COMPUTER NETWORK

- ✓ Protocol architectures & Comparison
- ✓ Network Types & Topologies

- Slides compiled by Sanghamitra De

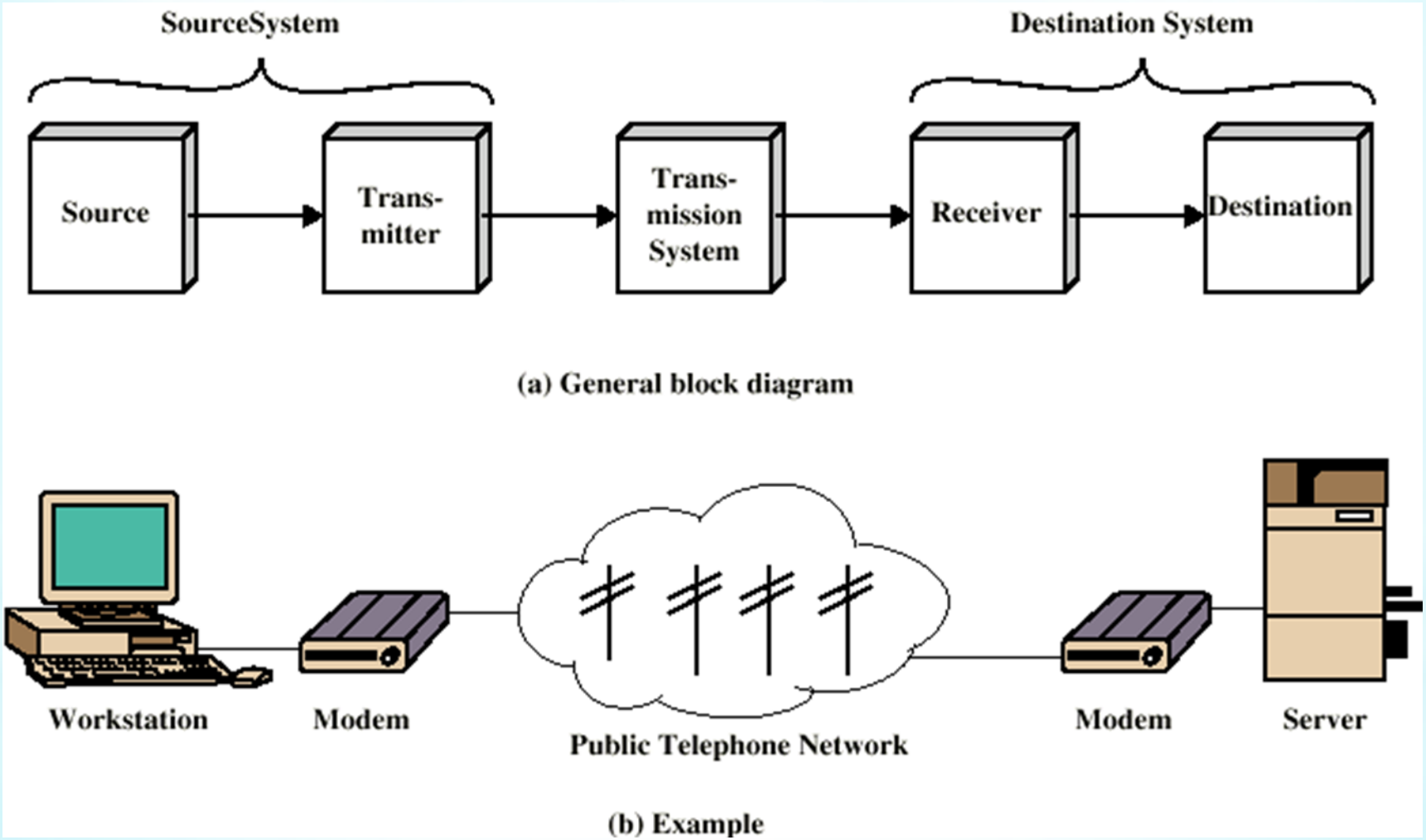
Basic Definitions

- A **network** is a combination of hardware and software that sends data from one location to another.
- A protocol is a set of rules governing how communicating parties/entities are to interact.
- Purpose of a protocol is to provide some service.
- E.g. FTP provides File Transfer service.
- A **protocol stack** is a complete set of network protocol layers that work together to provide networking capabilities. It is called a stack because it is typically designed as a hierarchy of layers, each supporting the one above it and using those below it.
- A protocol can be implemented by hardware, software, or a combination of both.

Network Functionalities

- Transmission System Utilization
- Interfacing
- Signal Generation
- Synchronization
- Exchange Management
- Error detection and correction
- Addressing and routing
- Recovery
- Message formatting
- Security
- Network Management

Simplified Communications Model - Diagram



A Communications Model

- Source
  - generates data to be transmitted
- Transmitter
  - Converts data into transmittable signals
- Transmission System
  - Carries data
- Receiver
  - Converts received signal into data
- Destination
  - Takes incoming data

ISO/OSI Model

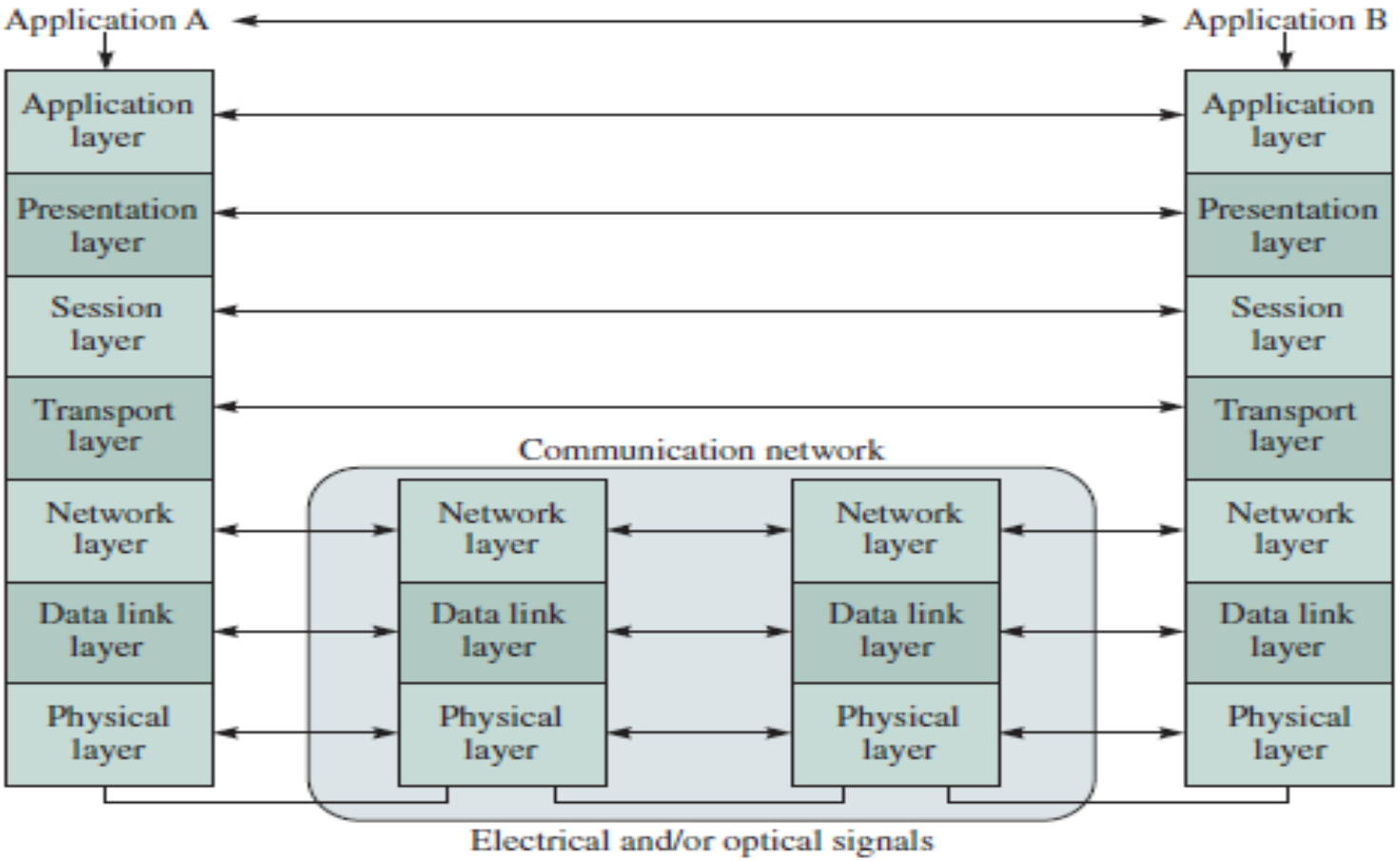


FIGURE The OSI reference model

ISO/OSI Model: Peer-to-Peer Processes

- At the physical layer, communication is direct.
- At the higher layers, however, communication must move down through the layers on device A, over to device B, and then back up through the layers.
- Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it.
- At layer I the entire package is converted to a form that can be transmitted to the receiving device.
- At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it.

ISO/OSI Model: Interfaces Between Layers

- The passing of the data and network information up/down through the layers of the sending/receiving device is made possible by an interface between each pair of adjacent layers.
- Each interface defines the information and services a layer must provide for the layer above it.
- Well-defined interfaces and layer functions provide modularity to a network.

ISO/OSI Model: Organization of the Layers

Seven layers can be thought of as belonging to three subgroups:

- Layers I, 2, and 3-physical, data link, and network are the network support layers

  - deal with the physical aspects of moving data from one device to another

- Layers 5, 6, and 7-session, presentation, and application-can be thought of as the user support layers

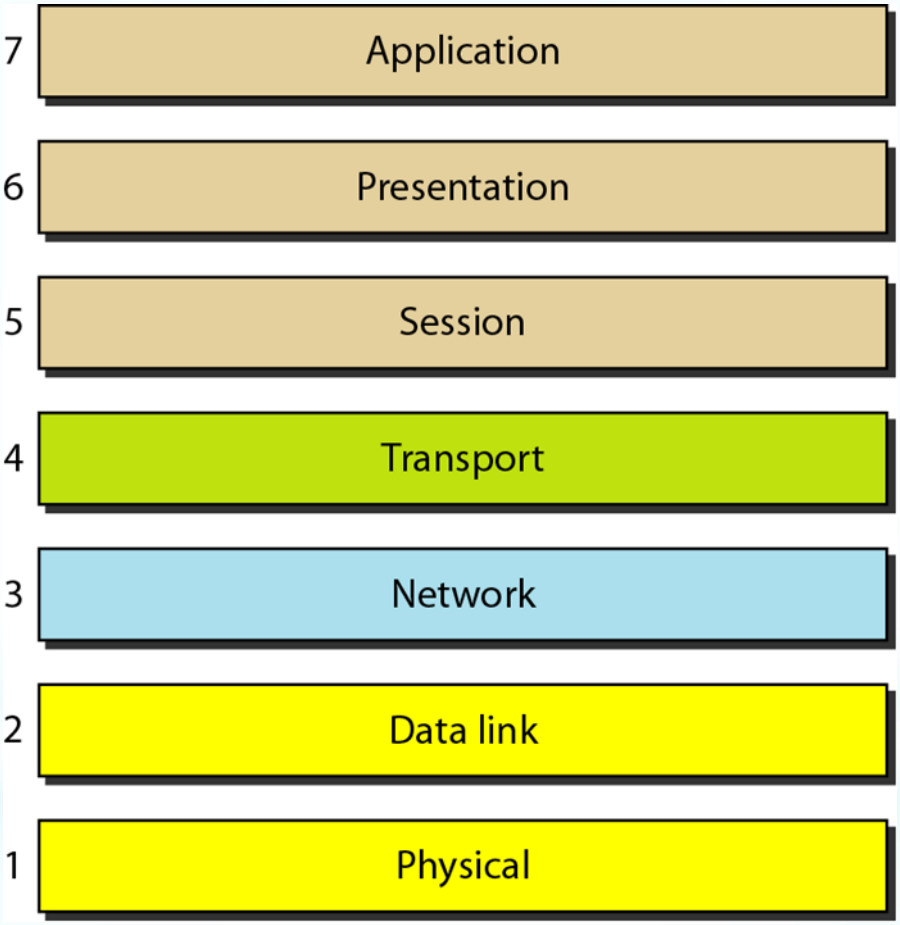
  - allow interoperability among unrelated software systems.

- Layer 4, the transport layer

  - links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use.

- OSI upper layers are mostly implemented in software
- OSI lower layers are a combination of hardware and software
- physical layer is mostly hardware

Seven layers of the OSI model



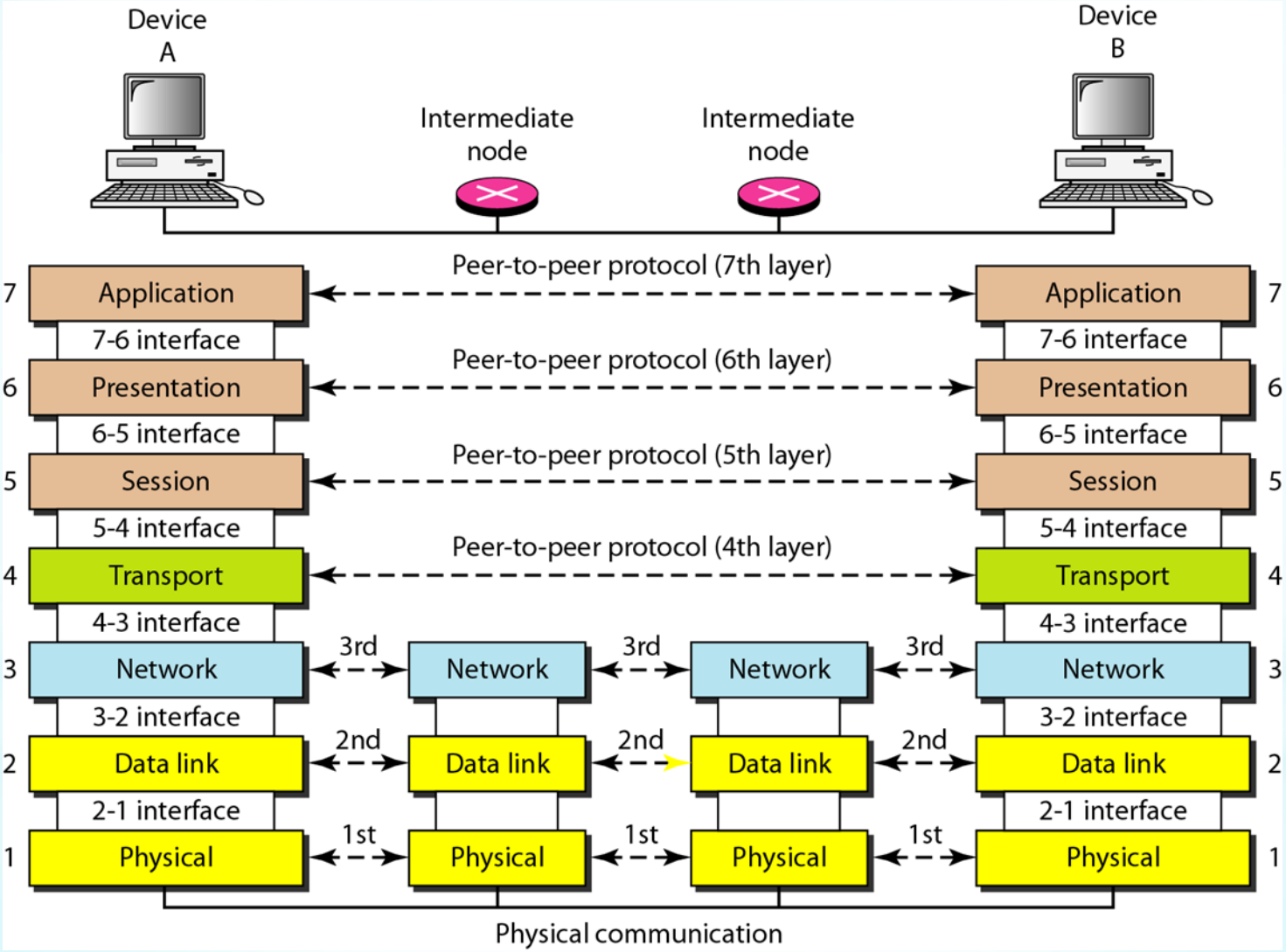
Protocol Data Units (PDU)

* At each layer, protocols are used to communicate
* Control information is added to user data at each layer
* Transport layer may fragment user data
* Each fragment has a transport header added
  - Destination Service Access Point (SAP)
  - Sequence number
  - Error detection code
* This gives a transport protocol data unit

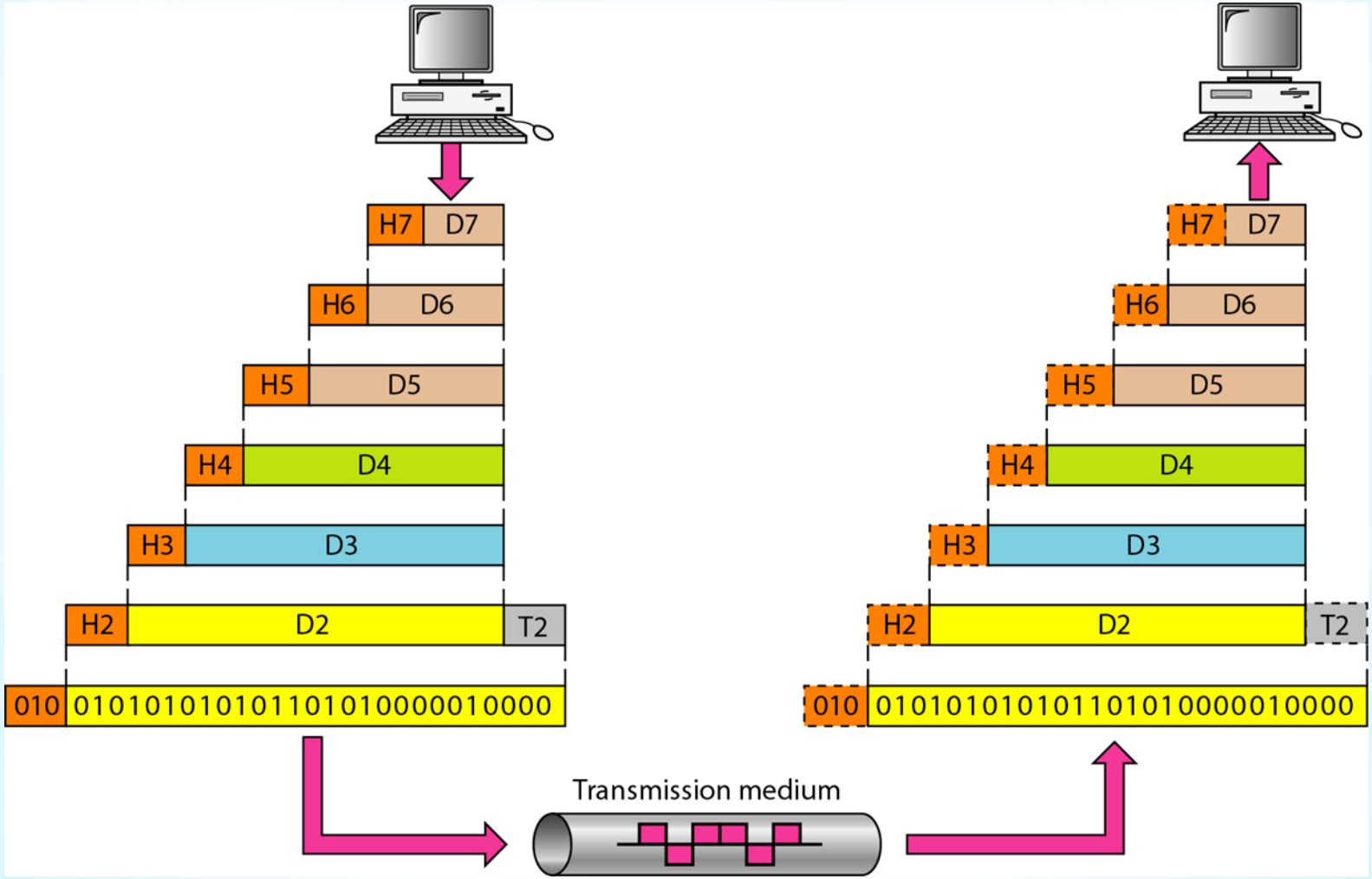
Network PDU

- Adds network header
  - network address for destination computer
  - Facilities requests

Interaction between layers in the OSI model



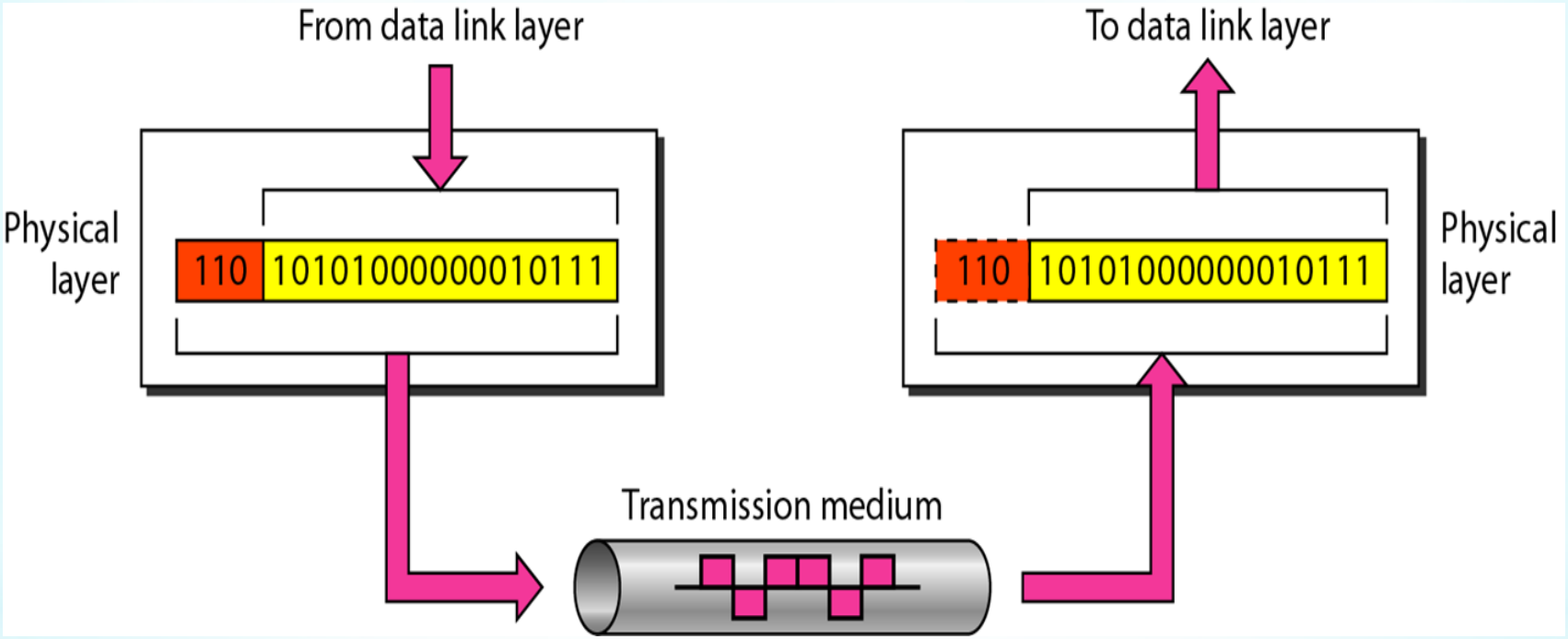
An exchange using the OSI model



Layers in the OSI Model

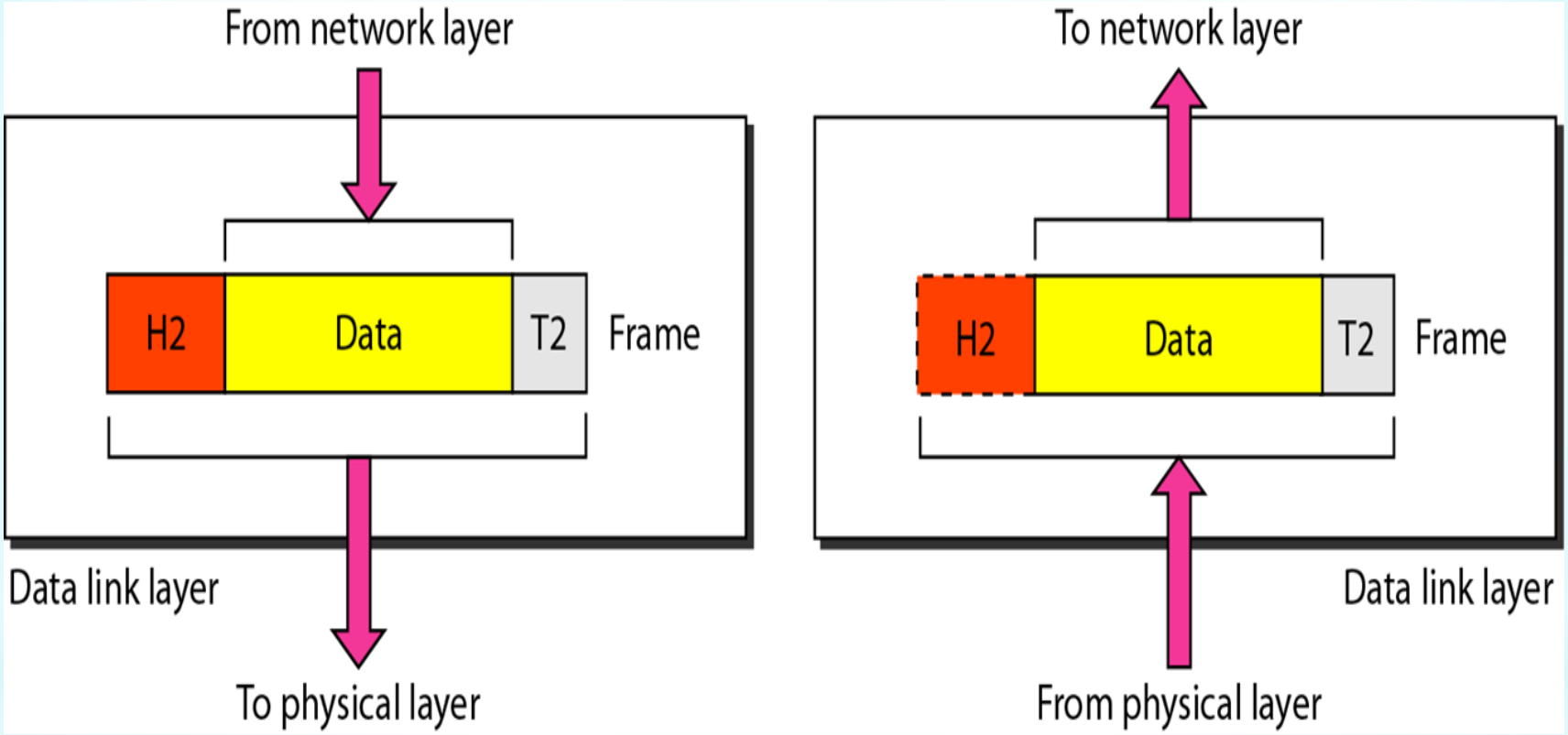
* Physical Layer
* Data Link Layer
* Network Layer
* Transport Layer
* Session Layer
* Presentation Layer
* Application Layer

Physical layer



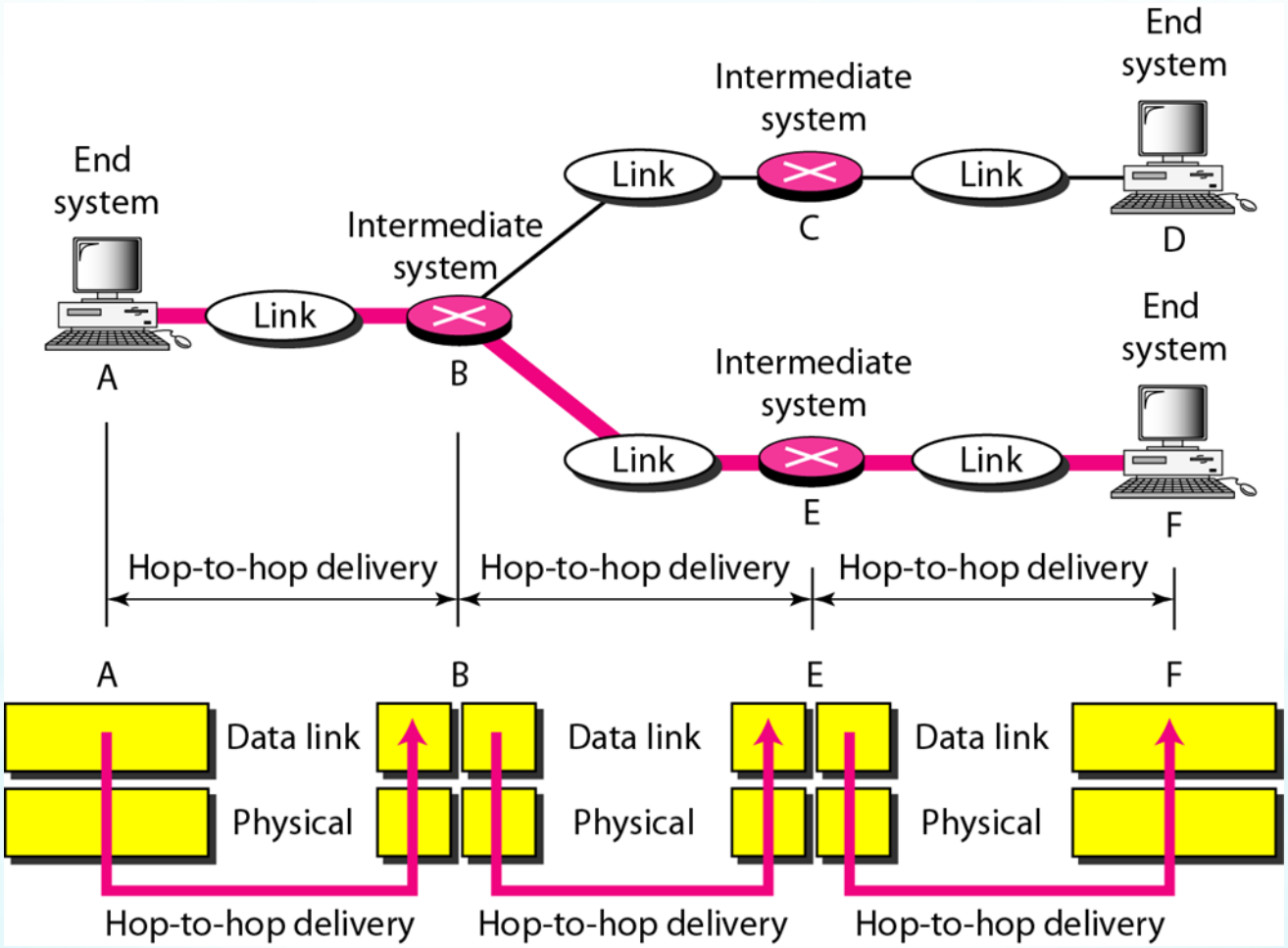
The physical layer is responsible for movements of individual bits from one hop (node) to the next.

Data link layer

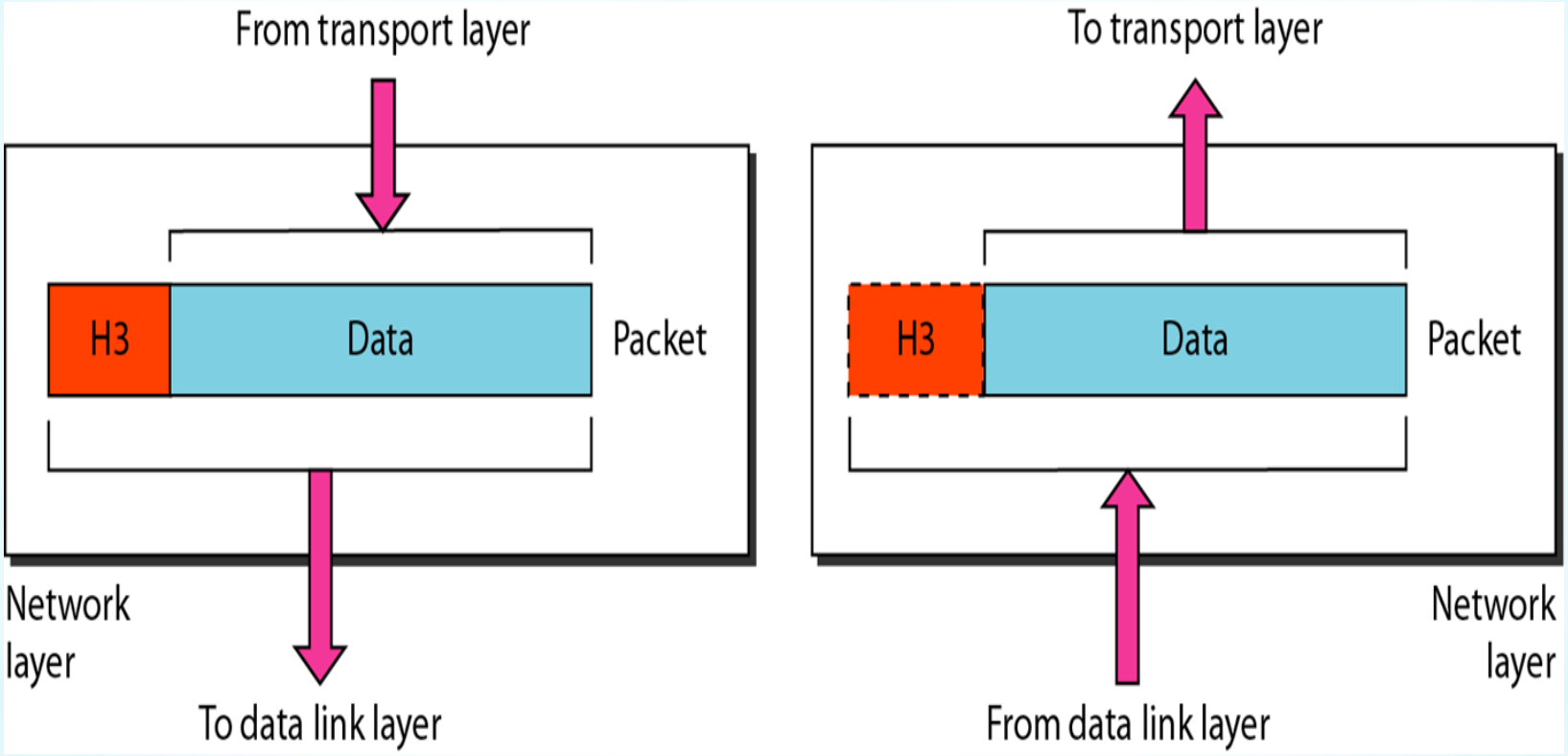


The data link layer is responsible for moving frames from one hop (node) to the next.

Hop-to-hop delivery

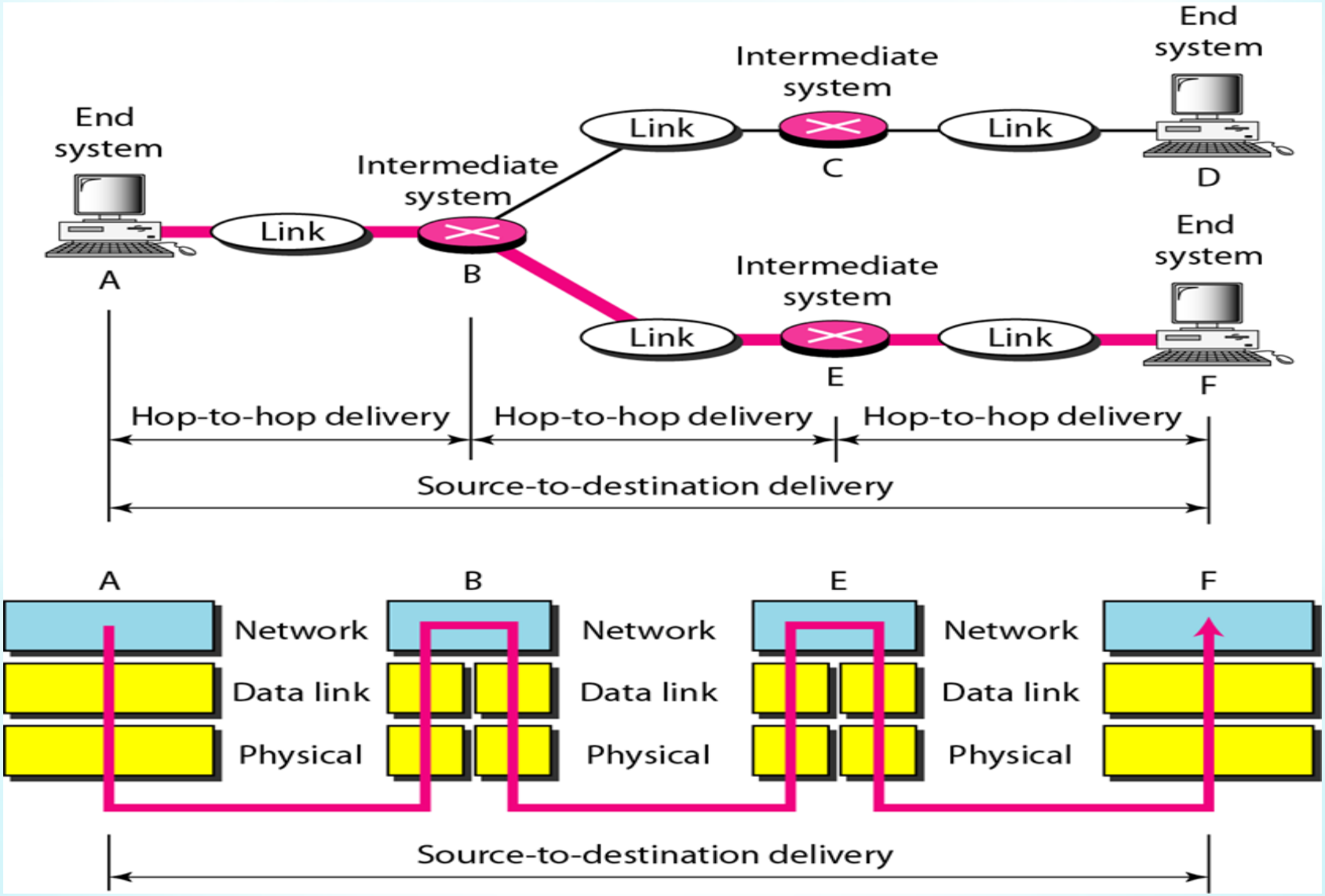


Network layer

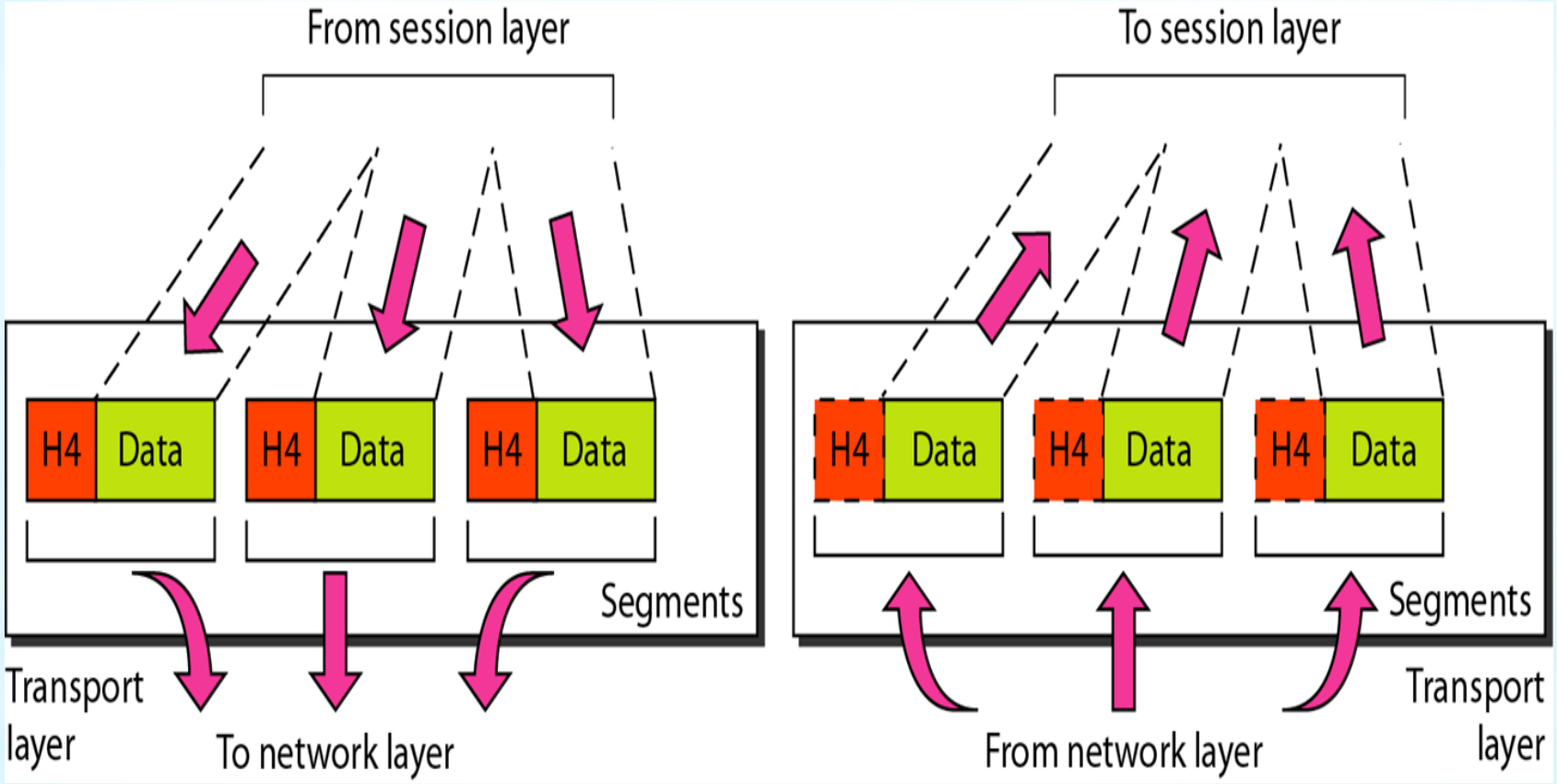


The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Source-to-destination delivery

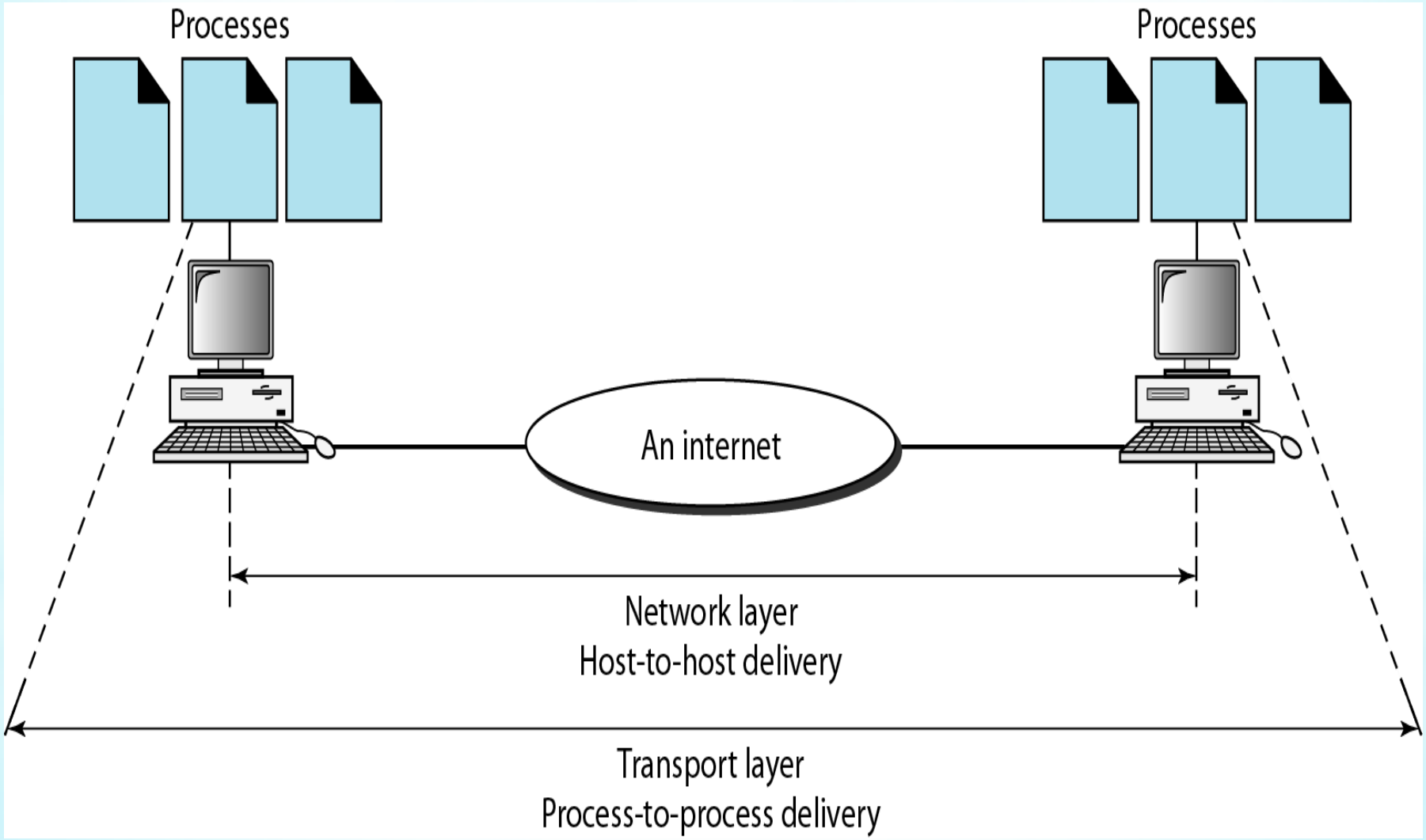


Transport layer

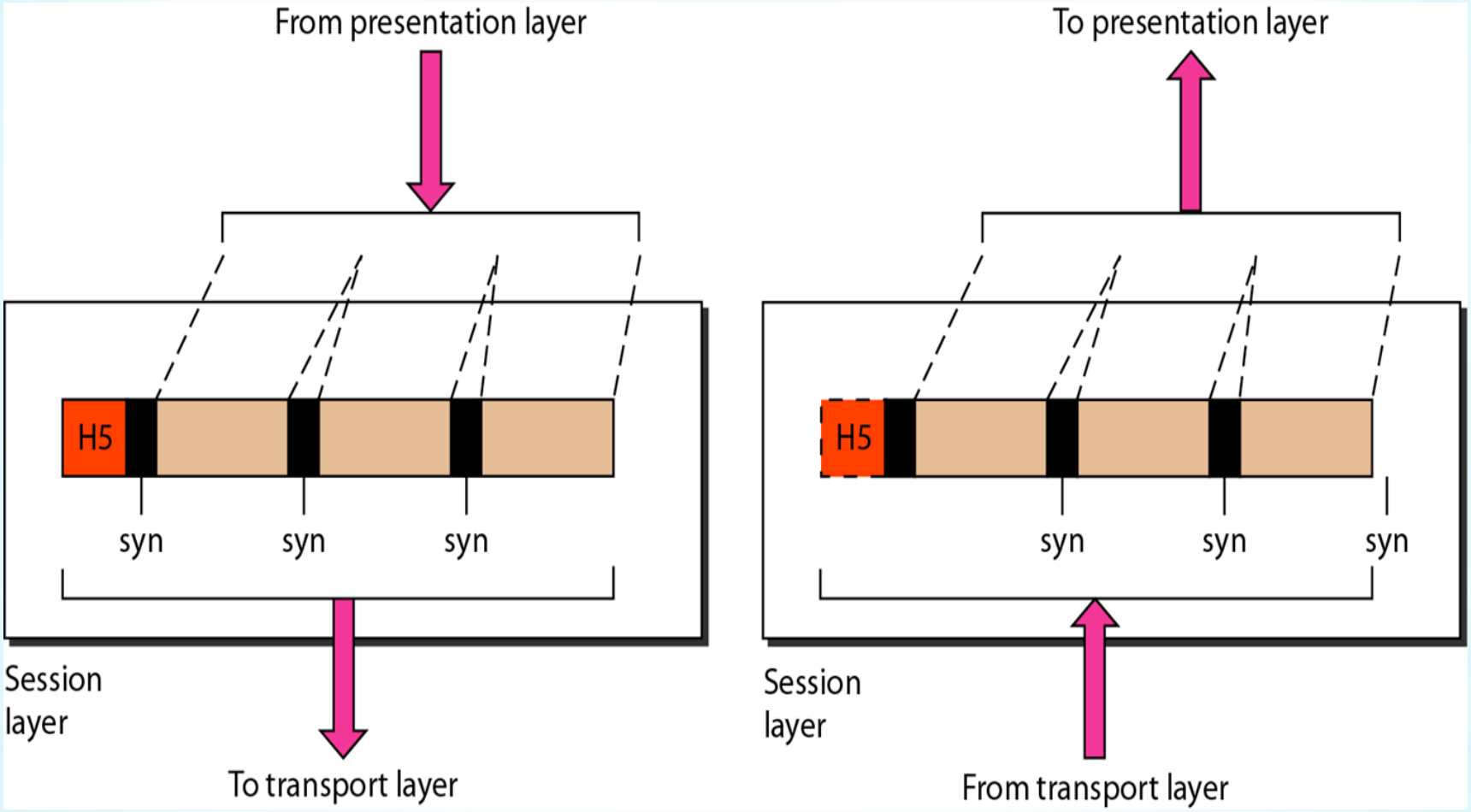


The transport layer is responsible for the delivery of a message from one process to another.

Reliable process-to-process delivery of a message

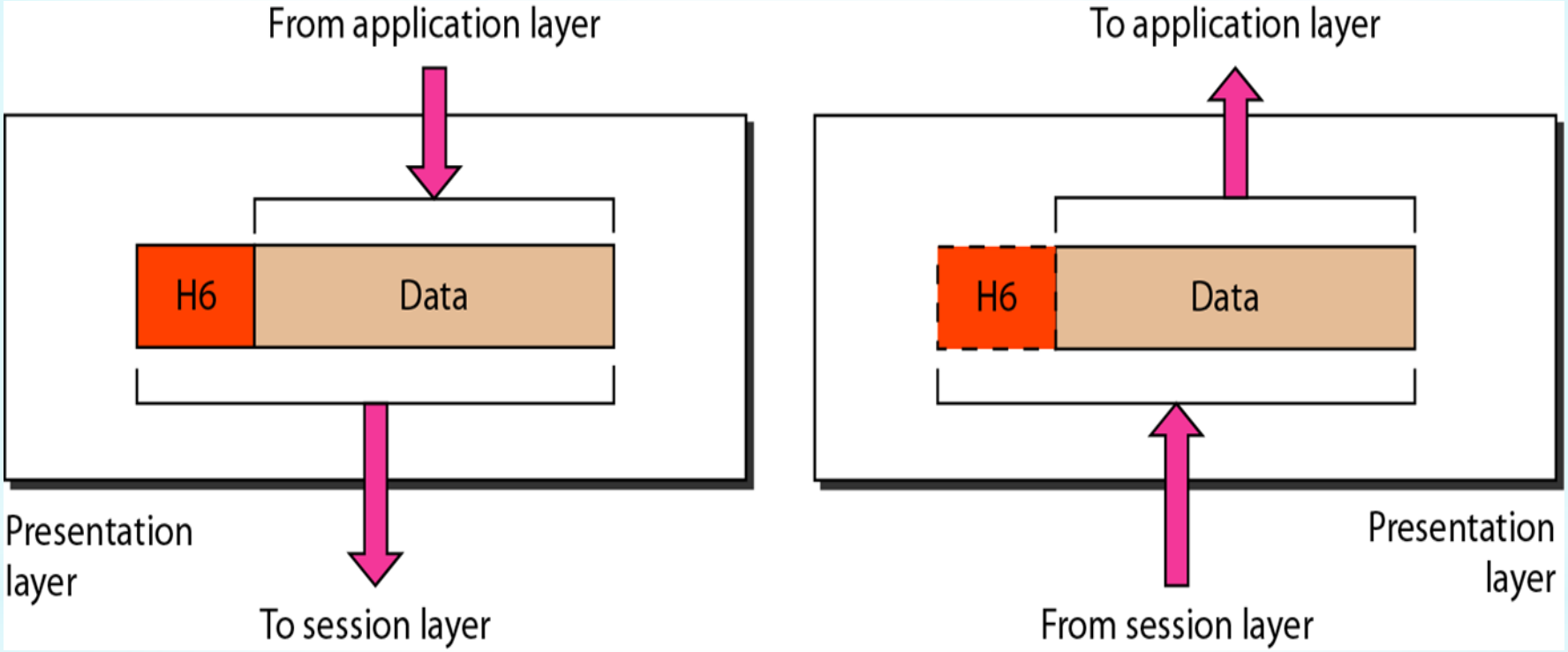


Session layer



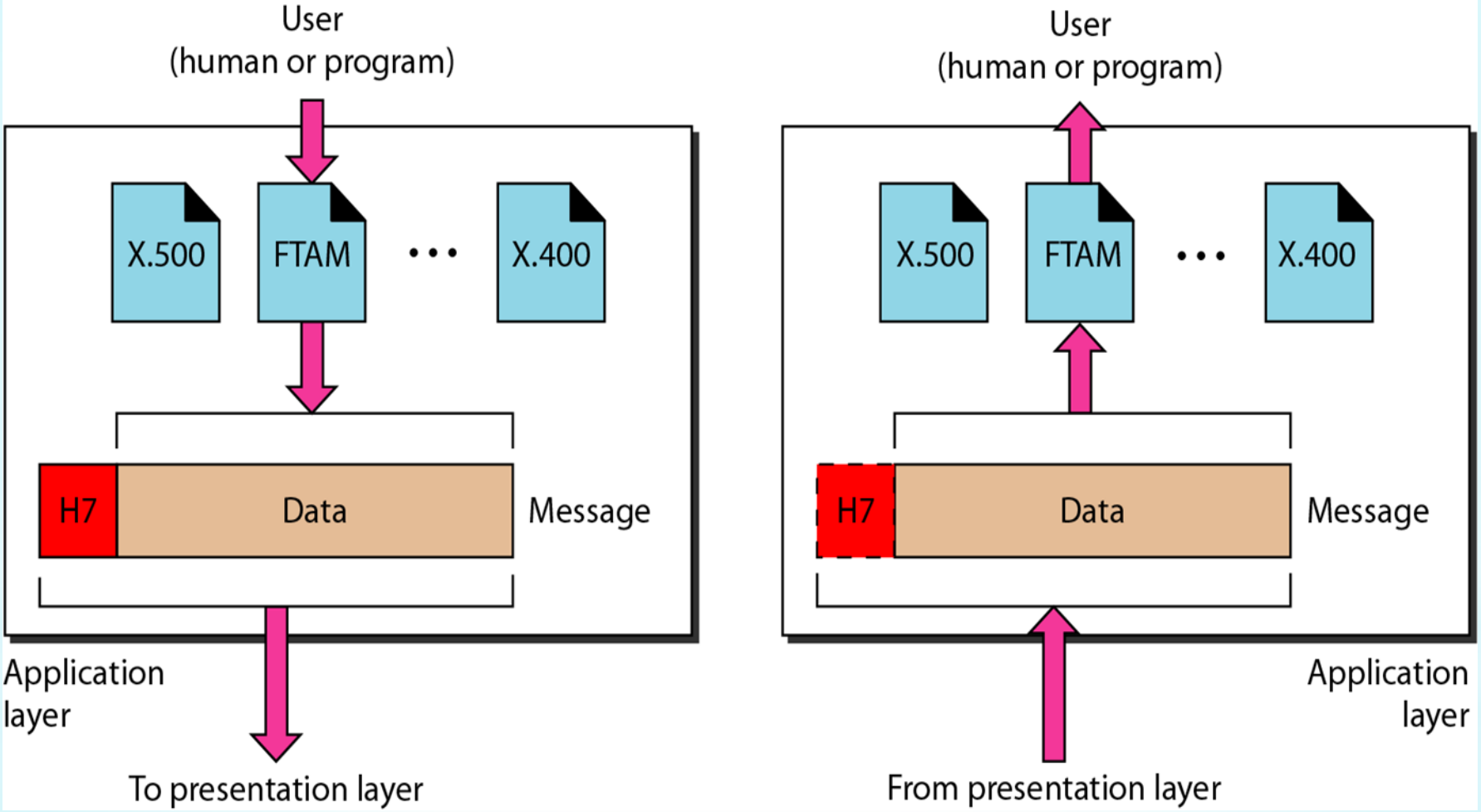
The session layer is responsible for dialog control and synchronization.

Presentation layer



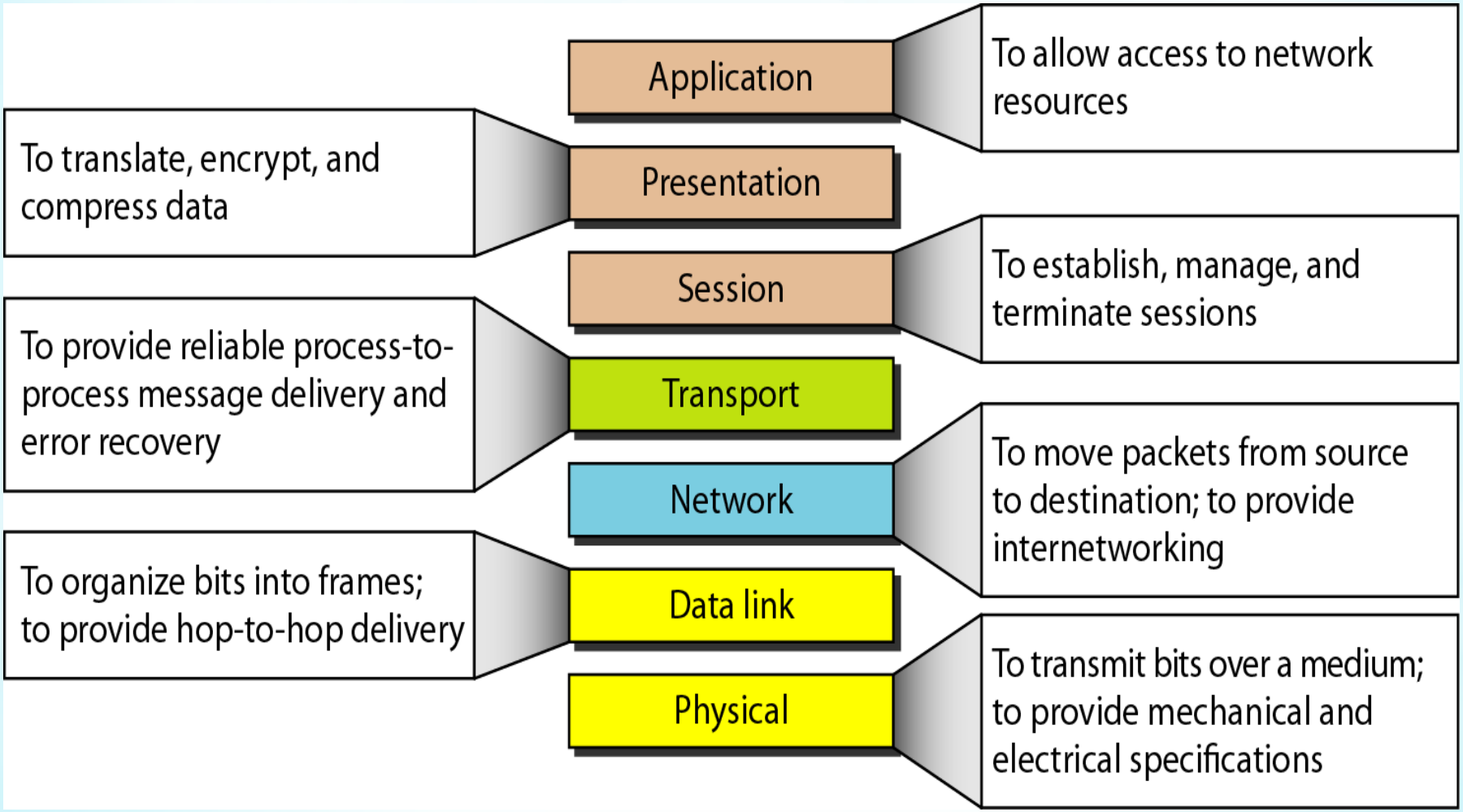
The presentation layer is responsible for translation, compression, and encryption.

Application layer



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

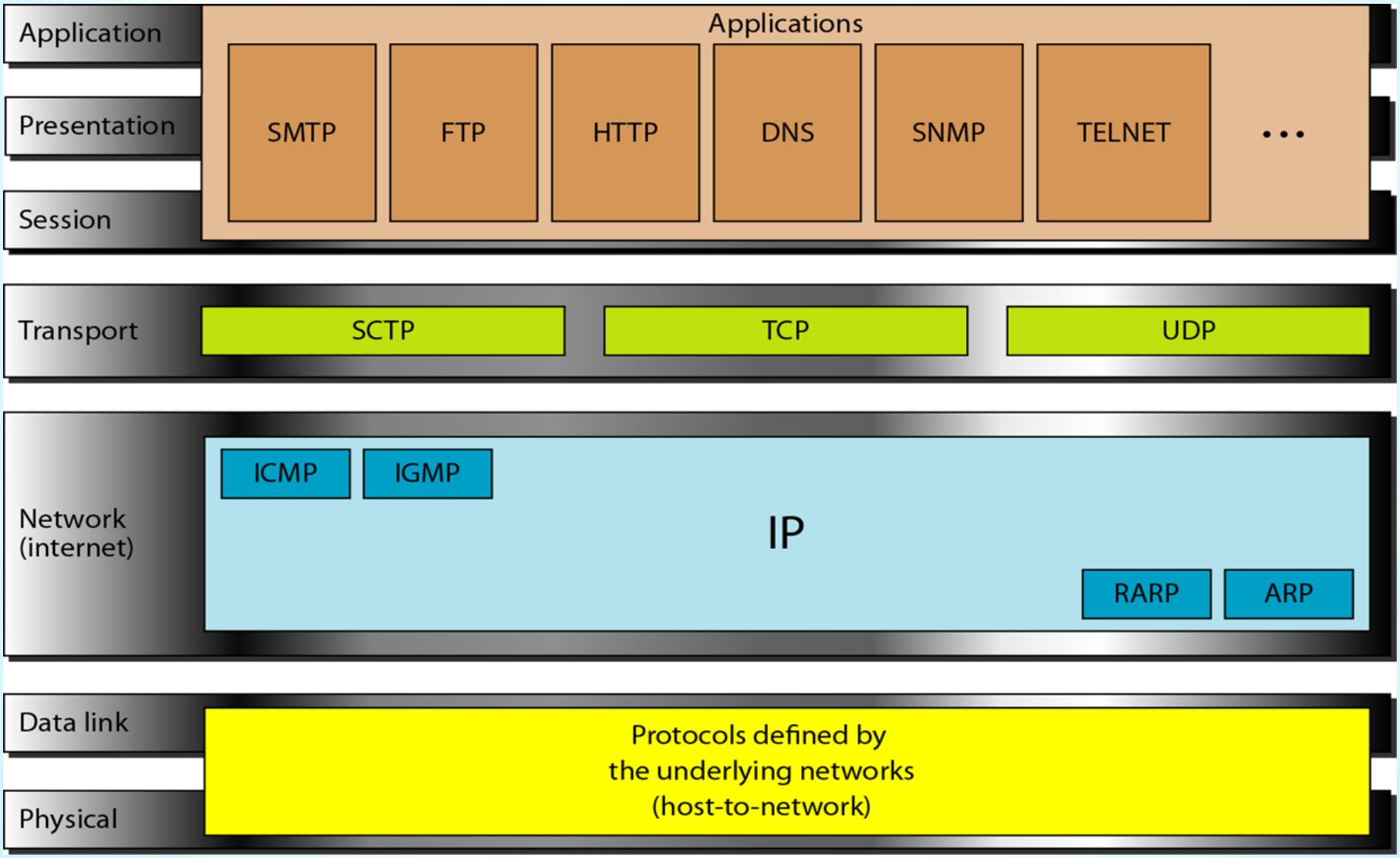
Summary


Application
To allow access to network resources
Presentation
To translate, encrypt, and compress data
Session
To establish, manage, and terminate sessions
Transport
To provide reliable process-to-process message delivery and error recovery
Network
To move packets from source to destination; to provide internetworking
Data link
To organize bits into frames; to provide hop-to-hop delivery
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

TCP/IP Protocol Suite

* Developed by the US Defense Advanced Research Project Agency (DARPA) for its packet switched network (ARPANET)
* Used by the global Internet
* Layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
* No official model but a working one.
* The original TCP/IP protocol suite was defined as having four layers:
  - **host-to-network**
  - **Internet**
  - **Transport**
  - **application**

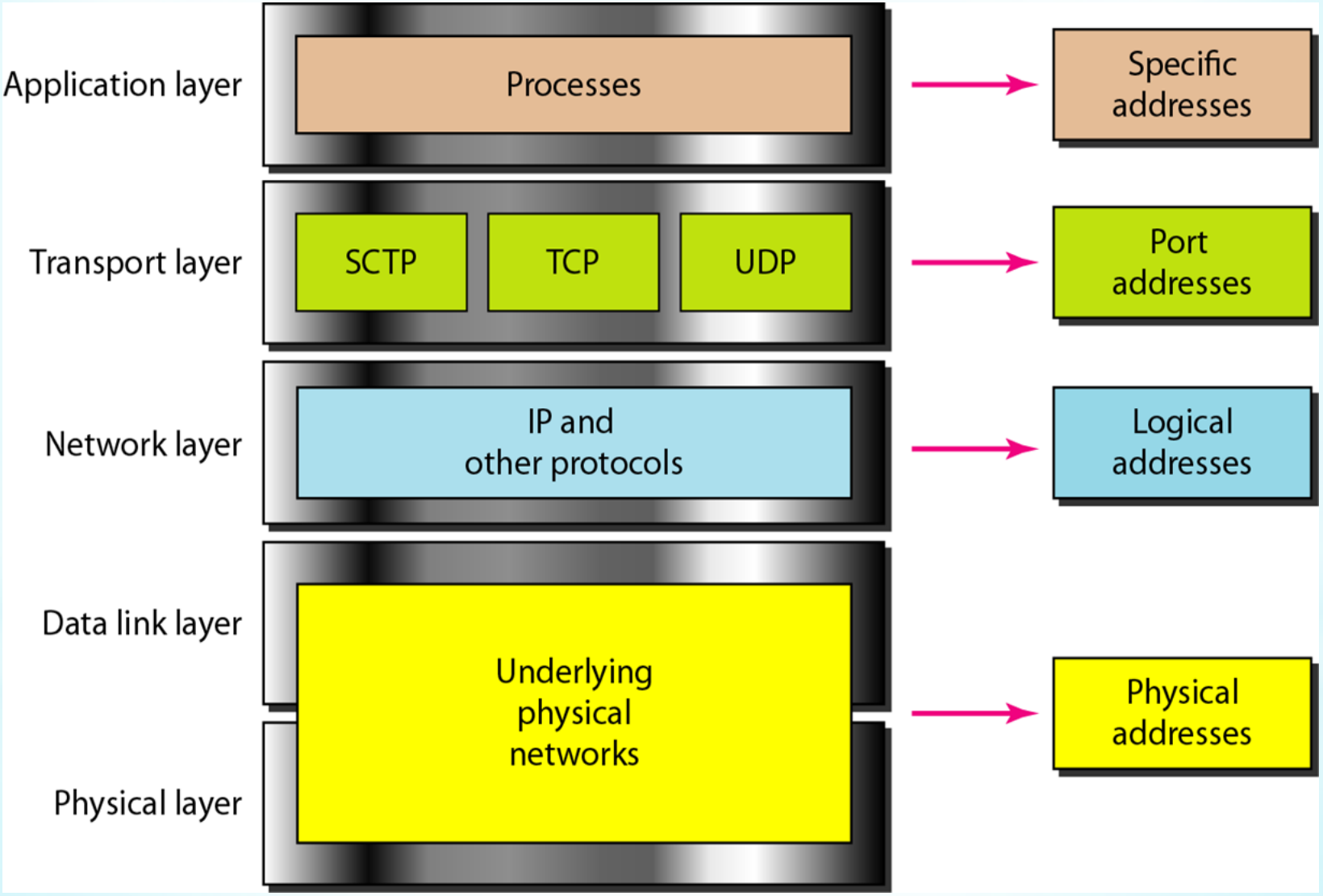
TCP/IP and OSI model



Addressing

* *Four levels of addresses are used in an internet employing the TCP/IP protocols:*
  - Physical Addresses
  - Logical Addresses
  - Port Addresses
  - Specific Addresses

Relationship of layers and addresses in TCP/IP



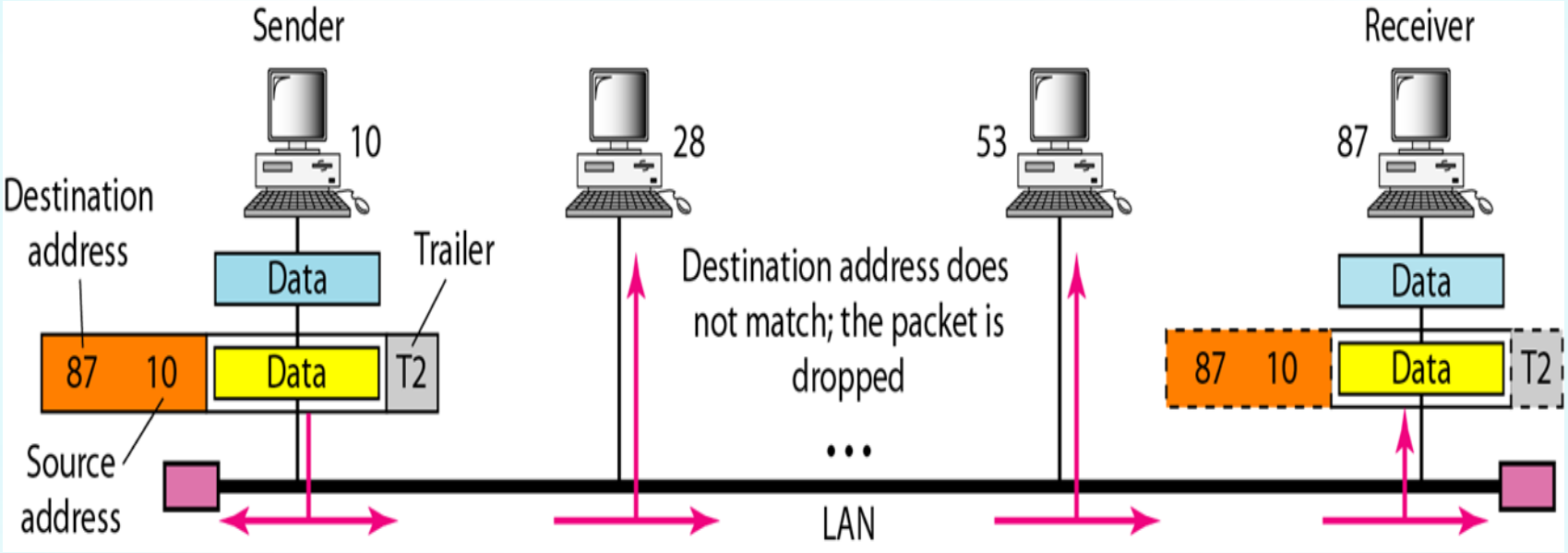
Physical Addresses

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

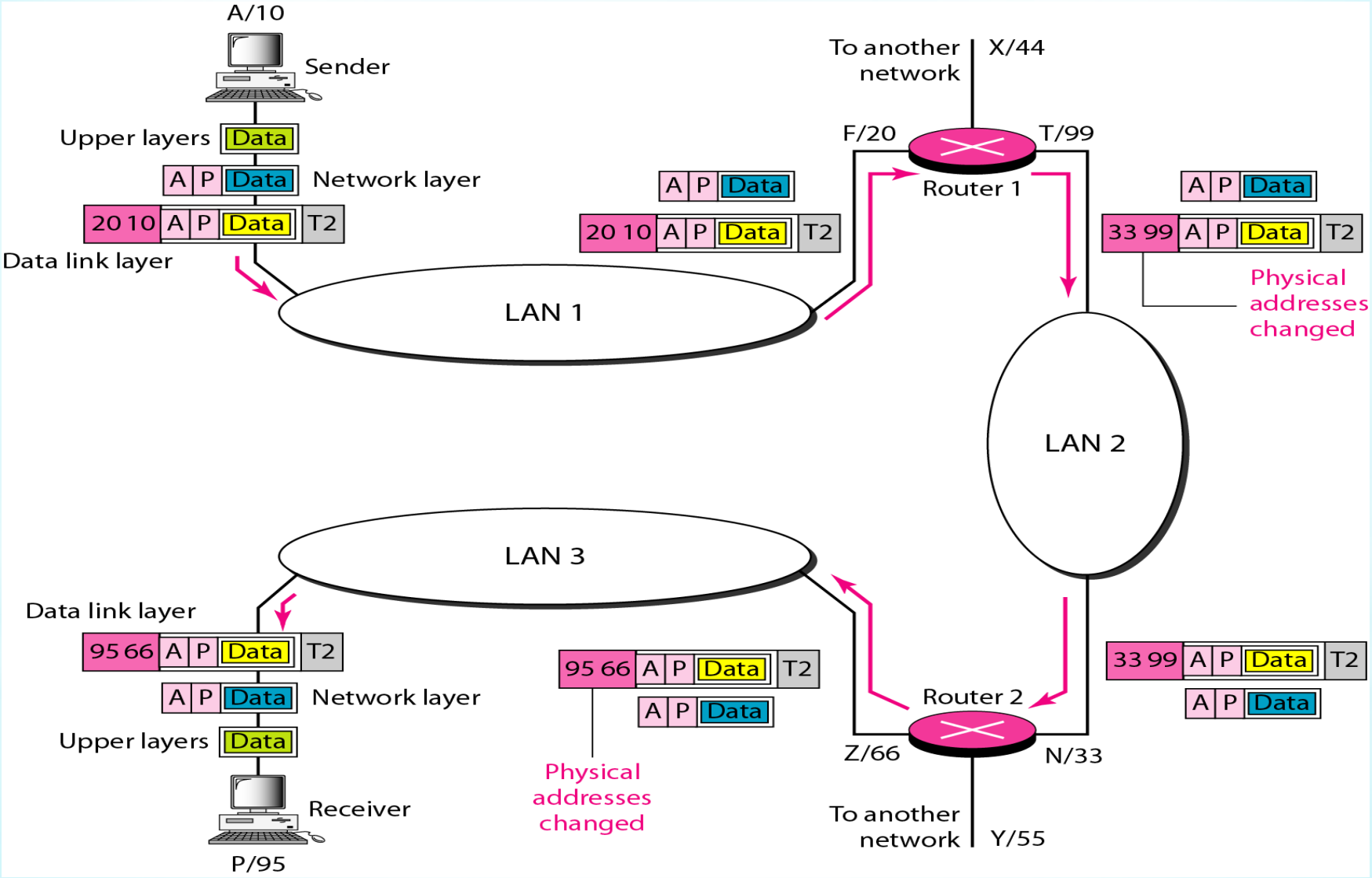
A 6-byte (12 hexadecimal digits) physical address.

Physical Addresses



E.g. 1: In the 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). As the figure shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver.

Logical Addresses



Logical Addresses

E.g. 2:

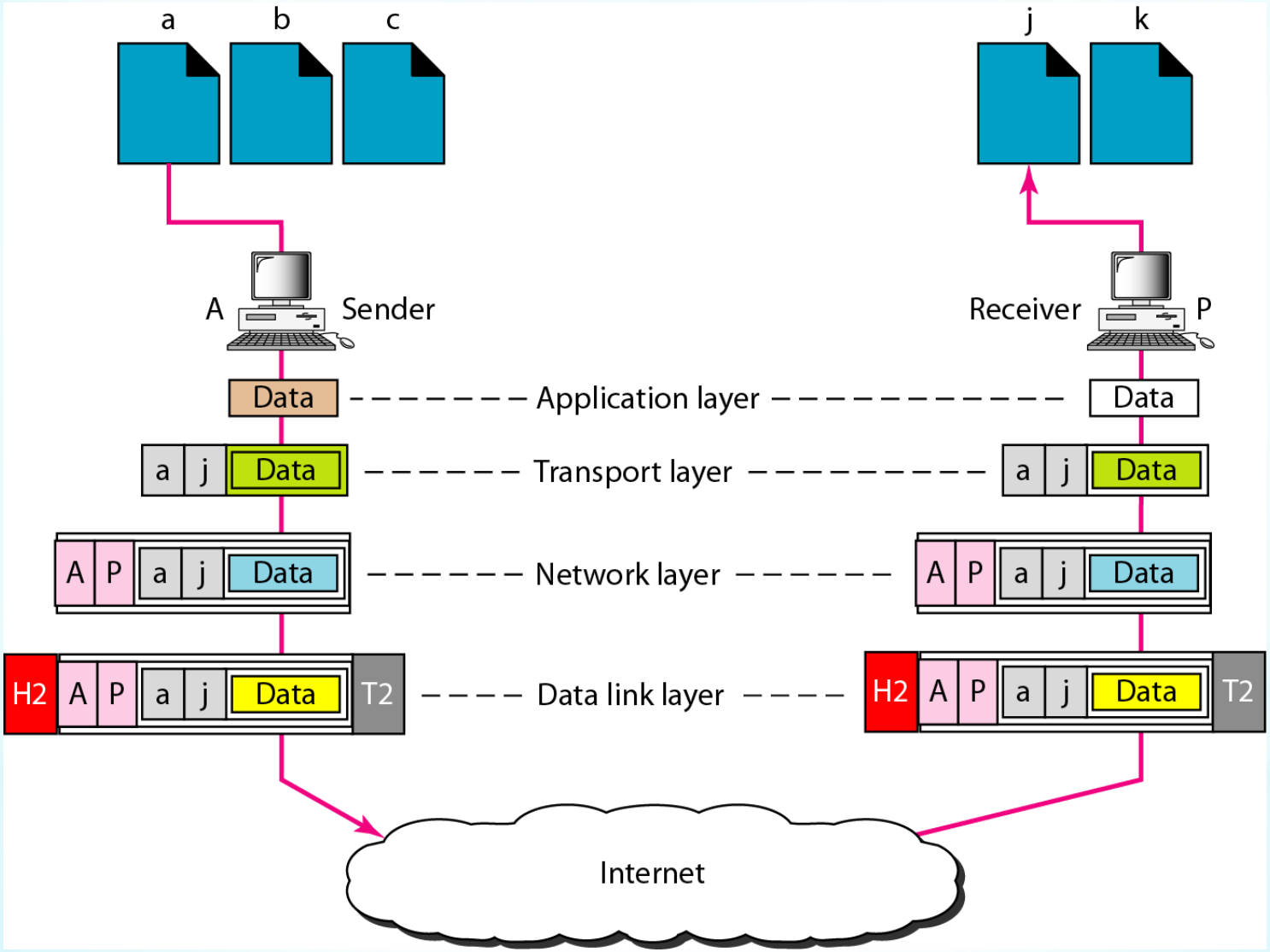
Figure shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection.

Port Addresses

E.g. 3:

Next figure 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.

Port Addresses

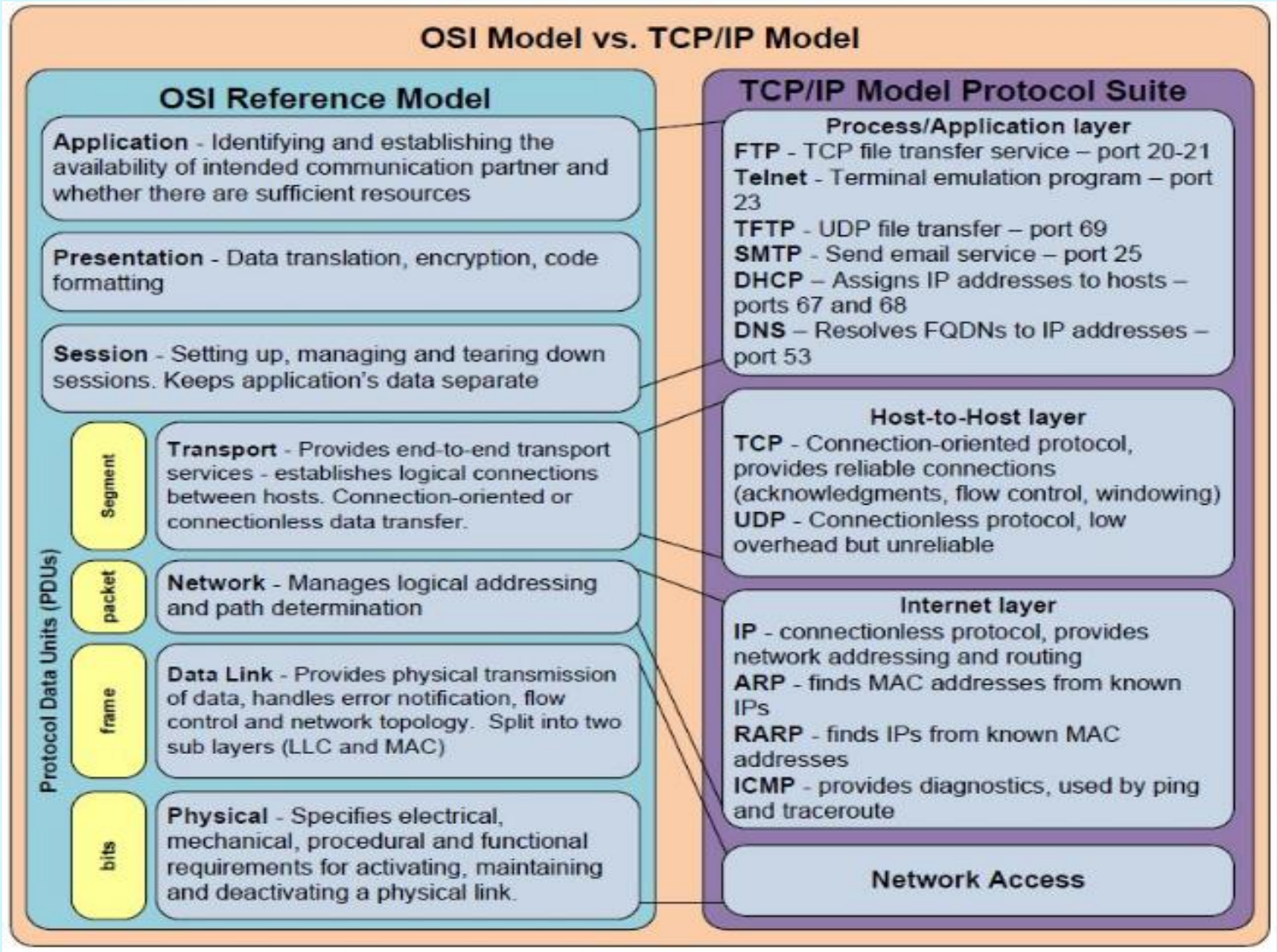


Port Addresses

- The physical addresses will change from hop to hop, but the logical addresses usually remain the same.
- A port address is a 16-bit address represented by one decimal number.

Table: protocol data unit (PDU) being processed in different layers.

Model Type	OSI Layers	Protocol Data Unit (PDU)	TCP/IP Layers
Host Layers	Application Layer	Data	Application Layer
	Presentation Layer		Session Layer
	Session Layer		Application
	Transport Layer	Segment (TCP) / Datagram (UDP)	Transport Layer
Media Layers	Network Layer	Packet	Internet Layer
	Data Link Layer	Frame	Network Access Layer
	Physical Layer	Bit	


OSI Model vs. TCP/IP Model
OSI Reference Model
Application - Identifying and establishing the availability of intended communication partner and whether there are sufficient resources
Presentation - Data translation, encryption, code formatting
Session - Setting up, managing and tearing down sessions. Keeps application's data separate
Protocol Data Units (PDUs)
Segment
Transport - Provides end-to-end transport services - establishes logical connections between hosts. Connection-oriented or connectionless data transfer.
packet
Network - Manages logical addressing and path determination
frame
Data Link - Provides physical transmission of data, handles error notification, flow control and network topology. Split into two sub layers (LLC and MAC)
bits
Physical - Specifies electrical, mechanical, procedural and functional requirements for activating, maintaining and deactivating a physical link.
TCP/IP Model Protocol Suite
Process/Application layer
FTP - TCP file transfer service – port 20-21
Telnet - Terminal emulation program – port 23
TFTP - UDP file transfer – port 69
SMTP - Send email service – port 25
DHCP – Assigns IP addresses to hosts – ports 67 and 68
DNS – Resolves FQDNs to IP addresses – port 53
Host-to-Host layer
TCP - Connection-oriented protocol, provides reliable connections (acknowledgments, flow control, windowing)
UDP - Connectionless protocol, low overhead but unreliable
Internet layer
IP - connectionless protocol, provides network addressing and routing
ARP - finds MAC addresses from known IPs
RARP - finds IPs from known MAC addresses
ICMP - provides diagnostics, used by ping and traceroute
Network Access

OSI MODEL	TCP/IP MODEL
Contains 7 Layers	Contains 4 Layers
Uses Strict Layering resulting in vertical layers.	Uses Loose Layering resulting in horizontal layers.
Supports both connectionless & connection-oriented communication in the Network layer, but only connection-oriented communication in Transport Layer	Supports only connectionless communication in the Network layer, but both connectionless & connection-oriented communication in Transport Layer
It distinguishes between Service, Interface and Protocol.	Does not clearly distinguish between Service, Interface and Protocol.
Protocols are better hidden and can be replaced relatively easily as technology changes (No transparency)	Protocols are not hidden and thus cannot be replaced easily. (Transparency) Replacing IP by a substantially different protocol would be virtually impossible
OSI reference model was devised before the corresponding protocols were designed.	The protocols came first and the model was a description of the existing protocols

Direction of Data flow

Simplex is one direction.

Example: data movement from keyboard to CPU.

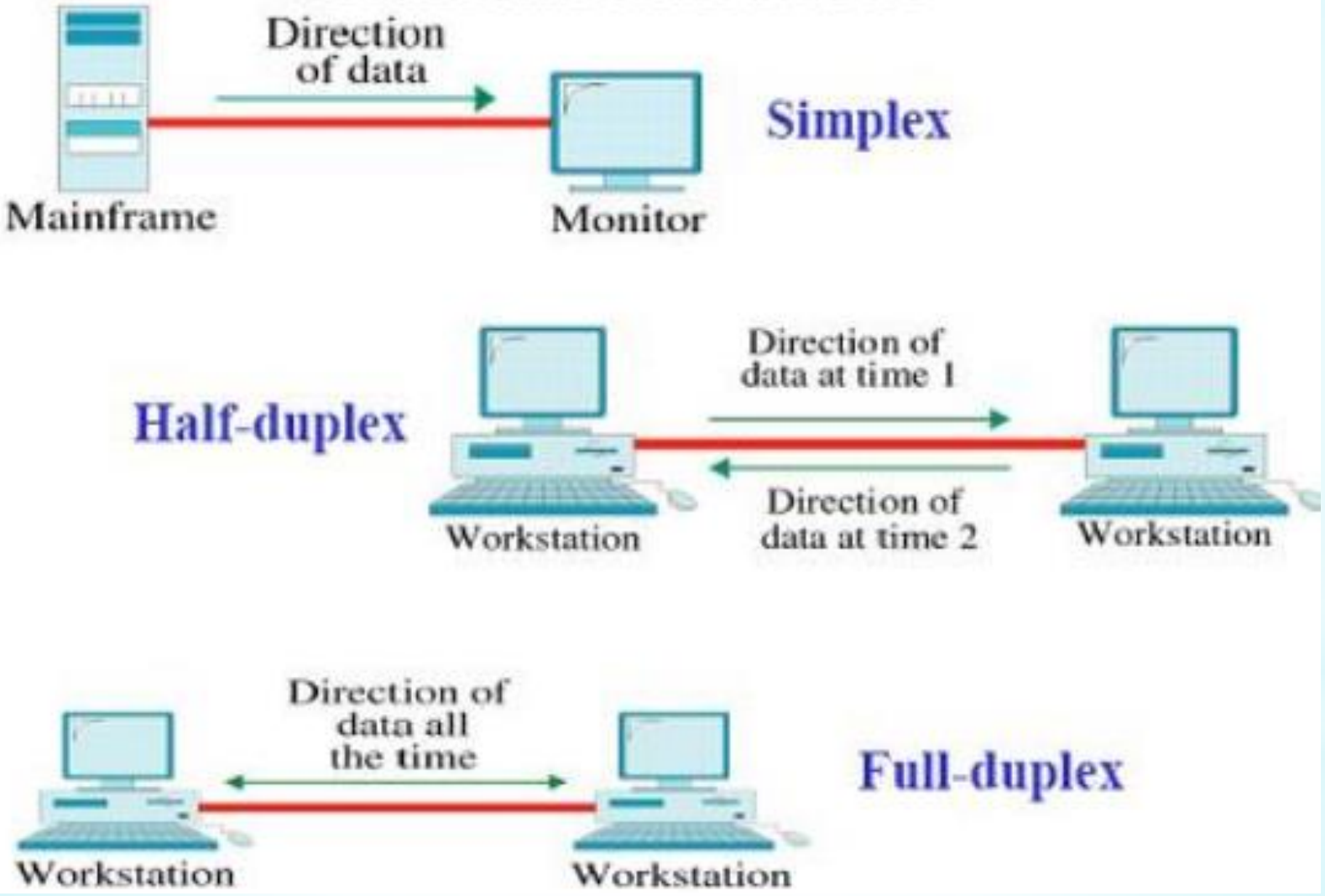
Half-Duplex allows only one direction data flow at a time.

Example: Railroads since it's cheaper to lay a single track. A dispatcher will hold a train up at one end of the single track until a train going the other direction goes through.

Full-Duplex allows data to flow in both directions simultaneously.

Example: Two-lane highway. In some cases, where traffic is heavy enough, a railroad will decide to lay a double track to allow trains to pass in both directions.

Transmission Mode



LAN, MAN, WAN

LAN (local area network) is a group of computers and network devices connected together, usually within the same building. By definition, the connections must be high speed and relatively inexpensive (e.g., token ring or Ethernet).

E.g. all computers connected in a department.

MAN (metropolitan area network) is a larger network that usually spans several buildings in the same city or town. Examples of a MAN are the part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

WAN (wide area network), in comparison to a MAN, is not restricted to a geographical location, although it might be confined within the bounds of a state or country. A WAN connects several LANs, and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive. The Internet is an example of a worldwide public WAN.

BASIS OF COMPARISON	LAN	MAN	WAN
Expands to	Local Area Network	Metropolitan Area Network	Wide Area Network
Meaning	A network that connects a group of computers in a small geographical area.	It covers relatively large region such as cities, towns.	It spans large locality and connects countries together. Example Internet.
Ownership of Network	Private	Private or Public	Private or Public
Design and maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long
Speed	High	Moderate	Low
Fault Tolerance	More Tolerant	Less Tolerant	Less Tolerant
Congestion	Less	More	More
Used for	College, School, Hospital.	Small towns, City.	Country/Continent.

Network Topologies

* Bus
* Ring
* Star
* Tree
* Mesh

Bus Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.

* **Features:**
* It transmits data only in one direction.
* Every device is connected to a single cable

Advantage:

* It is cost effective.
* Cable required is least compared to other network topology.
* Used in small networks.
* It is easy to understand.
* Easy to expand joining two cables together.

Bus Topology

Disadvantage:

* Cables fails then whole network fails.
* If network traffic is heavy or nodes are more the performance of the network decreases.
* Cable has a limited length.
* It is slower than the ring topology.

Ring Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

Features of Ring Topology

* A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
* The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
* In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
* Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

* Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
* Cheap to install and expand

Ring Topology

Disadvantages of Ring Topology

* Troubleshooting is difficult in ring topology.
* Adding or deleting the computers disturbs the network activity.
* Failure of one computer disturbs the whole network.

STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

Features of Star Topology

* Every node has its own dedicated connection to the hub.
* Hub acts as a repeater for data flow.
* Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

* Fast performance with few nodes and low network traffic.
* Hub can be upgraded easily.
* Easy to troubleshoot.
* Easy to setup and modify.
* Only that node is affected which has failed, rest of the nodes can work smoothly.

Star Topology

Disadvantages of Star Topology

* Cost of installation is high.
* Expensive to use.
* If the hub fails then the whole network is stopped because all the nodes depend on the hub.
* Performance is based on the hub that is it depends on its capacity

Mesh Topology

* It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.
* There are two techniques to transmit data over the Mesh topology, they are :
  - Routing
  - Flooding

* **Features of Mesh Topology**
  - Fully connected.
  - Robust.
  - Not flexible.

Mesh Topology

* **Advantages of Mesh Topology**
  - Each connection can carry its own data load.
  - It is robust.
  - Fault is diagnosed easily.
  - Provides security and privacy.
* **Disadvantages of Mesh Topology**
  - Installation and configuration is difficult.
  - Cabling cost is more.
  - Bulk wiring is required.

Tree Topology

* It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.
* **Features of Tree Topology**
  - Ideal if workstations are located in groups.
  - Used in Wide Area Network.

Tree Topology

* **Advantages of Tree Topology**
  - Extension of bus and star topologies.
  - Expansion of nodes is possible and easy.
  - Easily managed and maintained.
  - Error detection is easily done.
* **Disadvantages of Tree Topology**
  - Heavily cabled.
  - Costly.
  - If more nodes are added maintenance is difficult.
  - Central hub fails, network fails.

Hybrid Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

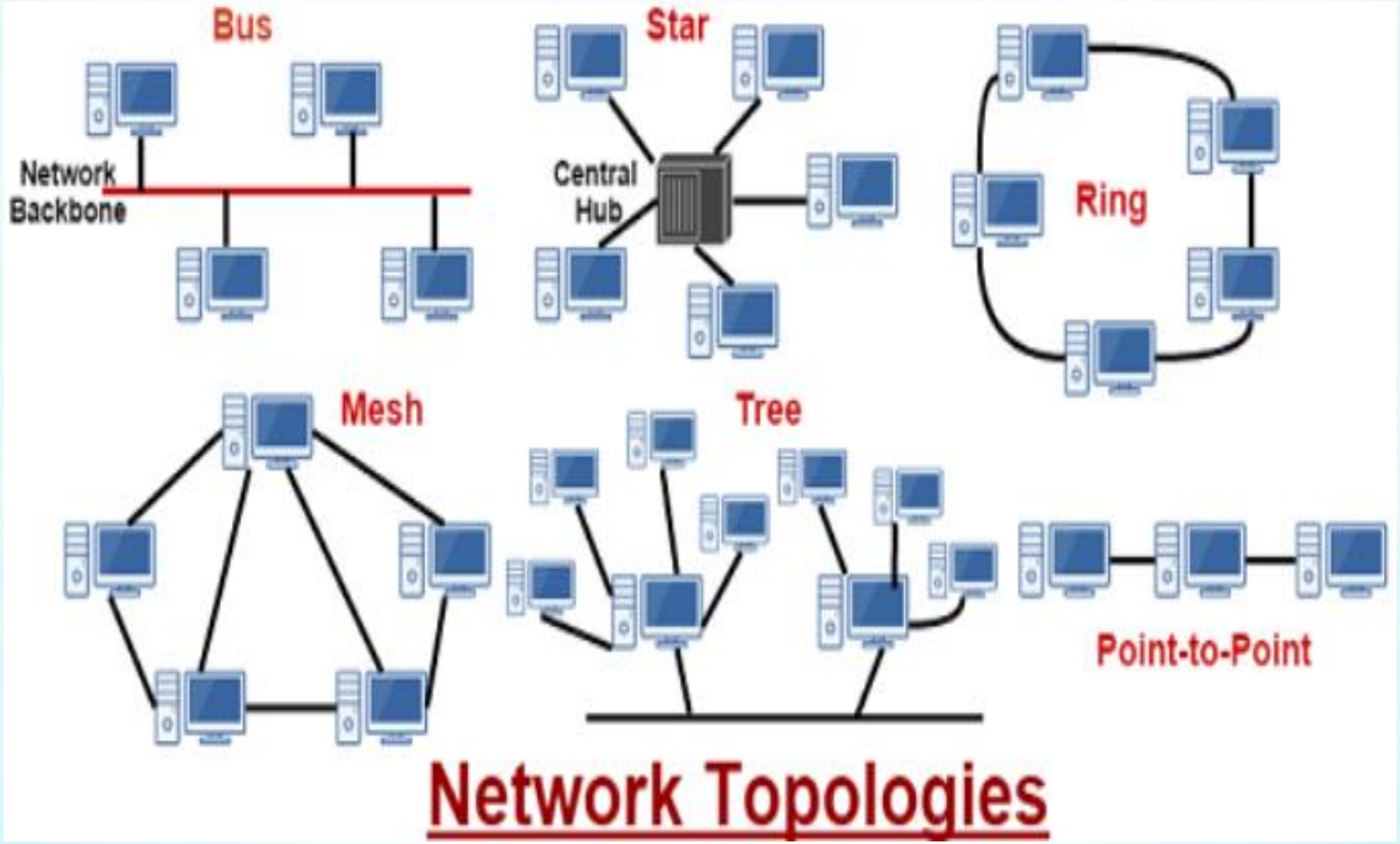
* **Features of Hybrid Topology**
  - It is a combination of two or topologies
  - Inherits the advantages and disadvantages of the topologies included

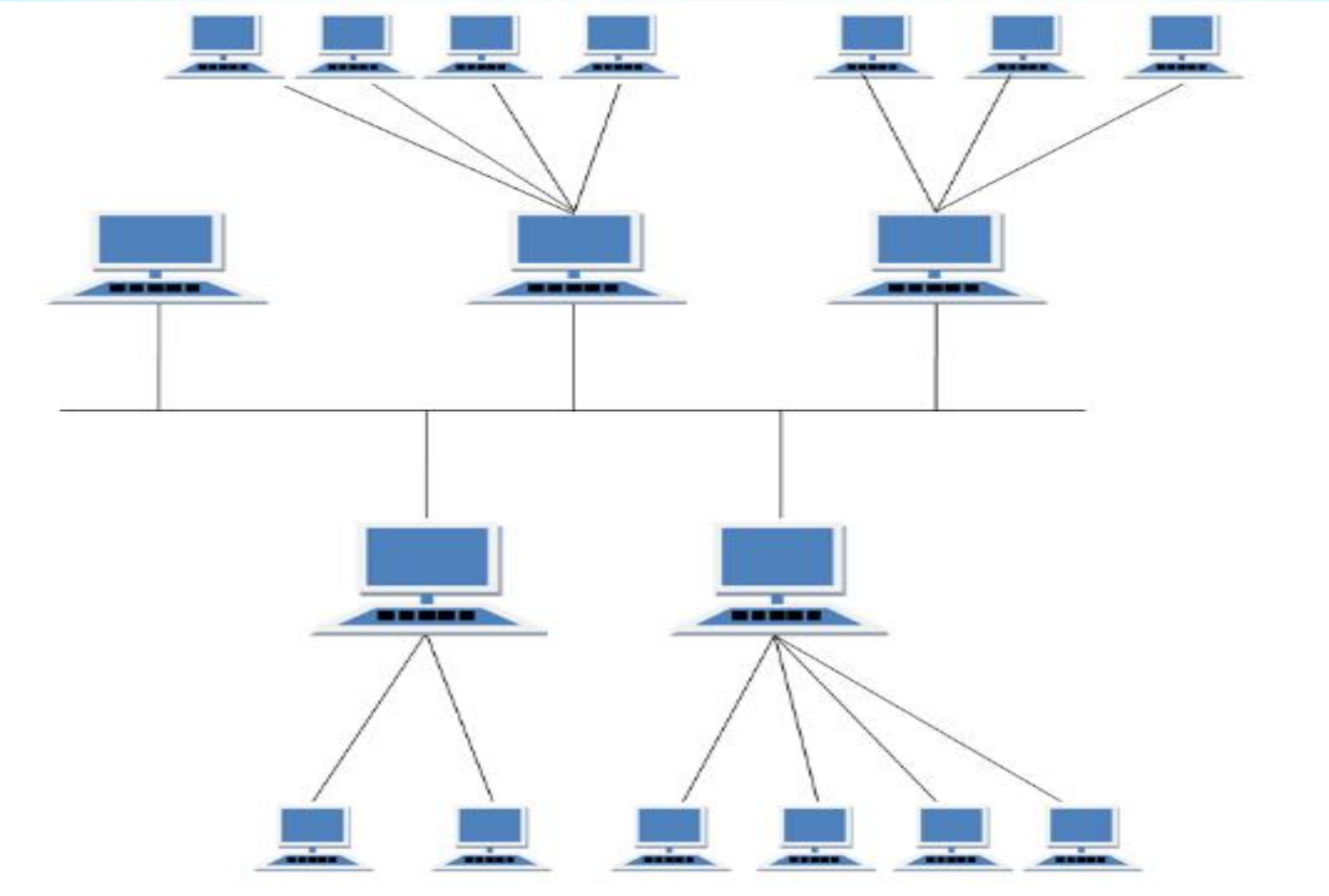
Hybrid Topology

* **Advantages of Hybrid Topology**
  - Reliable as Error detecting and trouble shooting is easy.
  - Effective.
  - Scalable as size can be increased easily.
  - Flexible.

* **Disadvantages of Hybrid Topology**
  - Complex in design.
  - Costly.

Topologies


Bus
Network
Backbone
Star
Central
Hub
Ring
Mesh
Tree
Point-to-Point
Network Topologies



Hybrid Topology

END