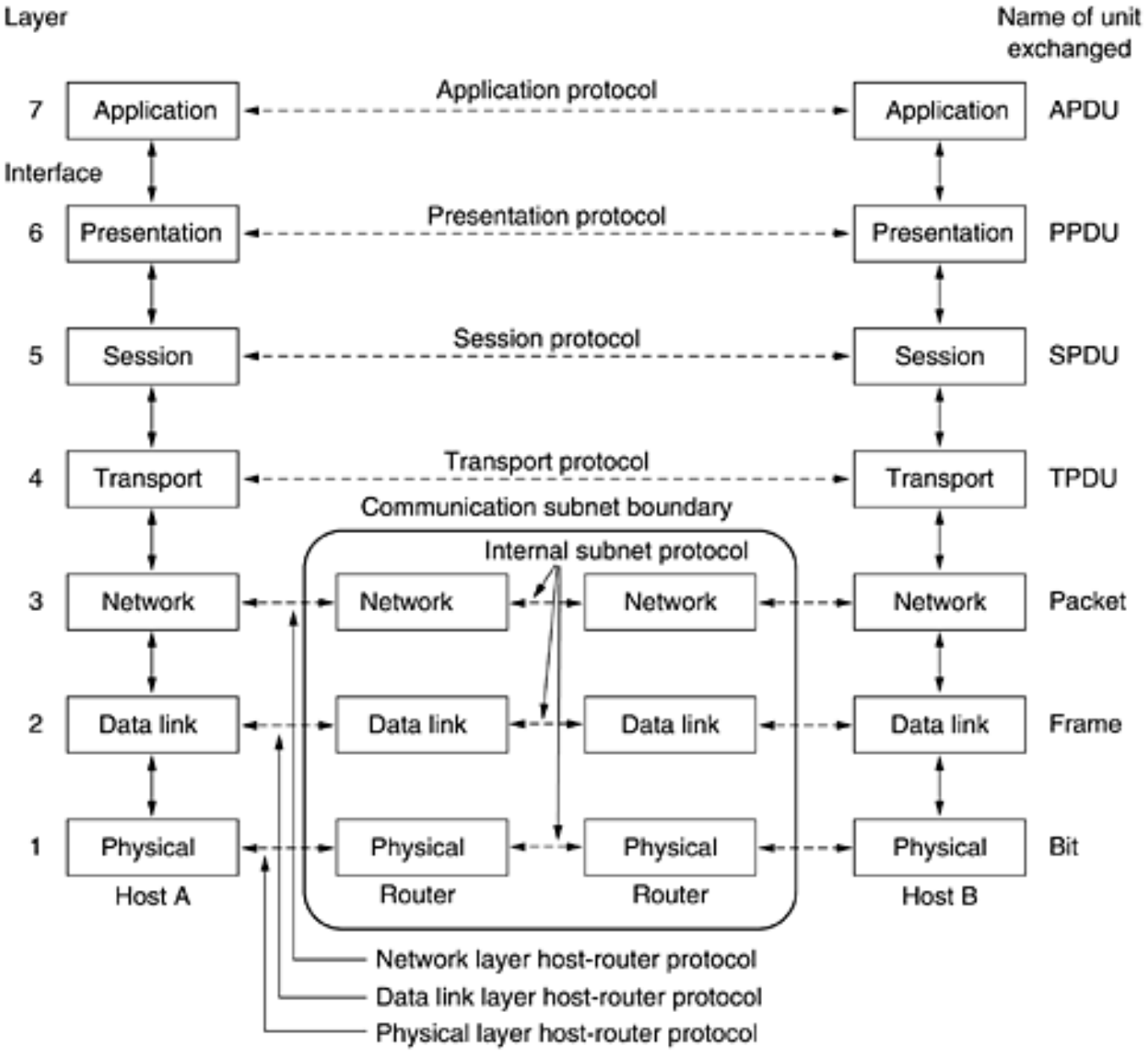
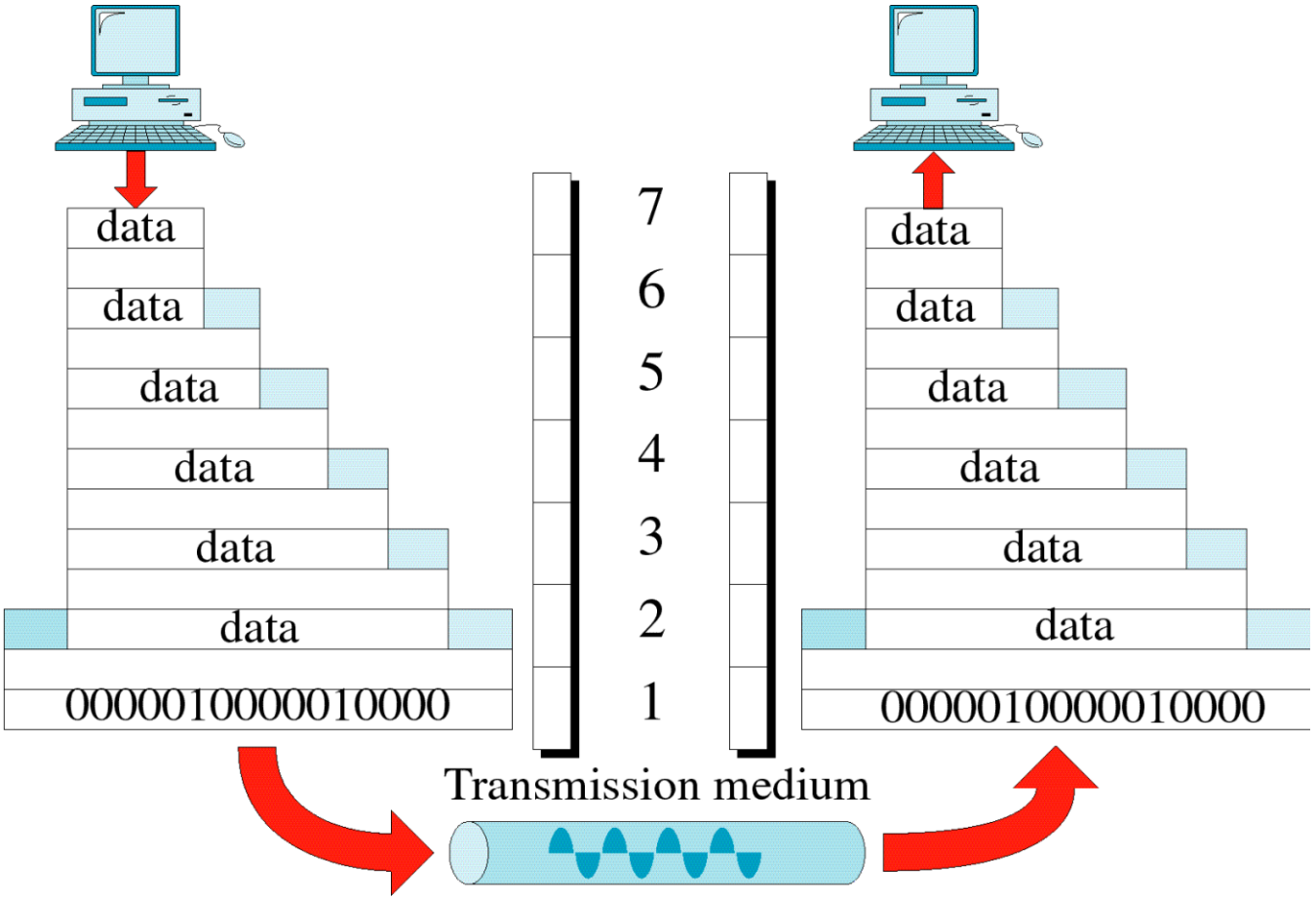

7
Application
6
Presentation
5
Session
4
Transport
3
Network
2
Data link
1
Physical

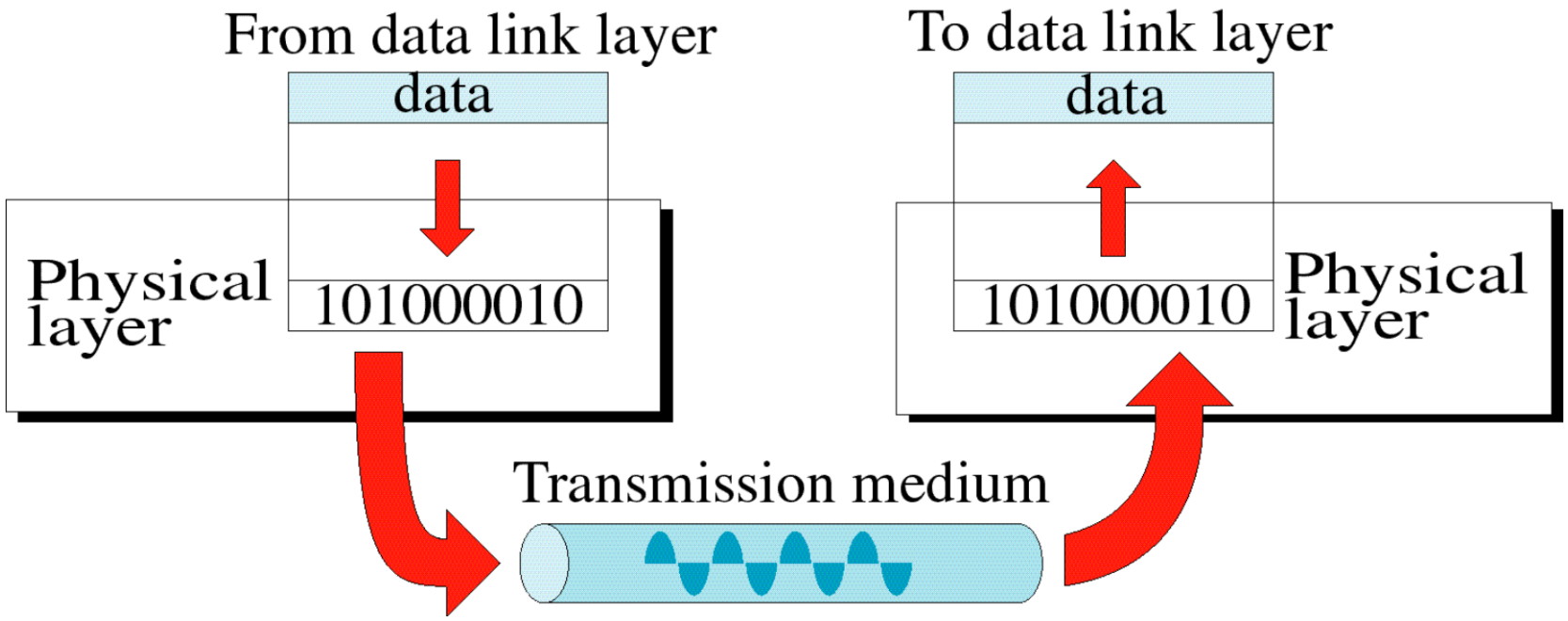
Figure The OSI reference model.



An Exchange Using the OSI Model



Physical Layer



The OSI Reference Model (The Physical Layer)

- The physical layer is concerned with **transmitting raw bits over a communication channel.** The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit.

- **Physical characteristics of interface and media**: It defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
- **Representation of bits**: The physical layer data consists of a stream of bits **without any interpretation.** For the transmission of bits over transmission channel, data are converted into signals using various types of encoding techniques.
- **Data Rate:** It is also defined by the physical layer.

The OSI Reference Model (The Physical Layer)

- **Synchronization of bits:** The sender and receiver must be synchronized at the bit level.

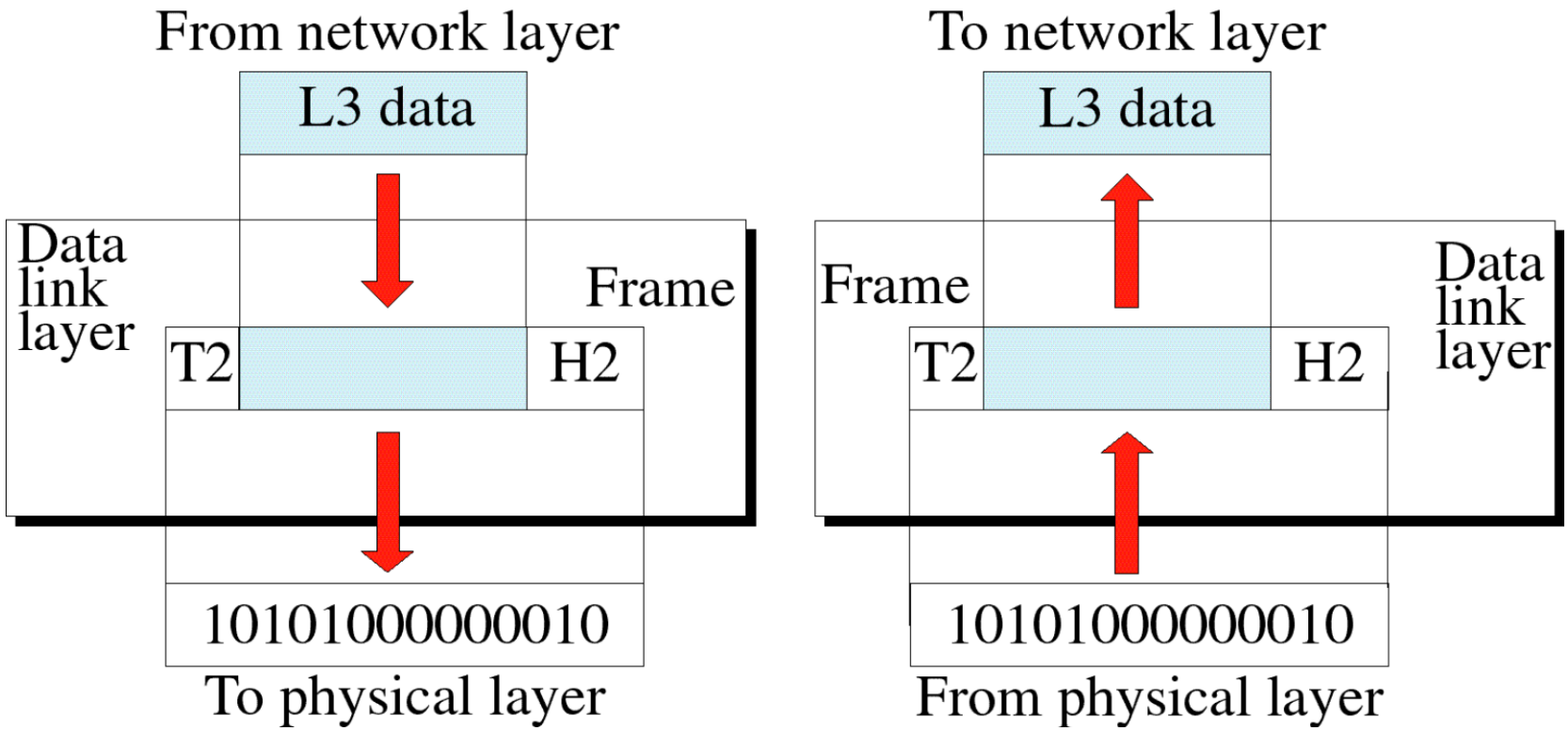
- **Line Configuration:** It defines the line configuration either point-to-point or multipoint line configurations.

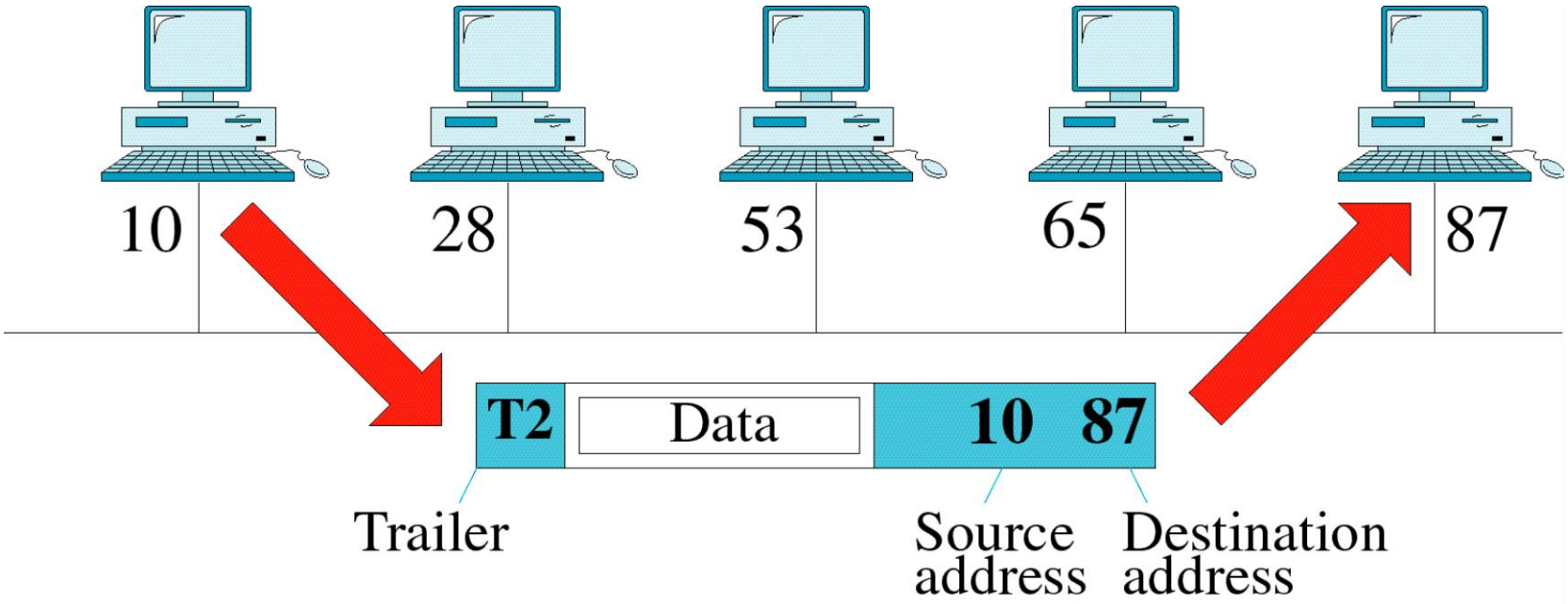
- **Physical Topology:** It defines how devices are connected to make a network. It may be *ring*, bus, tree, star, mesh topology.

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

Data Link Layer

- To organize **bits into frame**, to provide node-to-node delivery. It is also responsible for flow control, error control and access control.
- **Framing:** The data link layer divides the stream of bits received from the network layer into manageable data unit 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 physical address of the sender and receiver of the frame.
- Trailer is added for **error control**.
- **Access Control:** When two or more devices are connected to the same link, DLL protocols are necessary to determine which device has control over the link at any given time.


From network layer
L3 data
Data link layer
Frame
T2
H2
10101000000010
To physical layer
To network layer
L3 data
Frame
Data link layer
T2
H2
10101000000010
From physical layer


10
28
53
65
87
T2
Data
10 87
Trailer
Source address
Destination address

Network Layer

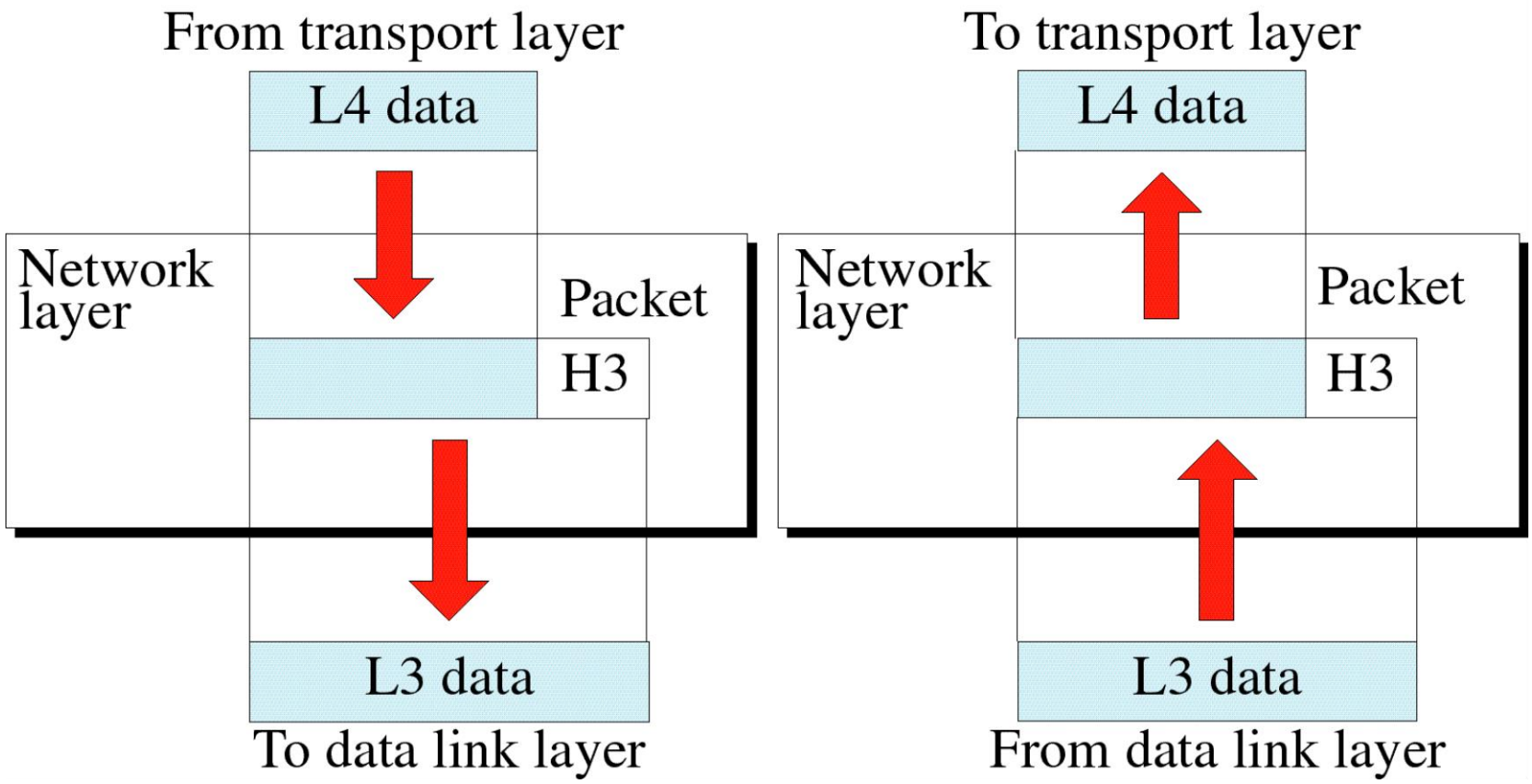
- To move **packets from source to destination**, provide **internetworking**.
- The **NL** is responsible for the **source-to-destination delivery of a packet** possibly across multiple networks, whereas the **DLL** oversees the **delivery of the packets between two systems** on the same network.
- If **two systems are connected to the same link**, there is usually **no need for a network layer**. However, if the **two systems are attached to different networks** with connecting devices between the networks, there is often a **need for the network layer to accomplish source to destination delivery**.

Network Layer

- **Logical Address:** The physical addressing implements by the DLL handles the addressing problem locally. If a packet passes the n/w boundary, we need another addressing system to help distinguish the source and destination systems. The NL adds a header to the packet coming from the upper layer that, among other things, includes the **logical address of the sender and receiver**.

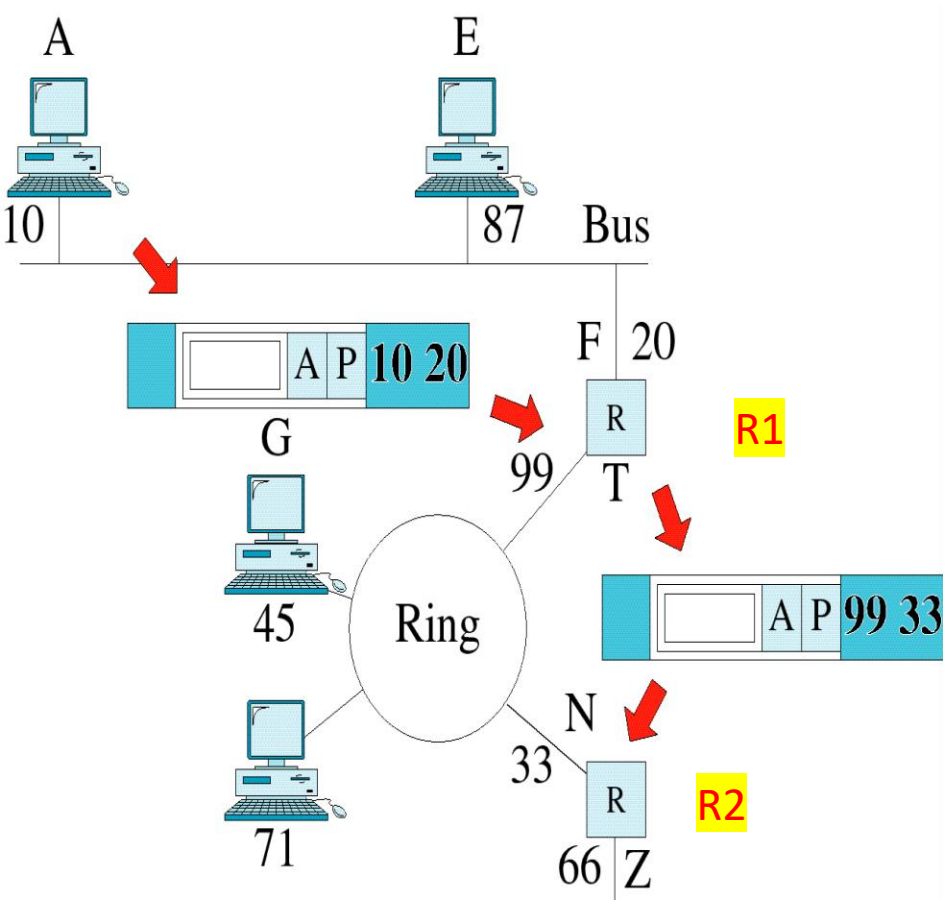
- **Routing:** When independent networks or links connected together to create an internetwork or a large network, the connecting devices (routers or gateways) **route the packets to their final destination.**

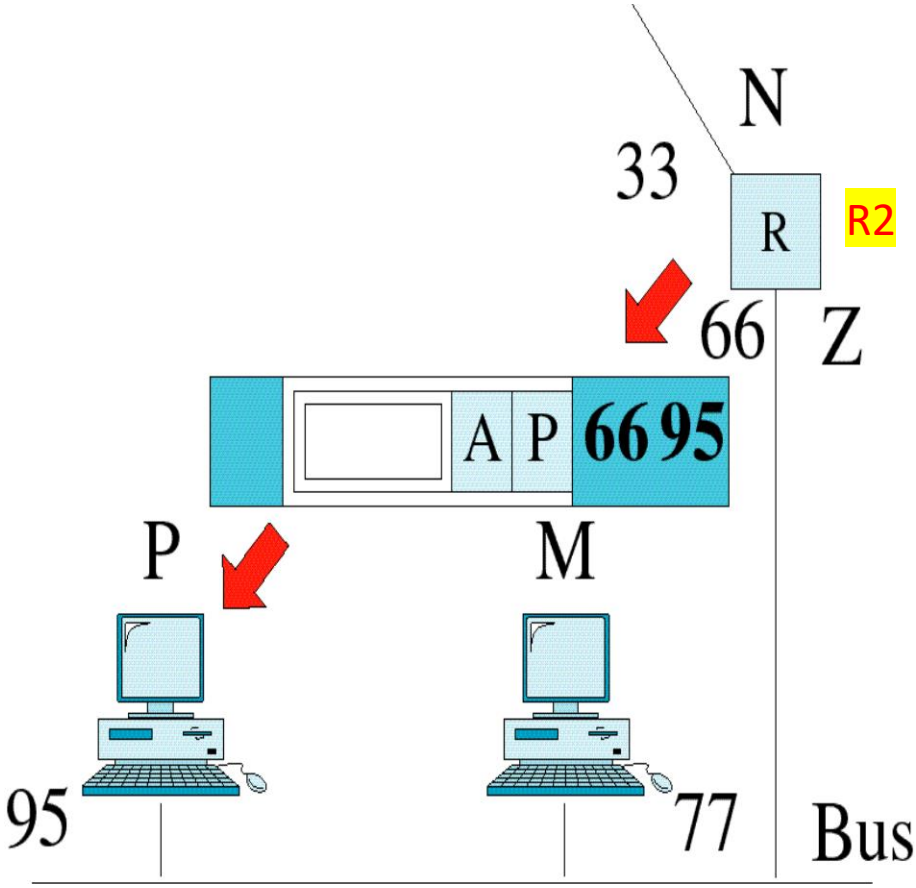
Network Layer



Alphabet represents Physical Address
Number represents Logical Address

Network Layer

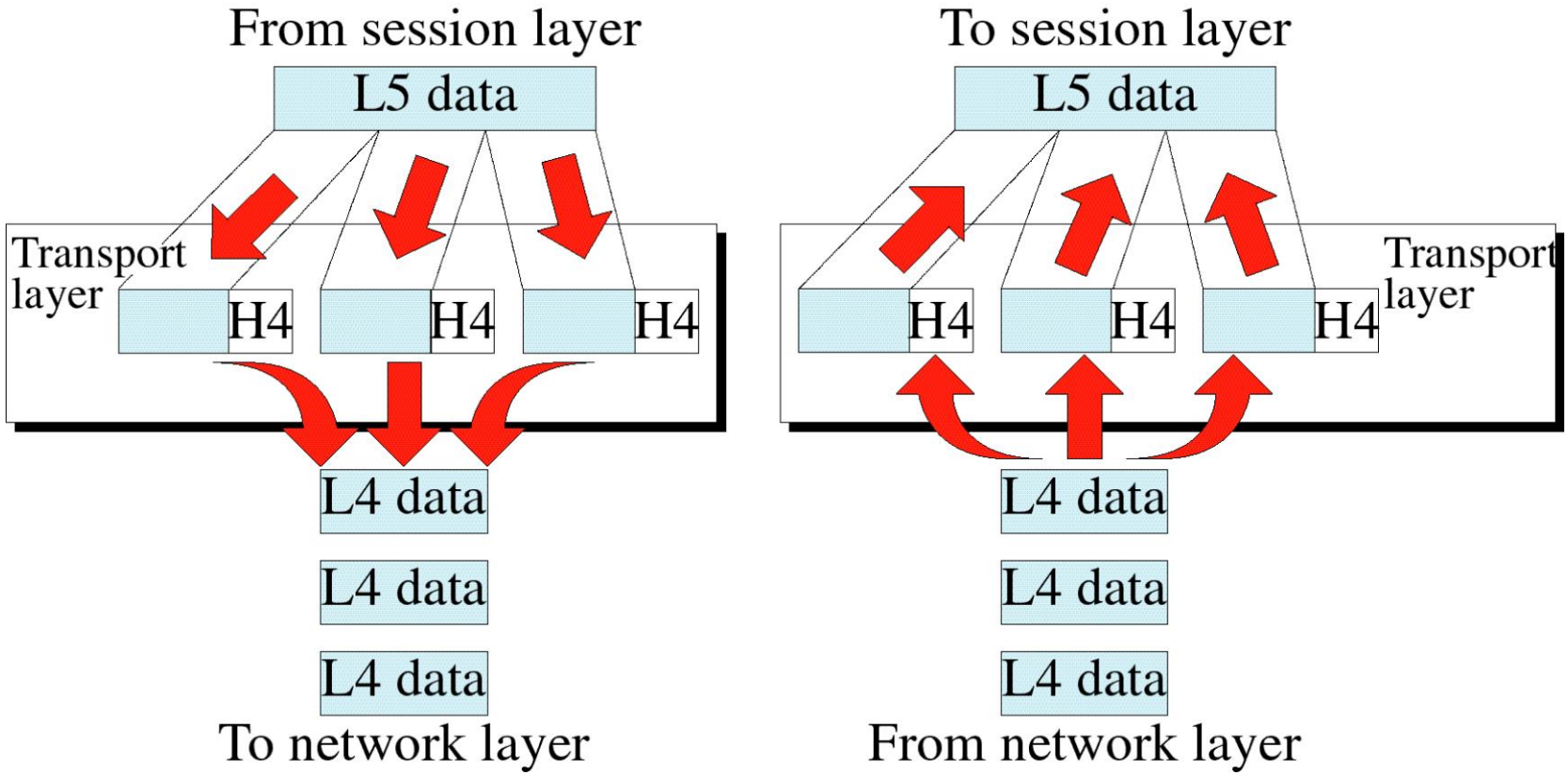




Transport Layer

- The Transport layer is responsible for source to destination (end-to-end) delivery of the **entire message** whereas the n/w layer oversees end-to-end delivery of **individual packets**, it doesn't recognize any relationship between those packets. But the TP Layer ensures that the whole message arrives intact and in order, overseeing both **error control** and **flow control** at the source-to-destination level.
- For security, the TL may create a connection between the two end ports. A connection is a single logical path between the source and destination that is associated with all packets in a message.
- This connection include three steps:
  1. Connection establishment
  2. Data Transfer
  3. Connection Release

Transport Layer



Transport Layer

- **Functions of Transport Layer:**
- **Service-point addressing**: Communication occurs not just from end machine to end machine but from end application to end application. Data generated by an application on one machine must be received not just by other machine but by the correct application on the other machine, so to ensure accurate delivery from access point to service access point, we need **another level of addressing** in addition to those at the DLL an NL levels.
- **E.g.s of services:**
- SMTP: Simple Mail Transfer Protocol
- FTP: File Transfer Protocol
- TELNET: Terminal Network
- SNMP: Simple Network Management Protocol
- HTTP: Hyper Text Transfer Protocol

Transport Layer

- According to **IANA (Internet Assigned No. Authority)**, port numbers are divided into three ranges.

1. **Well-known Port**: **0 to 1023**. They all are assigned and controlled by IANA.
2. **Registered Port**: **1024 to 49,151.** Not assigned & controlled by IANA, but they can be registered with IANA to prevent duplication.
3. **Dynamic Port [Private]**: **49,152 to 65,535**. They are neither controlled nor registered. They can be used for any process.

Well-known Ports

- 20 & 21: File Transfer Protocol (FTP)
- 22: Secure Shell (SSH)
- 23: Telnet remote login service
- 25: Simple Mail Transfer Protocol (SMTP)
- 53: Domain Name System (DNS) service
- 80: Hypertext Transfer Protocol (HTTP) used in the World Wide Web
- 110: Post Office Protocol (POP3)
- 119: Network News Transfer Protocol (NNTP)
- 143: Internet Message Access Protocol (IMAP)
- 161: Simple Network Management Protocol (SNMP)
- 443: HTTP Secure (HTTPS)

Transport Layer

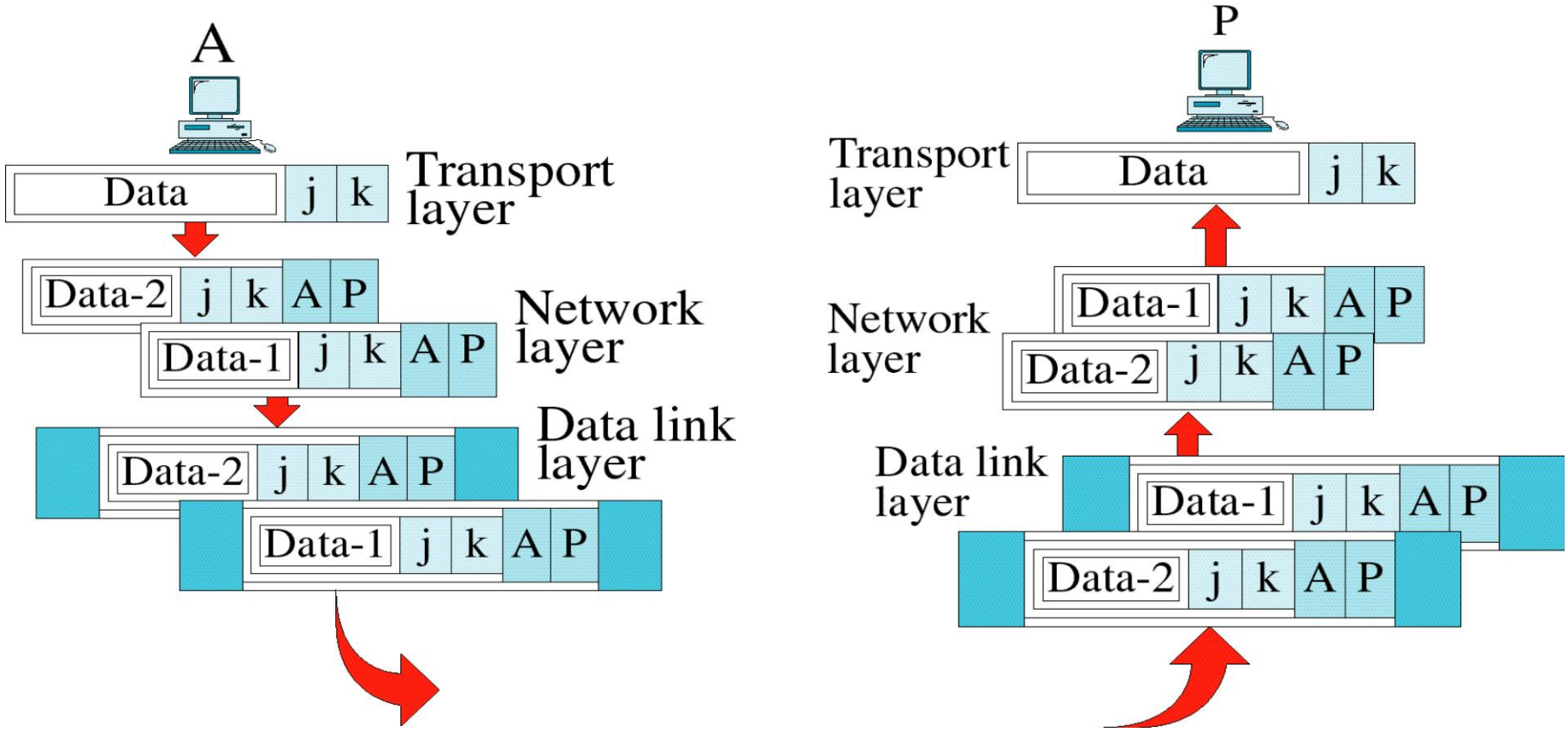
- **Segmentation and Reassembly**: A message is divided into transmittable segments (Packets), with each segment containing a sequence number.

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

- **Flow Control**: Like DLL, the TP is responsible for flow control, but flow control at this layer is performed end to end rather than across a single link.

- **Error Control**: Like DLL, the TP is responsible for error control, but flow control at this layer is performed end to end rather than across a single link.

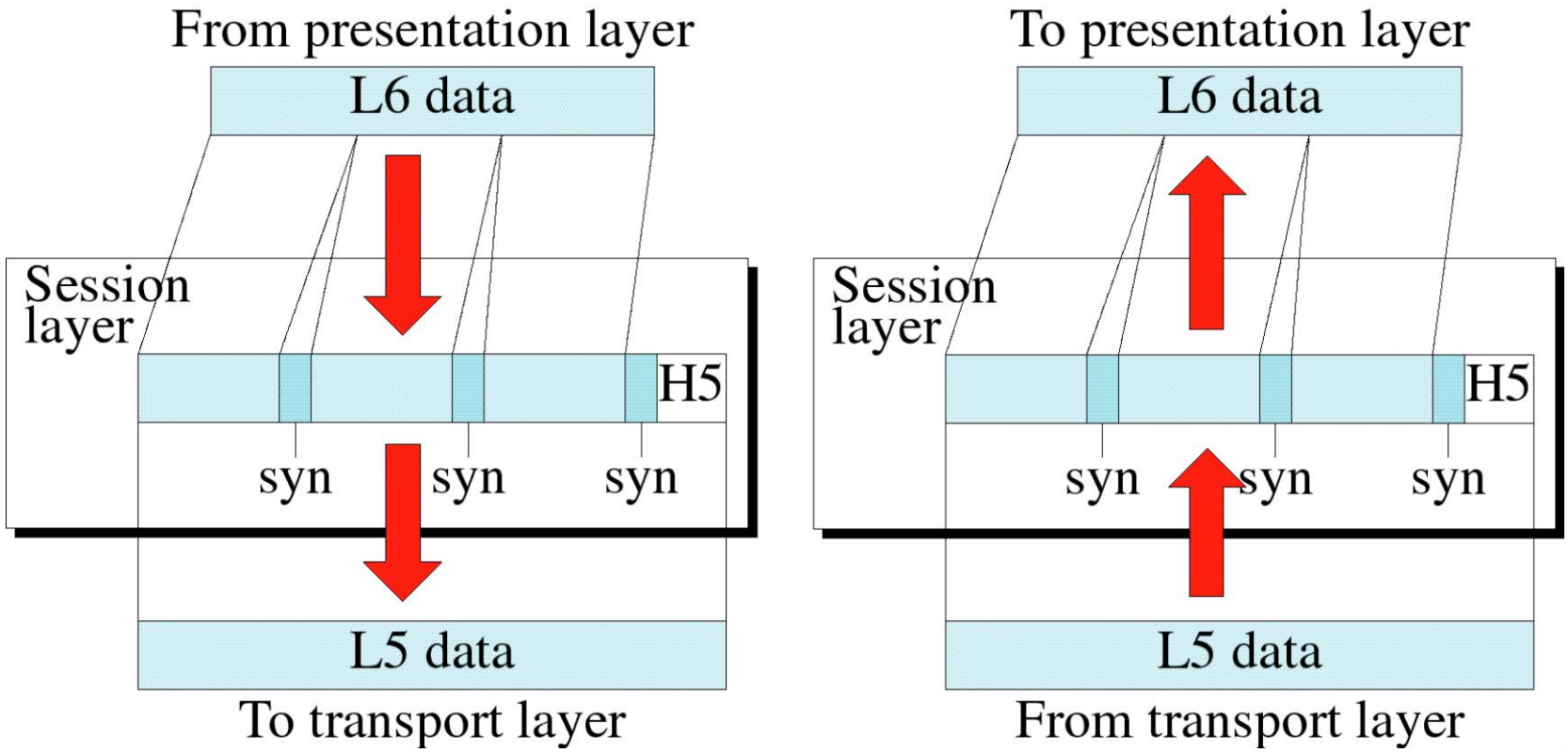
Transport Layer



Session layer

- The session layer is responsible fie **dialog control** and **synchronization**.
- It establishes, maintains, and synchronizes the interaction among communicating systems.
- **Functions of session layers:**
- **Dialog Control**: The session layer allows two systems to enter into a dialog.
- **Synchronization**: The session layer allows a process to add checkpoints to a stream of data. For e.g., 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.

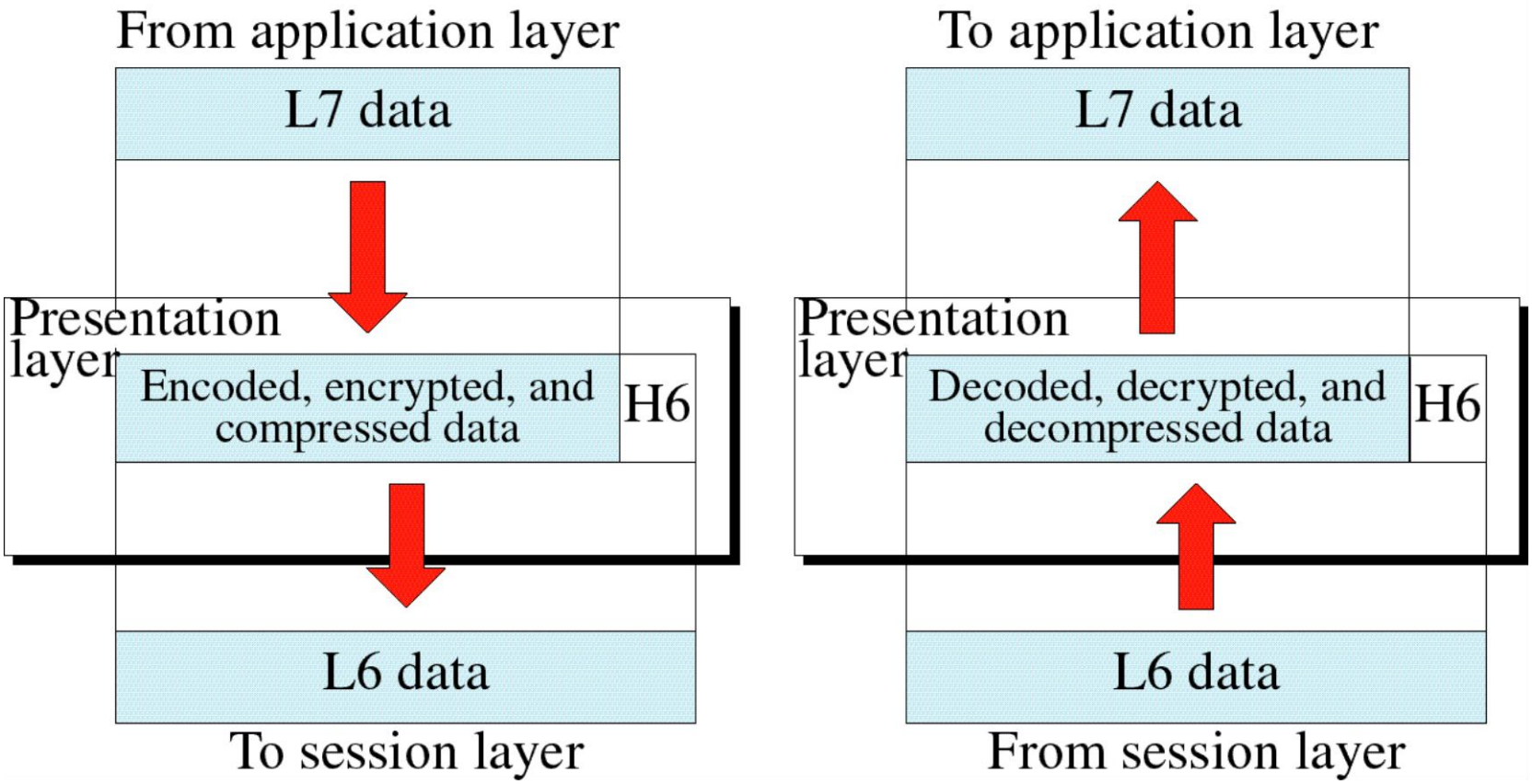
Session Layer



Presentation Layer

- The Presentation layer is responsible for translation, compression and encryption.
- **Translation:** The process (running program) in two systems are usually exchanging information in the form of **character strings, numbers** and so on. The information must be changed **to bit streams** before being transmitted. Because different computers use different encoding systems, the presentation layer at the sender changes the information from **its sender-dependent** format into **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 ensure privacy.
- **Compression:** Data compression reduces the number of bits contained in the information.

Presentation Layer



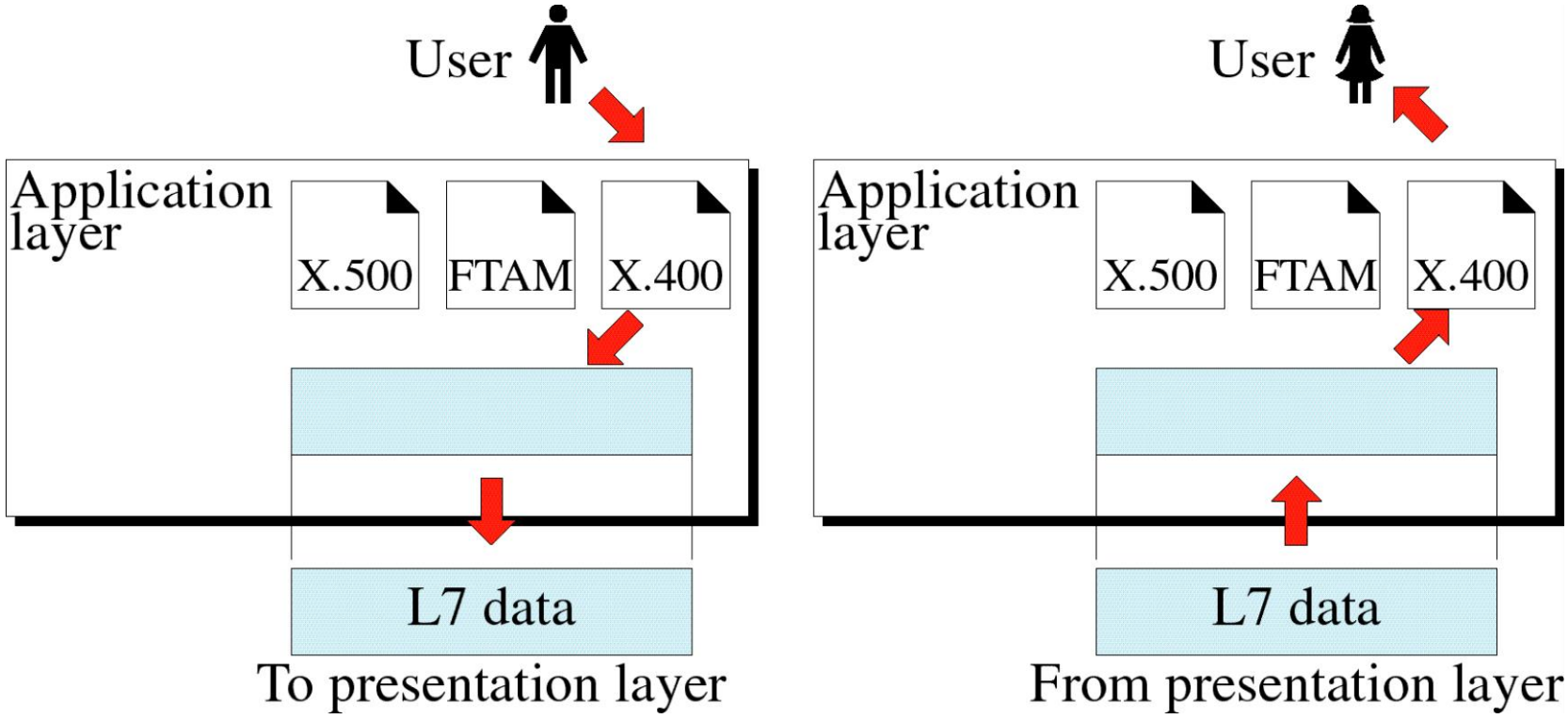
Application Layer

- The application layer is responsible **for providing services to the user.**
- Specific services provided by the application layer include following:

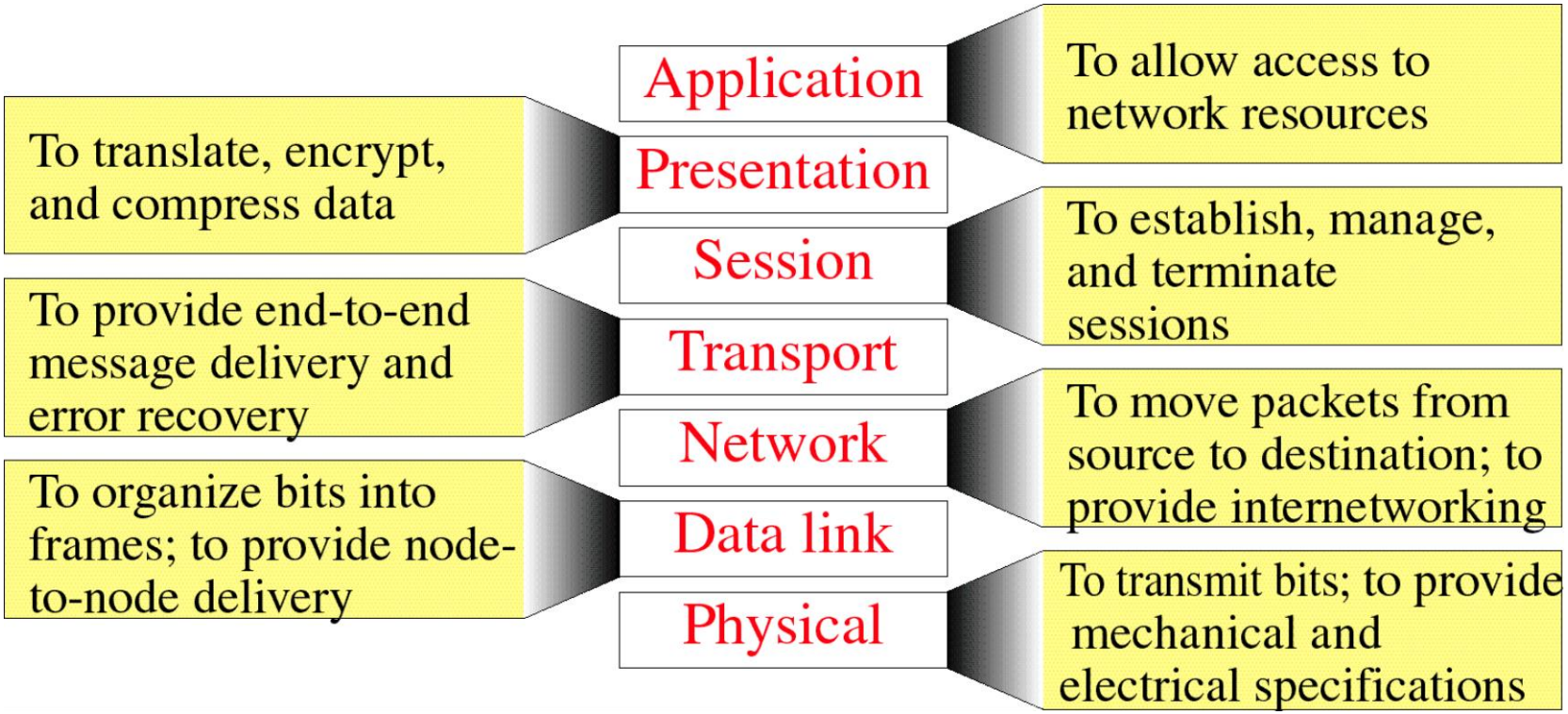
- **File transfer, access and management:** This application allows a user to access files in a remote host, to retrieve files from a remote computer for use in the local computer.

- **Mail server:** This application provides the basis for e-mail forwarding and storage.

Application Layer



Summary of Layer Functions



1.4.2 The TCP/IP Reference Model

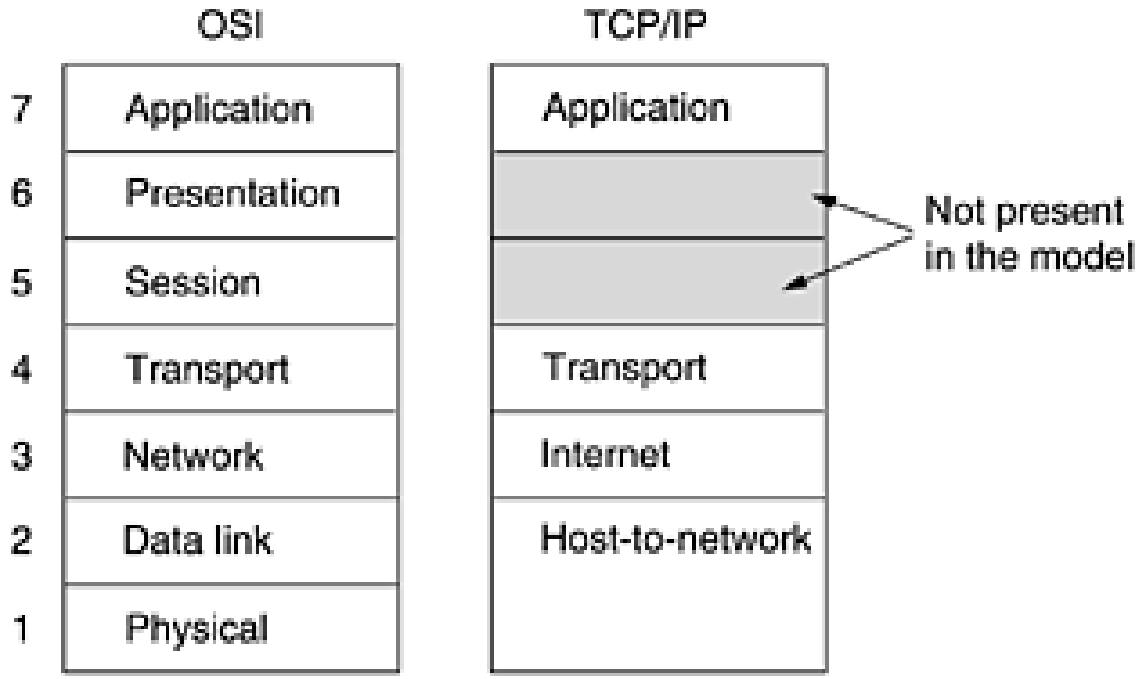
- The grandparent of all wide area networks, the ARPANET sponsored by DoD (Department of Defense) of US.

- It eventually connected **hundreds of universities and government installations,** using leased lines.

- When satellite and radio networks were added later, the existing protocols had trouble interworking with them, so a new reference architecture was needed.

1.4.2 The TCP/IP Reference Model

- The TCP/IP reference model has four layers: **host-to-network Layer, internet Layer, transport Layer, Application Layer**
- The Host-to-network layer of TCP/IP is equivalent to Data link and physical layer of OSI model.
- The Internet layer of TCP/IP is equivalent to Network layer of OSI model.
- The Application layer of TCP/IP is roughly doing the job of the session, presentation and application layer of OSI.



Differences between TCP & OSI

- **TCP/IP** is a standard **protocol** used for every network including the Internet, whereas,
- **OSI** is not a **protocol** but a reference **model** used for **understanding and designing** the system architecture.

- **TCP/IP** is a four-layered **model**, whereas, **OSI** has seven layers.

- **TCP/IP** is Tangible, whereas, **OSI** is not.

1.4.2 The TCP/IP Reference Model (The Internet Layer)

- The job of Internet Layer is to permit hosts **to inject packets into any network** and have them travel **independently** to the destination (potentially on a different network).
- They may **arrive in a different order** than they were sent, in which case it is the job of higher layers to rearrange them.
- The internet layer defines an official **packet format** and **protocol** called IP (**Internet Protocol**).

1.4.2 The TCP/IP Reference Model (The Transport Layer)

- First protocol of Transport layer is **TCP (Transmission Control Protocol):**
- It is a connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet.
- It fragments the incoming byte stream into discrete messages and passes each one on to the internet layer.
- At the destination the receiving, the receiving TCP process reassembles the received messages into the output stream.
- TCP also handles **flow control.**

1.4.2 The TCP/IP Reference Model (The Transport Layer)

- The second protocol is **UDP** (User Datagram Protocol).
- It is an unreliable, connectionless protocol for applications.
- It is widely used for one, client-server-type, request-reply queries and applications in which **prompt delivery** is **more important than accurate delivery**, such as transmitting speech or video.