Computer Communication Architecture

Unit-4

(LH 3)

Topics

- Overview of Protocols and Standards
- OSI Reference Model
- TCP/IP Models and comparison with OSI

Overview of Protocols and Standards

- Protocols
- A Protocol is *a set of rules that governs data communications*.
- For communication to occur, the entities must agree on a protocol.
- The key elements of a Protocol are:
  - Syntax
  - Semantics
  - Timing

Key elements of protocol

- **Syntax**
  - Structure or format of the data
  - Indicates how to read the bits-field delineation
- **Semantics**
  - Interprets the meaning of the bits
  - Knows which fields define what action
- **Timing**
  - When data should be sent and what
  - Speed at which data should be sent or speed at which it is being received

Standards

- A formalized regulations that must be followed.
- Are guidelines that explain to all IT stakeholders-from device manufacture to software programmers and network administrators-how a particular protocol should operate.
- Defines interoperability between different devices or systems of different vendors.

Data communication Standards

- Data communications standards fall under two categories:

1. De facto
2. De jure

Types of Standards

De facto

- Latin phrase that means *in fact* (literally *by or from fact or convention*)
- Standards that have not been approved by law or organized body, but accepted widely by public or market forces.
- A good example of a de facto standard is the paper clip icon used in e-mail programs to represent an attachment.

De jure

- Latin phrase that means *by law* or *by regulation*
- Standards according to law
- Endorsed by a formal standards organization
- The organization ratifies each standard through its official procedures and gives the standard its stamp of approval.
- ASCII (American Standard Code for Information Interchange), the most common format for text files in computers and on the Internet.

Questions

- Compare de facto and de jure standards.

Standard Organization

- Standards are developed through the cooperation of standards creation committee, forums, and government regulatory agencies.
- A standards organization, sometimes referred to as a standards body, is an organization with authority to endorse official standards for given applications.

Standard Creation Committee

ISO:	International Standards Organization
ITU-T:	International Telecommunications Union-Telecommunication Standards Sector
ANSI:	American National Standards Institute
IEEE:	Institute of Electrical and Electronics Engineers
EIA:	Electronics Industries Association
W3C:	World Wide Web Consortium
OMA:	Open Mobile Alliance
IETF:	Internet Engineering Task Force
IRTF:	Internet Research Task Force
BSI:	British Standards Institution
TIA:	Telecommunication Industry Association

Network Models

- Reflects a design or architecture to accomplish communication between different systems.
- Also referred to as *network stacks* or *protocol suites*
- Examples:
  - TCP/IP
  - OSI-RM
- Usually *consists of layers*

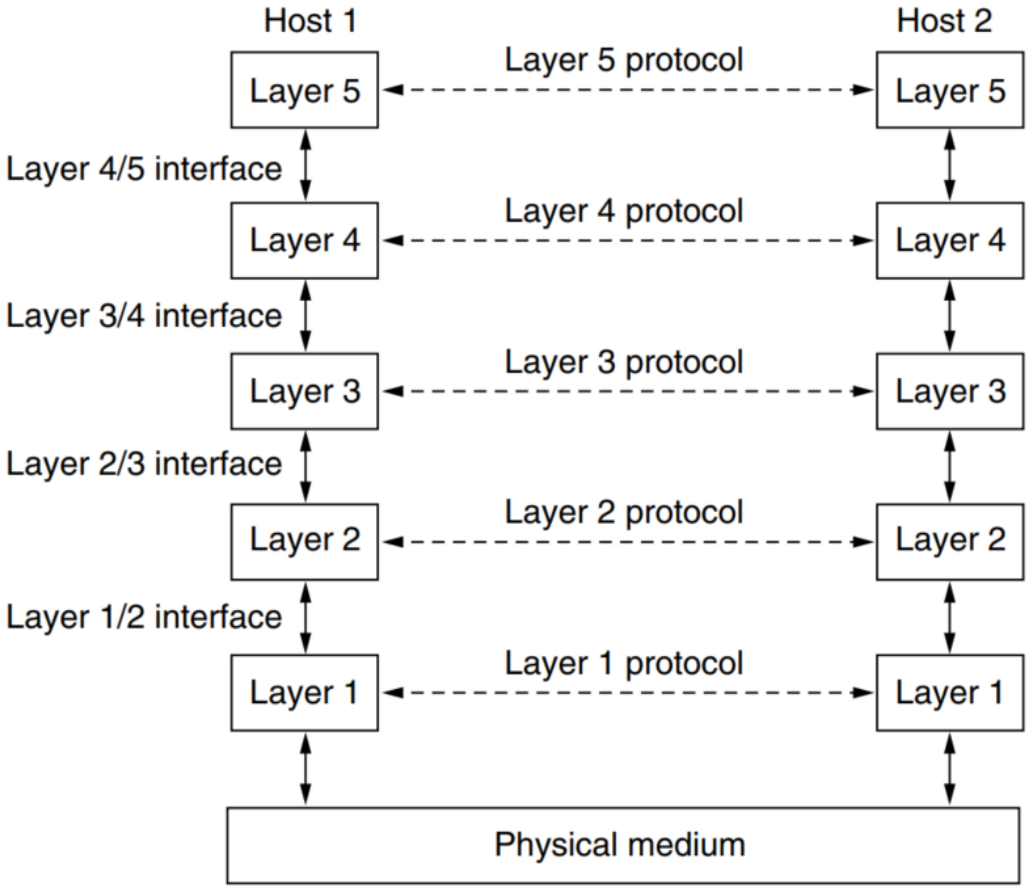
Layered Architecture

- A network model built with layers.
- Each layers implements their specific protocols.
- Each layers has its specific functionality.
- Each layer provides *service* to layer above it.
- Between adjacent layers is an *interface*.
  - *Services* – connection oriented and connectionless.
  - *Interface* – defines which *primitives* and services the lower layer will offer to the upper layer.
  - *Primitives* – operations such as request, indicate, response, confirm.

Layered Architecture

- *To reduce the design complexities, network designer organize the protocols, network hardware and software that implements the protocol in layers*.
- A protocol in one layer perform a certain set of operation on data, the data is then passed to the next layer where another protocol perform different set of operations. i.e. each layer provide certain services to upper layer.
- A protocol layer can be implemented in software, in hardware or in a combination of the two.

Figure: Layered Architecture



Layered Architecture

- The protocol at various layer are called protocol stack.
- The key concept of protocol stack is each n-1 layer provides service to upper layer n.
- These layers communicate with each other by exchanging n-message. These message are called layered-n protocol data unit or n-PDU.
- Between each pair of layer is an interface that define the services the lower layer to upper one.
- Example:
  - the application-to-transport interface defines how application program make use of the transport layers.
  - this interface level would define how a web browser program would talk to TCP/IP transport layers

Protocol Analogy: Sending a Letter

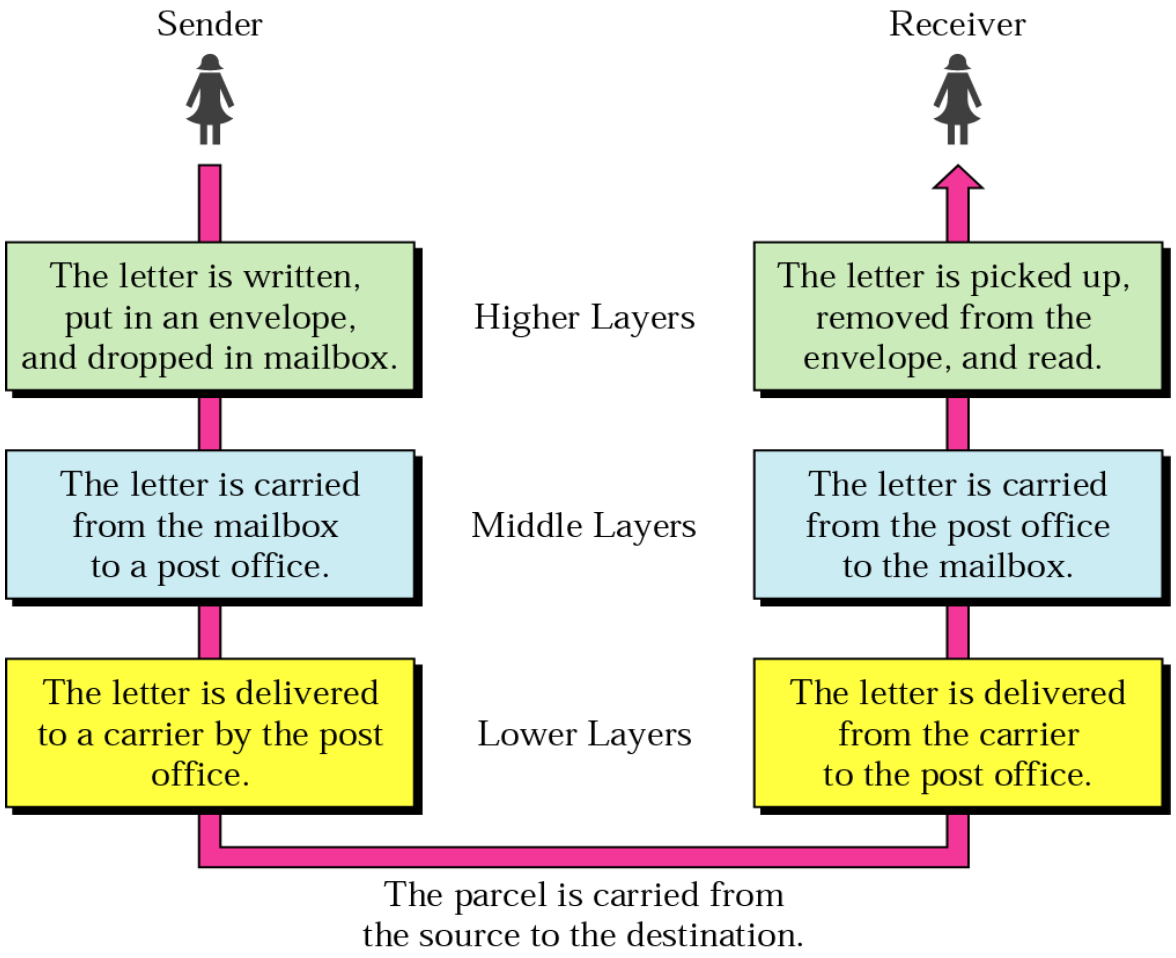


Figure: Protocol Analogy: Organization of Air Travel

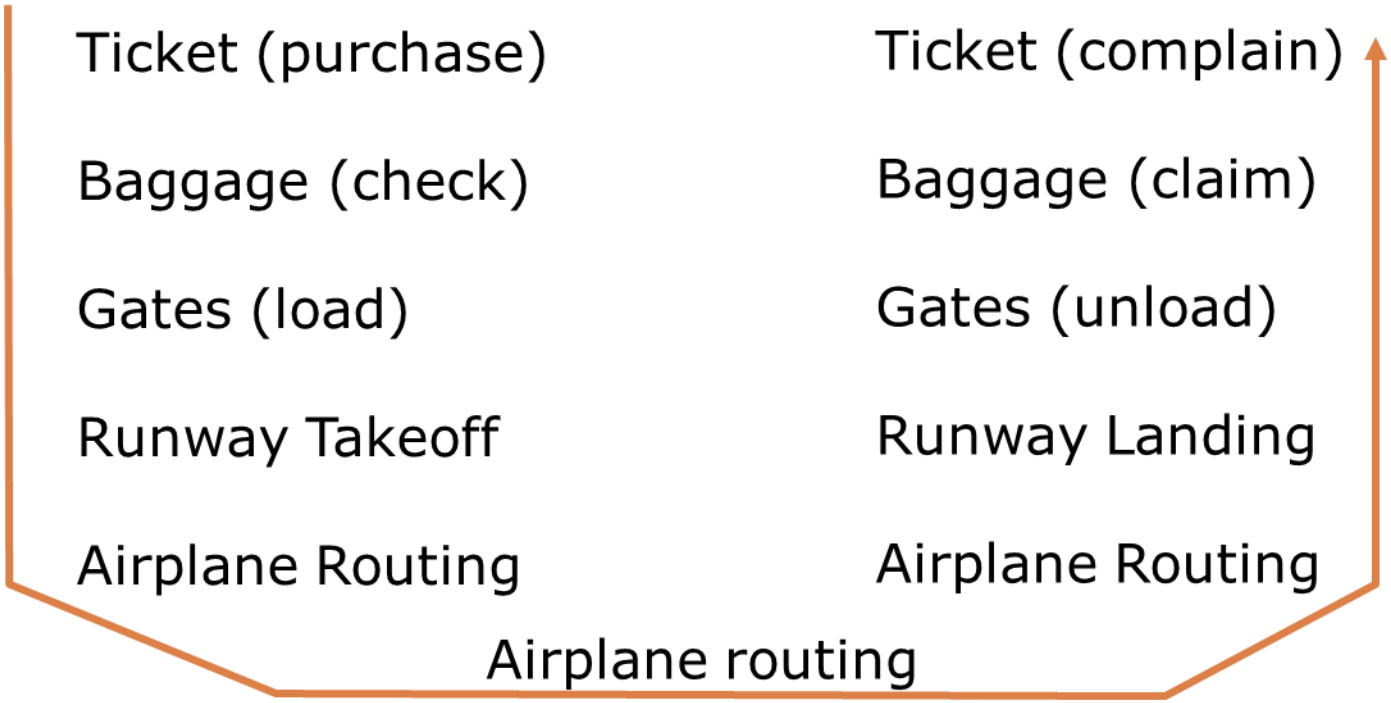
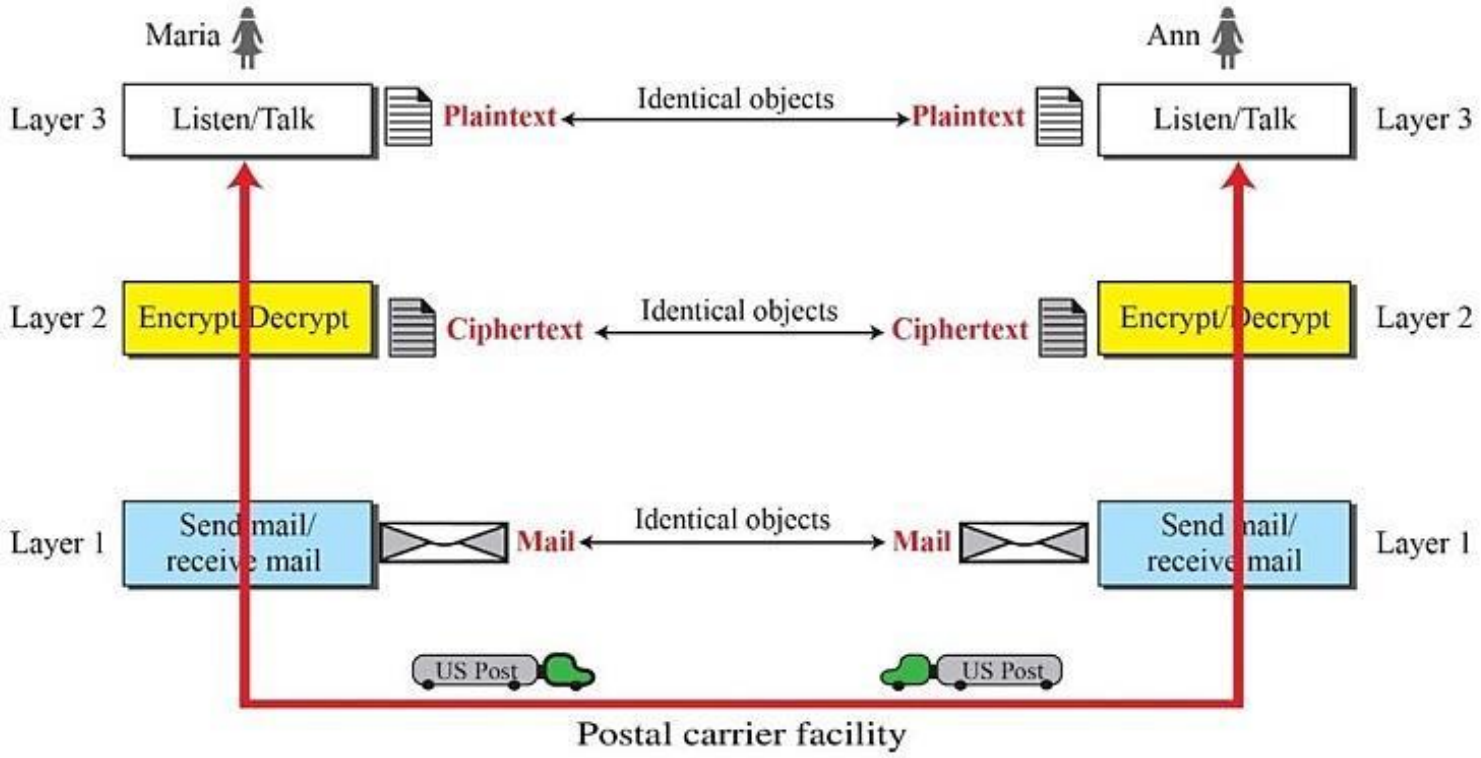


Figure: A single-layer protocol

Figure: A Three-layer Protocol



Reference Model

- A non-implementation framework that provides a clear understanding of the functions and processes necessary for consistent non-proprietary protocol development.
- Example: OSI-RM (Open System Interconnection- Reference Model)

Protocol Model

- Implementation specific frame-work
- Example: TCP/IP protocol suite

Layered Protocol Models

- OSI Reference Model
- TCP/IP Protocol

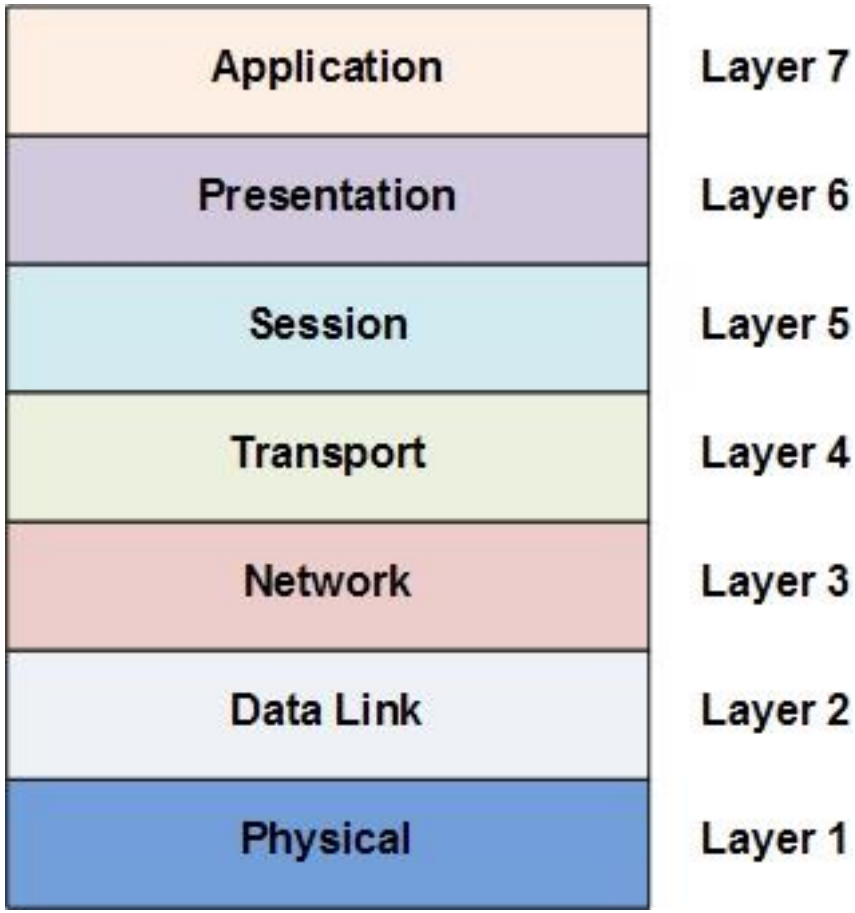
OSI Reference Model

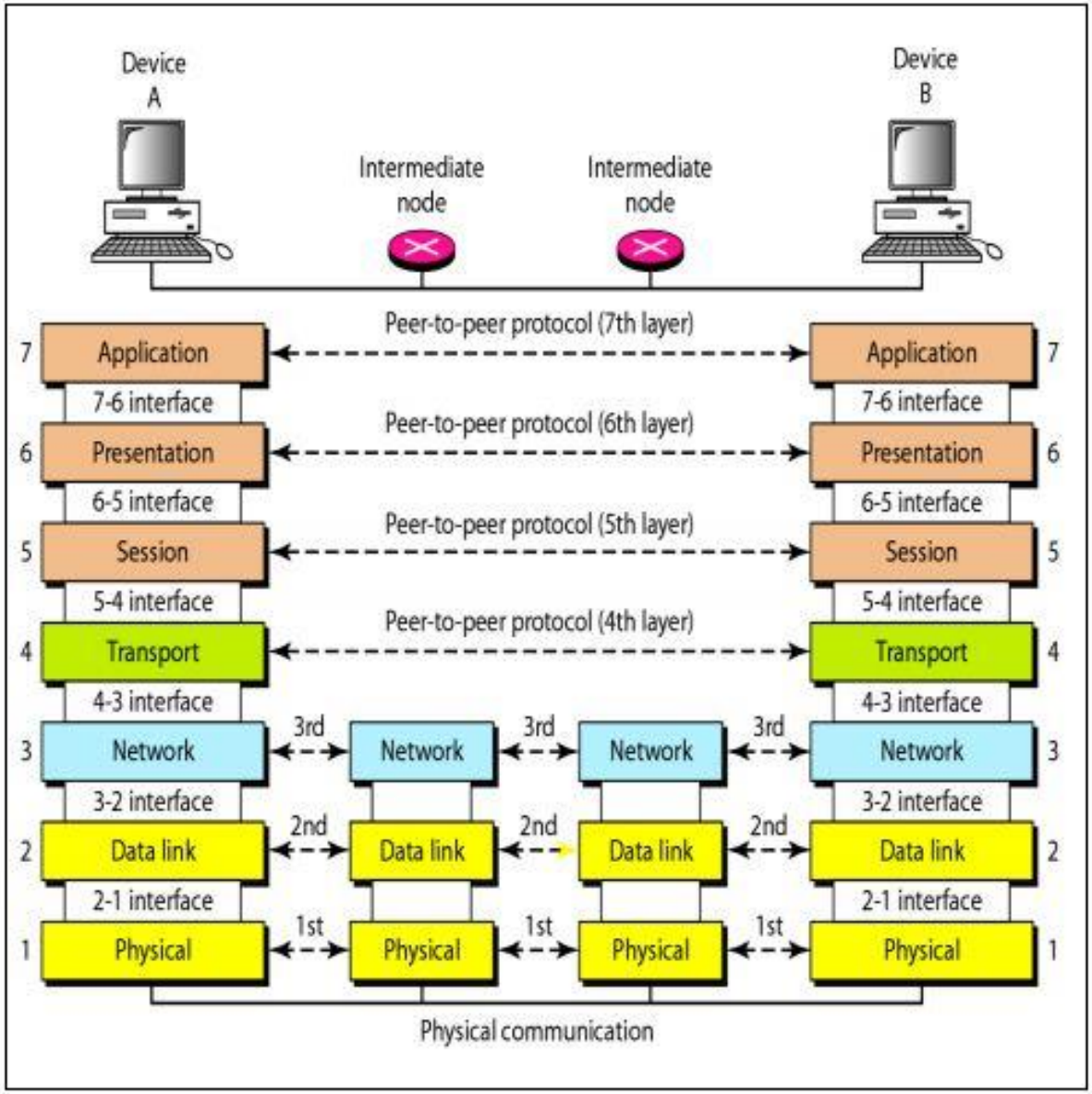
- The Open System Interconnection (OSI) *reference model* is the primary architectural network. It describes how data and network information are communicated from an application on one computer through the network media to an application on another computer.
- It is *theoretical set of protocols* developed to allow systems with different platforms to communicate with each other. Platform could mean hardware, software or operating system.
- **The OSI is not a protocol**; it is a model for understanding and designing a network architecture that is flexible, robust and interporerable.
- The Open Systems Interconnection (OSI) Model was developed by International Organization for standardization (ISO) in 1978 and revised in 1984.
- It is a hierarchical model (layered framework) that groups its processes into 7 layers, each of which defines a part of the process of moving across a network.

Benefits of OSI Model

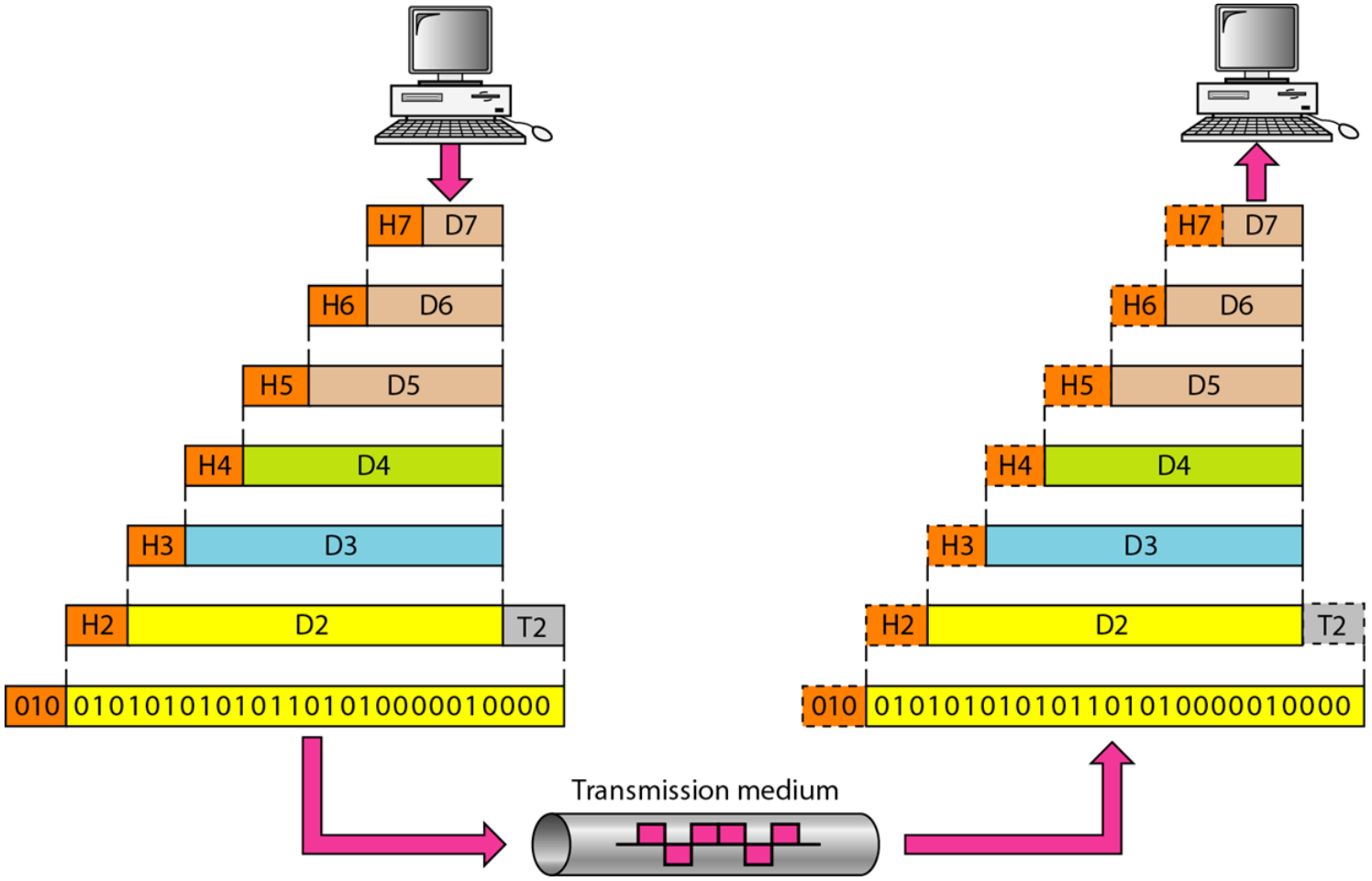
- It breaks network communication into smaller, more manageable parts.
- It standardizes network components to allow multiple vendor development and support.
- It allows different types of network hardware and software to communicate with each other.
- It prevents changes in one layer from affecting other layers.
- It divides network communication into smaller parts to make learning it easier to understand.

The OSI-RM


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


Device A
Device B
Intermediate node
Intermediate node
Peer-to-peer protocol (7th layer)
Peer-to-peer protocol (6th layer)
Peer-to-peer protocol (5th layer)
Peer-to-peer protocol (4th layer)
7 Application
7-6 interface
6 Presentation
6-5 interface
5 Session
5-4 interface
4 Transport
4-3 interface
3 Network
3-2 interface
2 Data link
2-1 interface
1 Physical
3rd
2nd
1st
Physical communication

An exchange using the OSI Model



Encapsulation/De-encapsulation

- The process of moving data between layers of the OSI Model

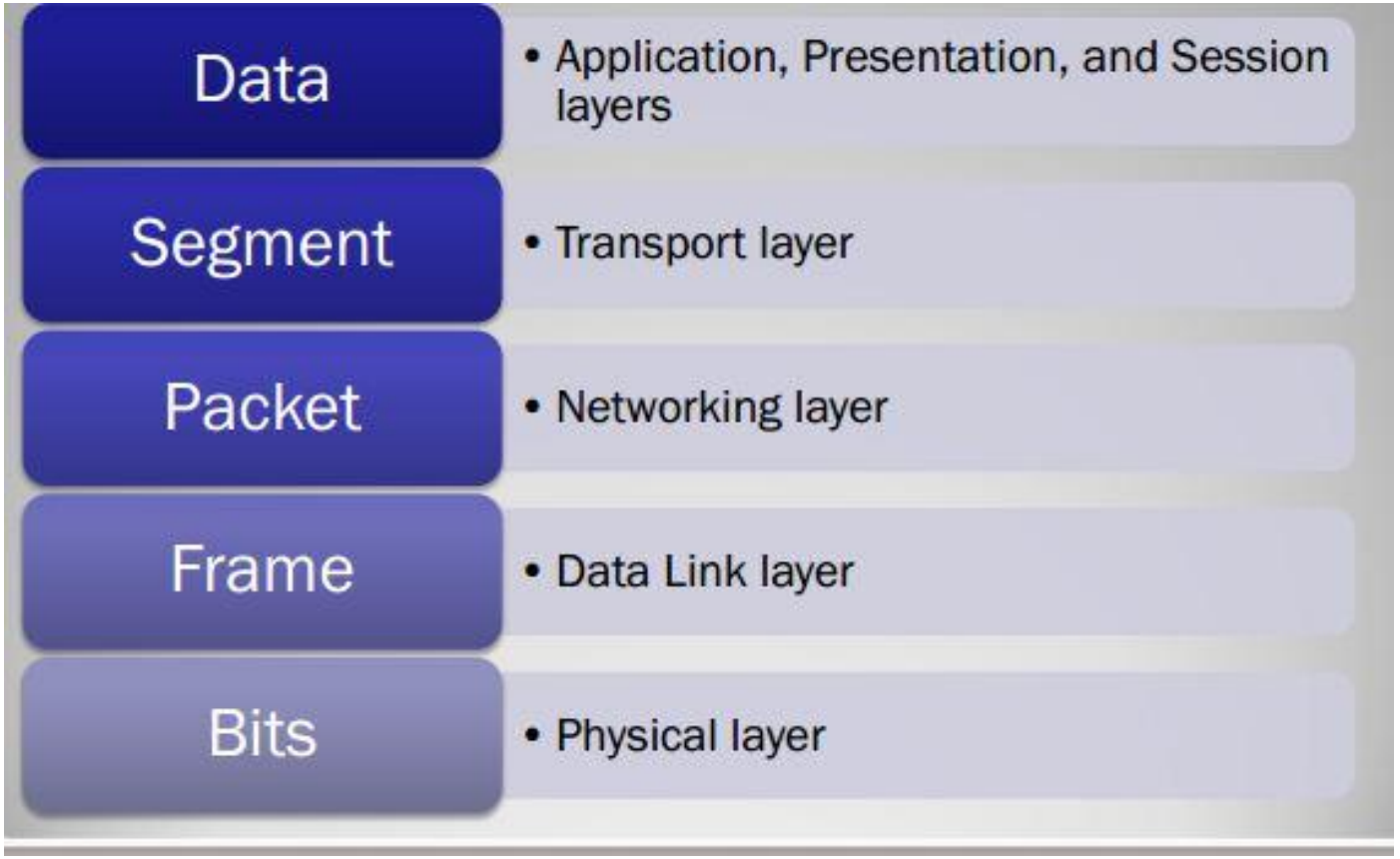
Encapsulation:

Data > segment >packet > frame >bits

De-encapsulation:

Bits > frame >packet > segment> data

How Data is referred in OSI?



Organization of the layers

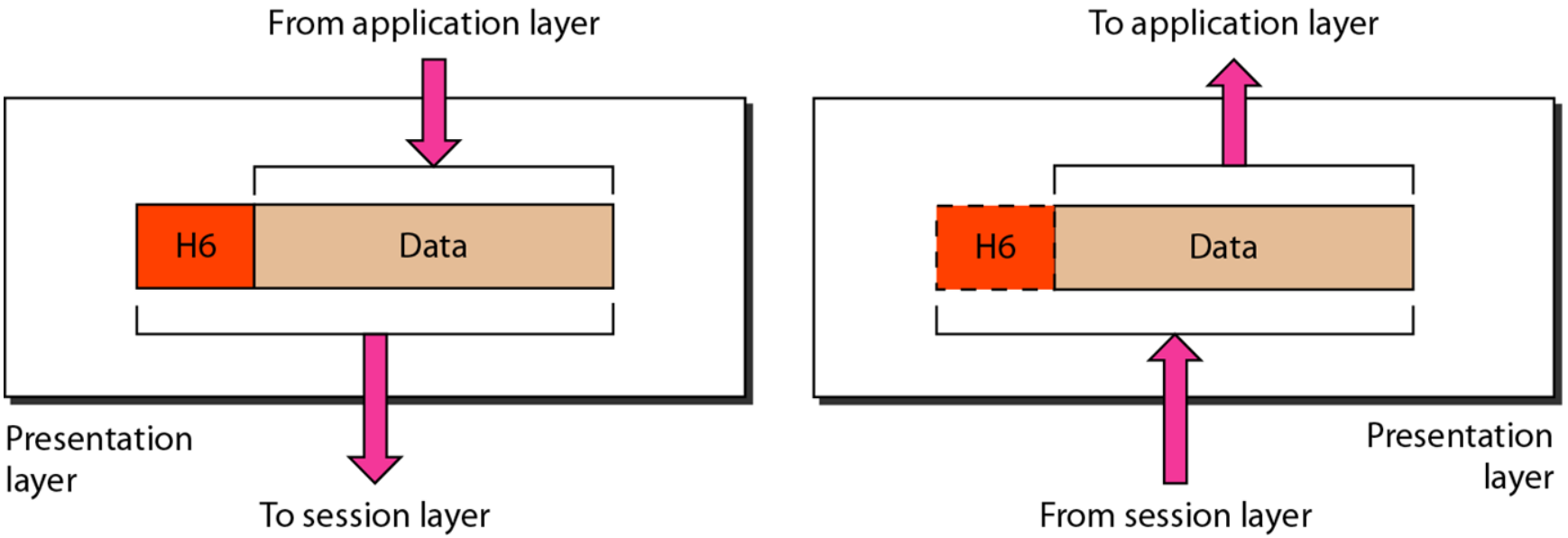
- The top three layers (Application, Presentation and Session) define how the applications within the end stations will communicate with each other and with user.
- The transport layer ensures end-to-end reliable data transmission on a single link.
- The bottom three layer (Network, Data and Physical layers) are user support layer. They allow interoperability among unrelated software systems.

Layer 7: Application Layer

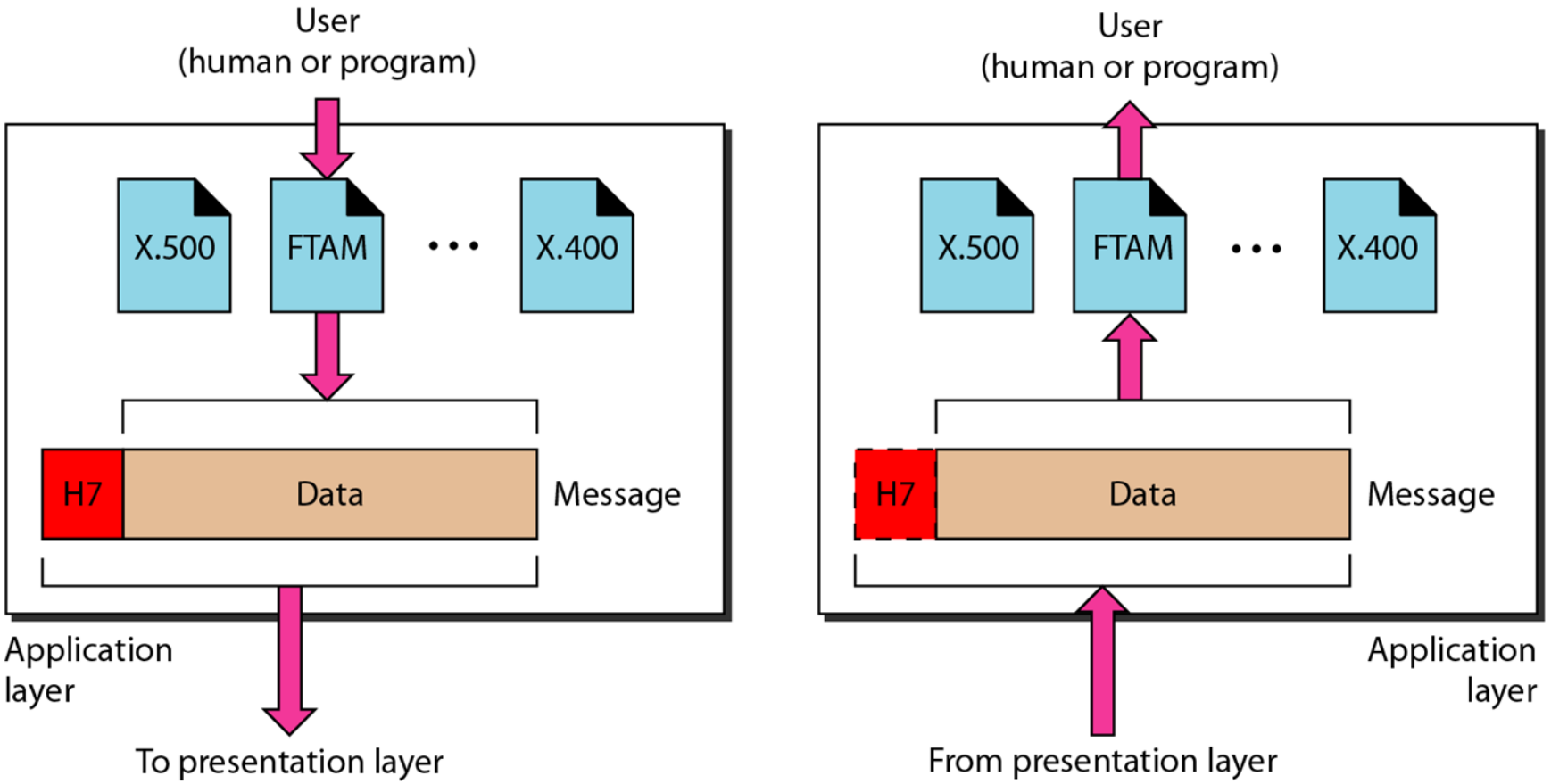
- It is the top layer of OSI reference model.
- The application layer enables the user to communicate its data to the receiver by providing certain services.
- It acts as an interface between application program and the network.
- For example:
  - File Transfer Protocol (FTP),
  - Telnet,
  - SMTP(Simple Mail Transfer Protocol)
  - Network File System (NFS)
  - Hyper Text Transfer Protocol (HTTP) etc.

Layer 6: Presentation Layer

- Presentation layer defines the format in which the data is to be exchanged between the two communicating entities before transmission.
- The presentation layer at sending side receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer.
- At the receiving side, the presentation layer receives data from the session layer decompresses and decrypts the data as required and translates it back as per the encoding scheme used at the receiver.
- Major Functions: data translation and code formatting, data compression, decompression, encryption and decryption


From application layer
H6
Data
Presentation layer
To session layer
To application layer
H6
Data
Presentation layer
From session layer

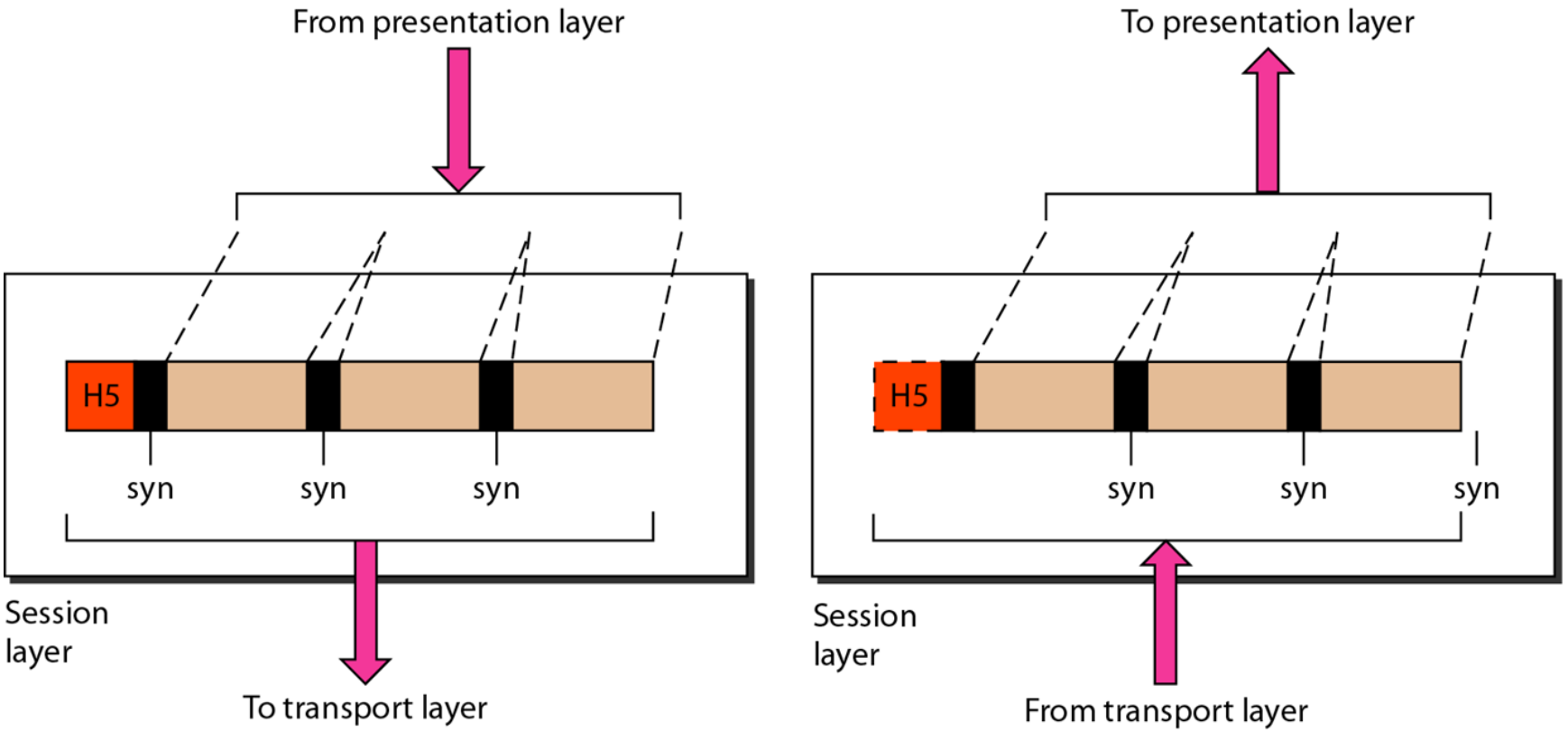
Layer 7: Application Layer



Layer 5: Session Layer

- The session layer allows users on different devices to establish sessions (set up, manage and terminate) between them.
- It keeps different applications' data separate from other applications' data.
- Sessions offer various service:
  - dialog control (keeping track of whose turn it is to transmit, defines communication mode i.e. simple, half duplex and full duplex),
  - Synchronization (adds checkpoints, or synchronization points)

- The session layer at the sending side accepts data from the presentation layer adds checkpoints to it called *syn bits* and passes the data to the transport layer. At the receiving end the session layer receives data from the transport layer removes the checkpoints inserted previously and passes the data to the presentation layer.
- The checkpoints or synchronization points is a way of informing the status of the data transfer.


From presentation layer
H5
syn
syn
syn
Session layer
To transport layer
To presentation layer
H5
syn
syn
syn
Session layer
From transport layer

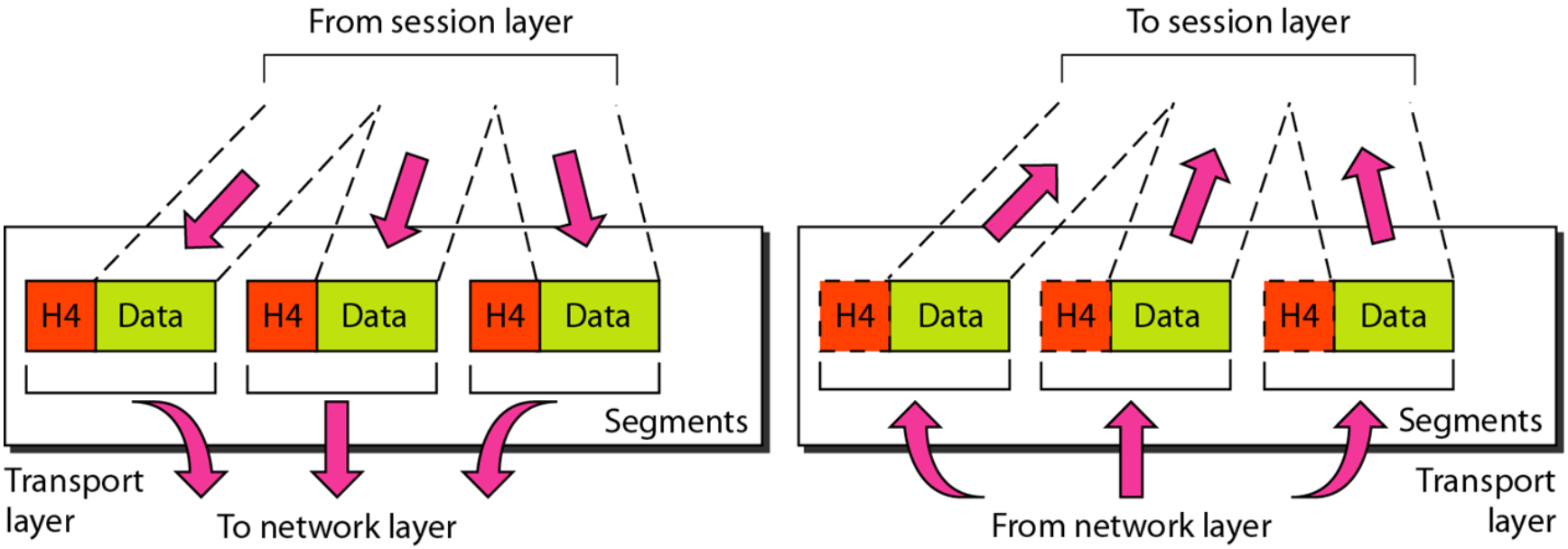
Layer 4: Transport Layer

- The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. using *flow control*.
- To ensure process to process delivery the transport layer makes use of *port address* to identify the data from the sending and receiving process. (port addressing)
- The data can be transported in a *connection oriented* or *connectionless manner*.
- The transport layer accepts a message from the (session) layer above it, splits the message into smaller unit (segments) and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.

The transport layer provides:

- **Port addressing**: add port address to the transport layer header for correct delivery of data to the process
- **Flow control:** to ensure that the transmitting device does not send more data than the receiving device can handle.
- **Segmentation and Reassembly**: data is divided into smaller units, segments, and reassembled at receiver unit.
- **Connection control**: connection oriented or connection-less
- **Multiplexing:** combines data from several sources for transmission over the data path
- **Error control**: data ensured they are received at that destination

Layer 4: Transport Layer



Layer 4: Transport Layer

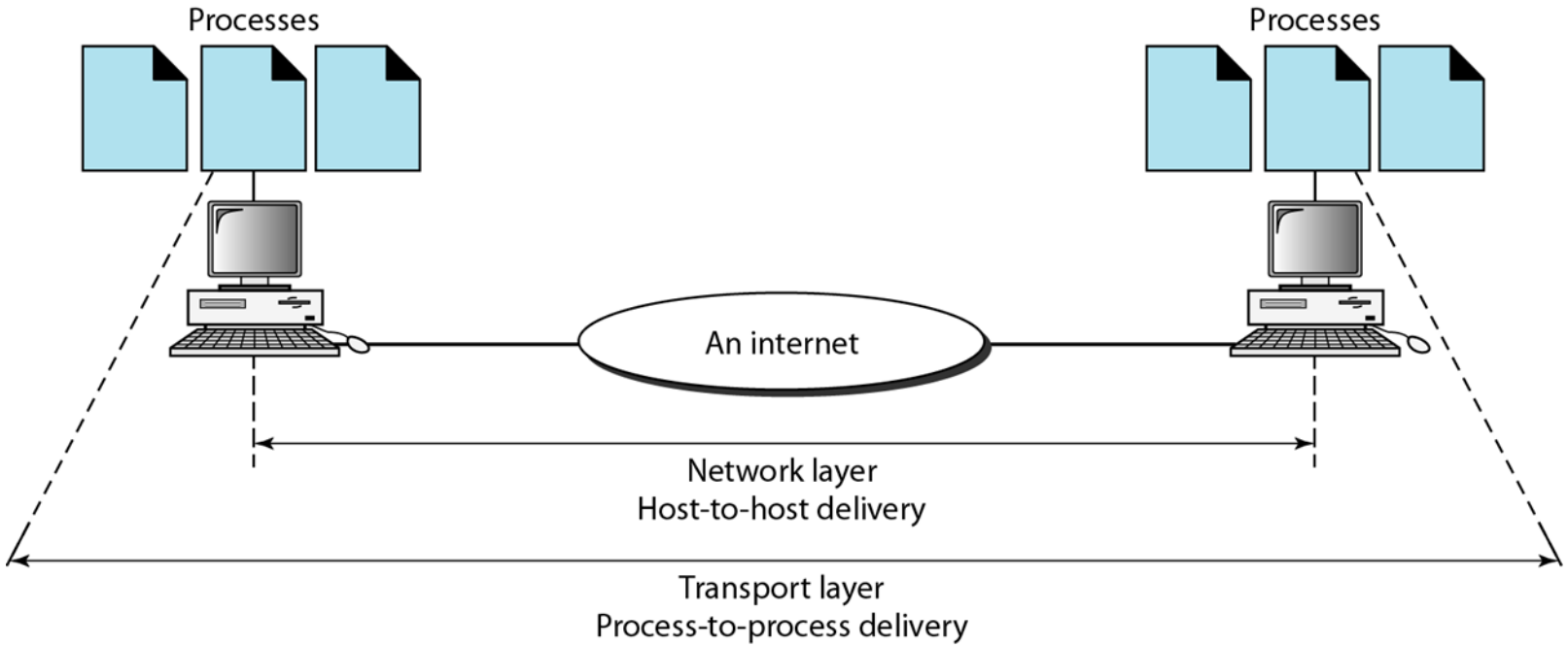
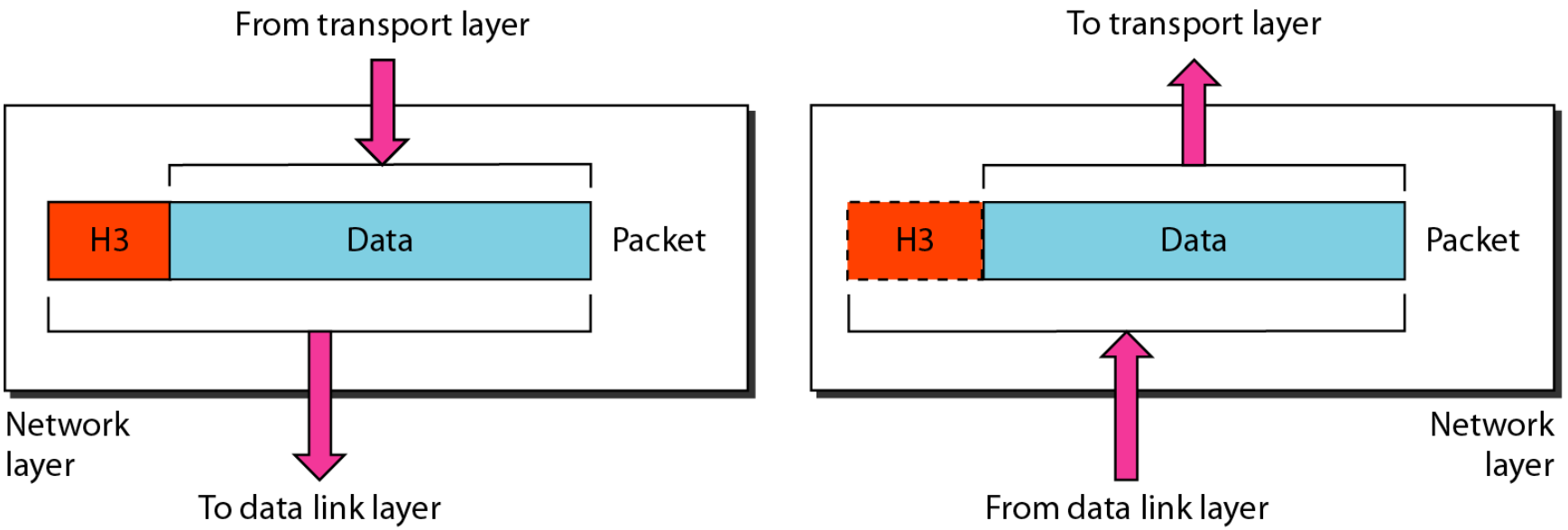


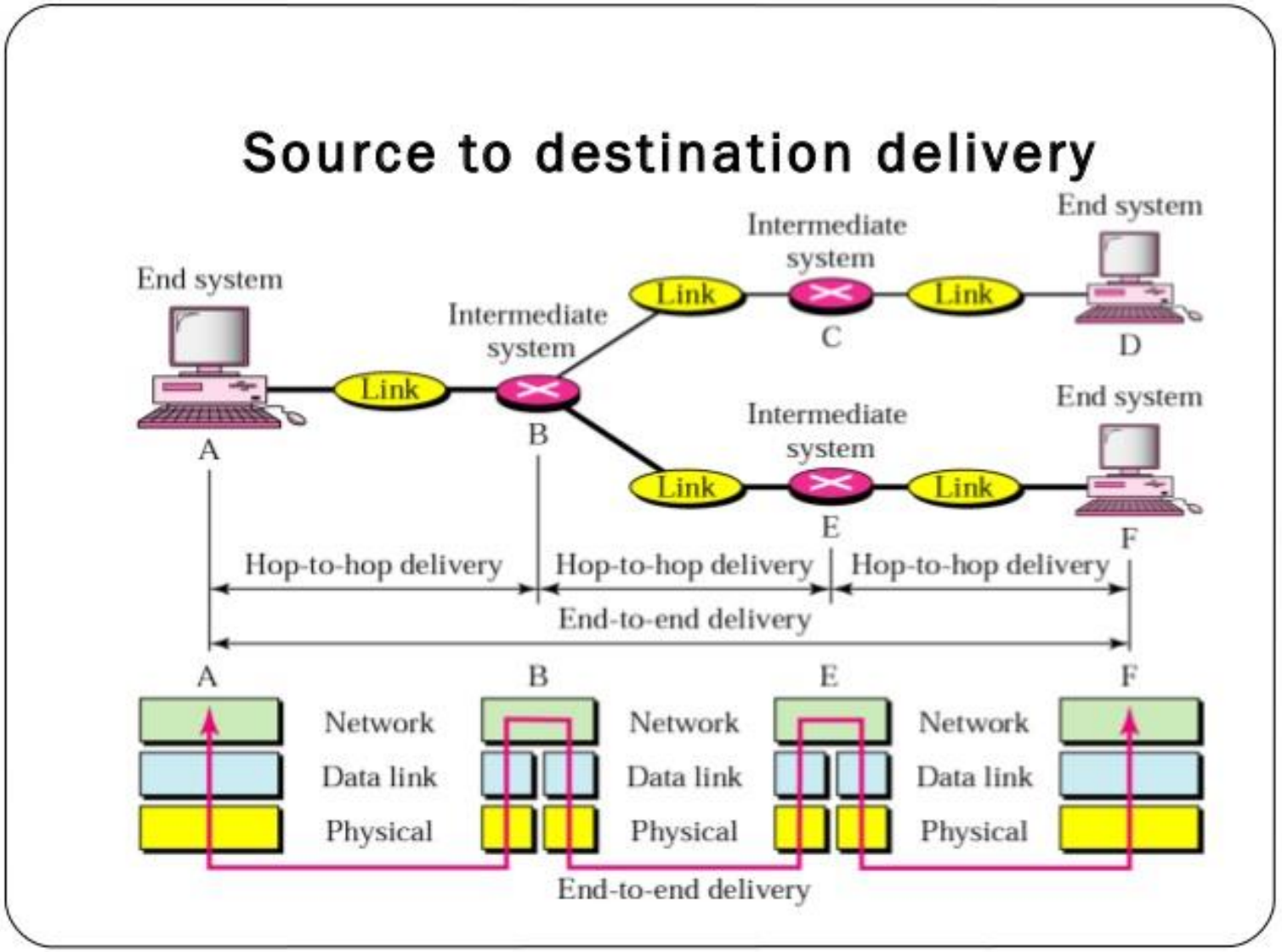
Figure: Reliable Process-to-process delivery of message

Layer 3: Network Layer

- The network layer is responsible for source to destination of delivery of data. Hence it may have to route the data through multiple networks via multiple intermediate devices. In order to achieve this the network layer relies on two things:
  - Logical Addressing
  - Routing
- The network layer at the sending side accepts data from the transport layer, divides it into **packets**, adds addressing information in the header and passes it to the data link layer. At the receiving end the network layer receives the **frames** sent by data link layer, converts them back into packets, verifies the physical address (verifies if the receiver address matches with its own address) and the send the packets to the transport layer.
- The router works on this layer.

Layer 3: Network Layer




Source to destination delivery
End system
Intermediate system
End system
Link
Link
Link
Intermediate system
C
D
A
B
Link
Intermediate system
End system
Link
Link
E
F
Hop-to-hop delivery
Hop-to-hop delivery
Hop-to-hop delivery
End-to-end delivery
A
B
E
F
Network
Network
Network
Data link
Data link
Data link
Physical
Physical
Physical
End-to-end delivery

Layer 2: Data Link Layer

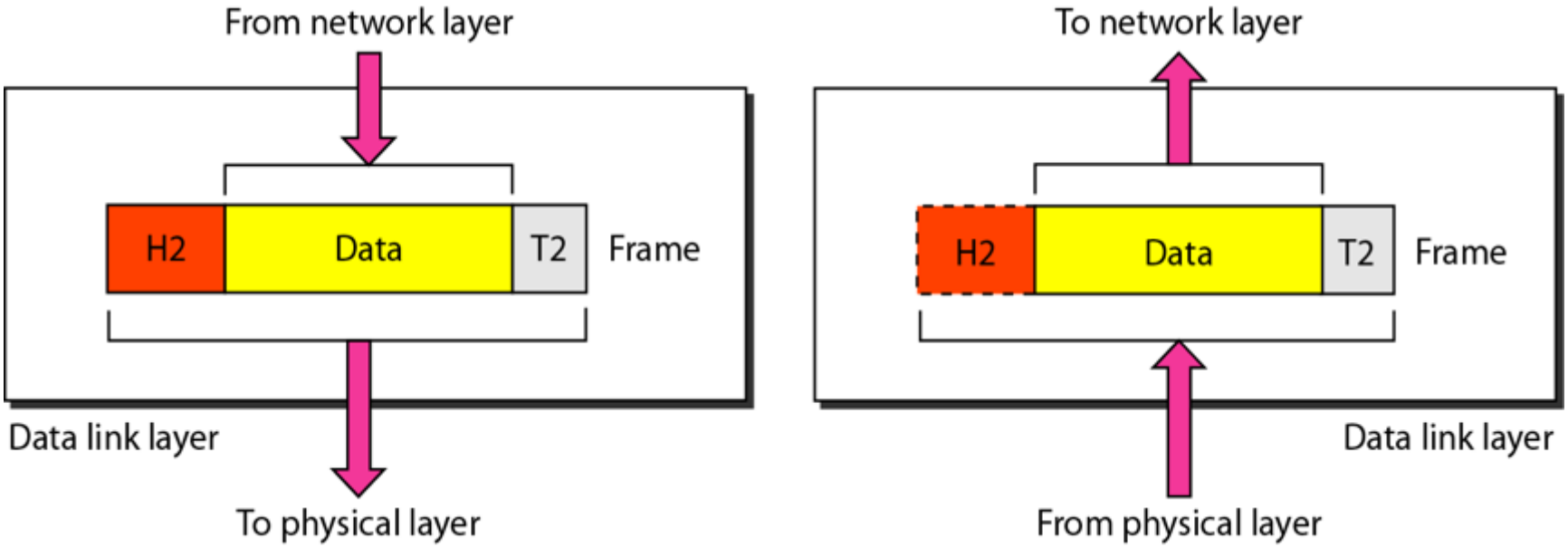
- The Data Link layer provides the physical transmission of data to the device on LAN using physical addressing and handles error notification, network topology, access control, and flow control.
- On the sender side, the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer. This process is called Framing.
- It has two layers:
  - Media access control (MAC)
  - Logical Link control (LLC)

Layer 2: Data Link Layer

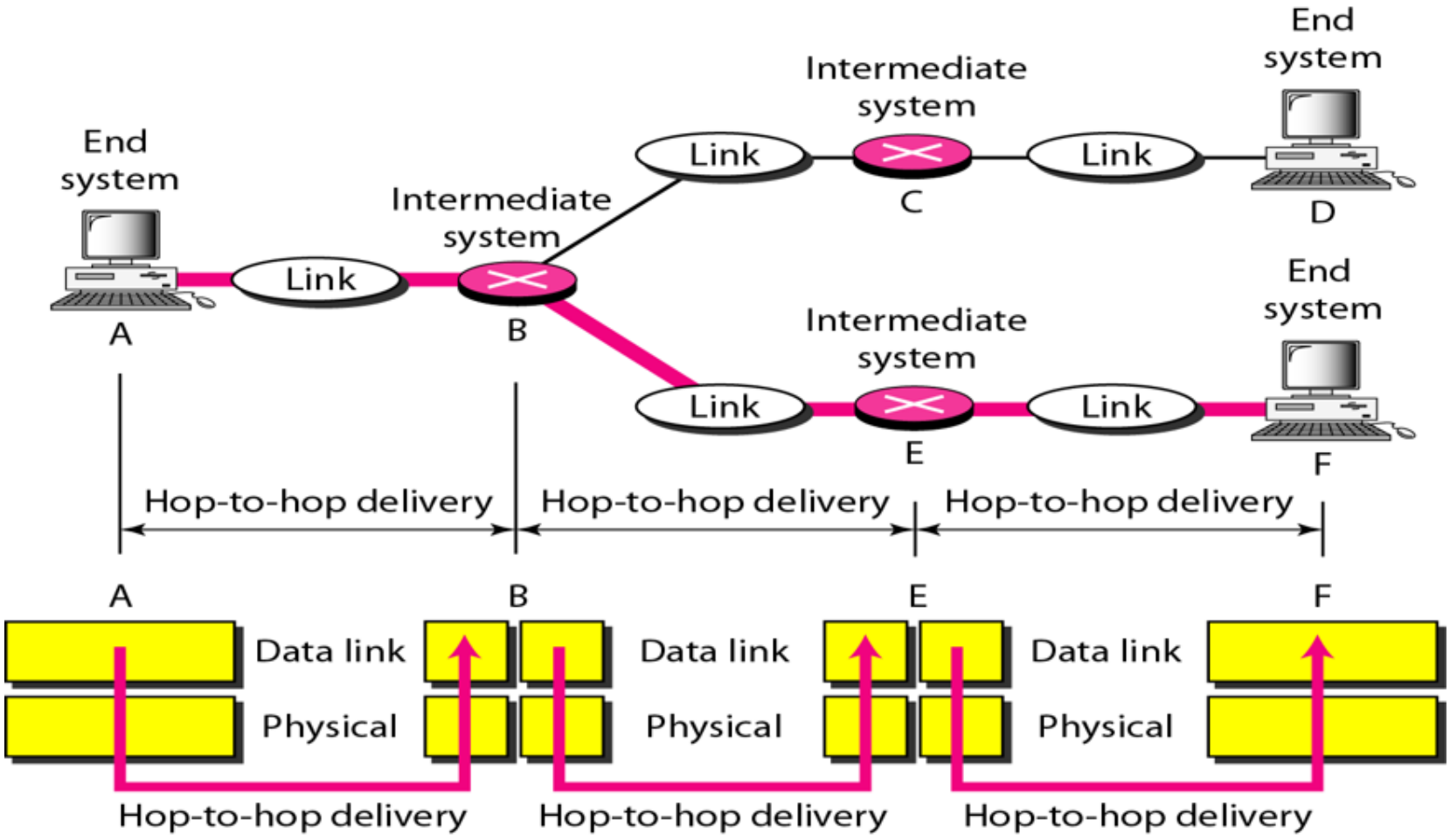
Functions of Data Link Layer

- Framing
- Physical Addressing
- Flow control
- Error control
- Access control

Layer 2: Data Link Layer



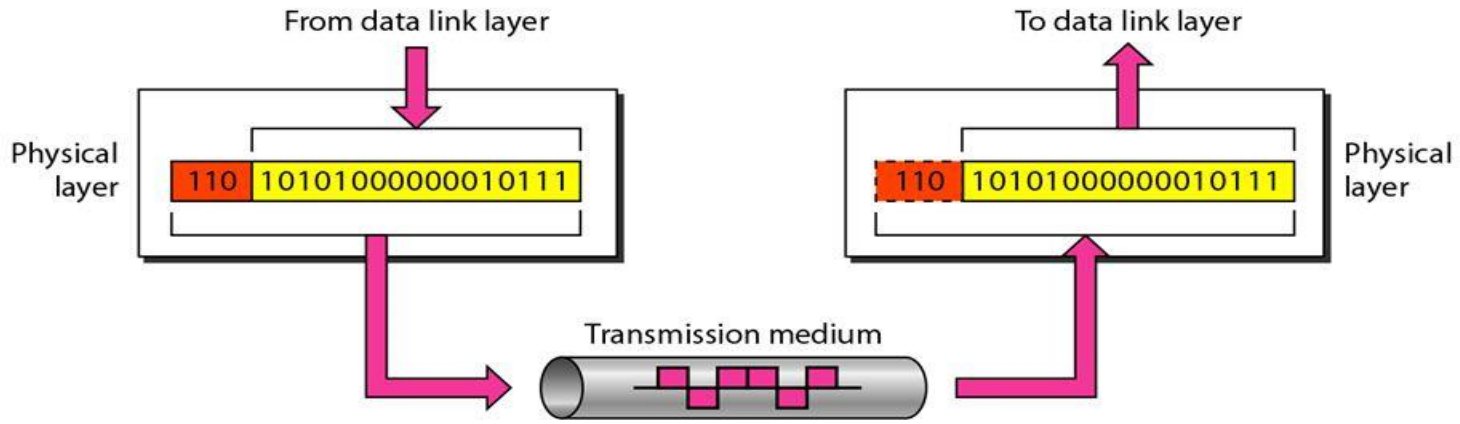
Layer 2: Data Link Layer



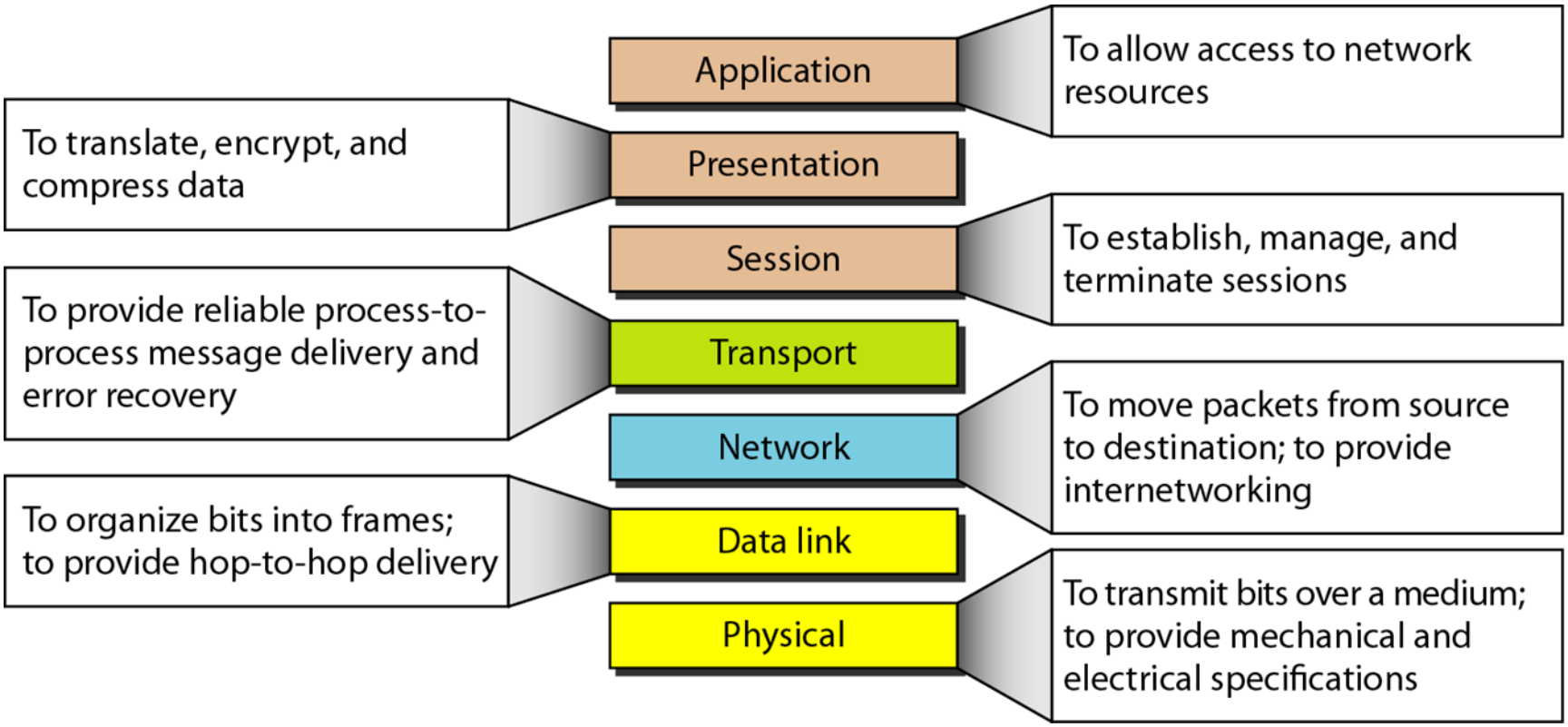
Layer 1: Physical Layer

- The physical layer is concerned with transmitting raw bits over a communication channel.
- The physical layer deals with the physical characteristics of the transmission medium.
- It defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems.
- Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications.

Physical layer



Summary of Layers

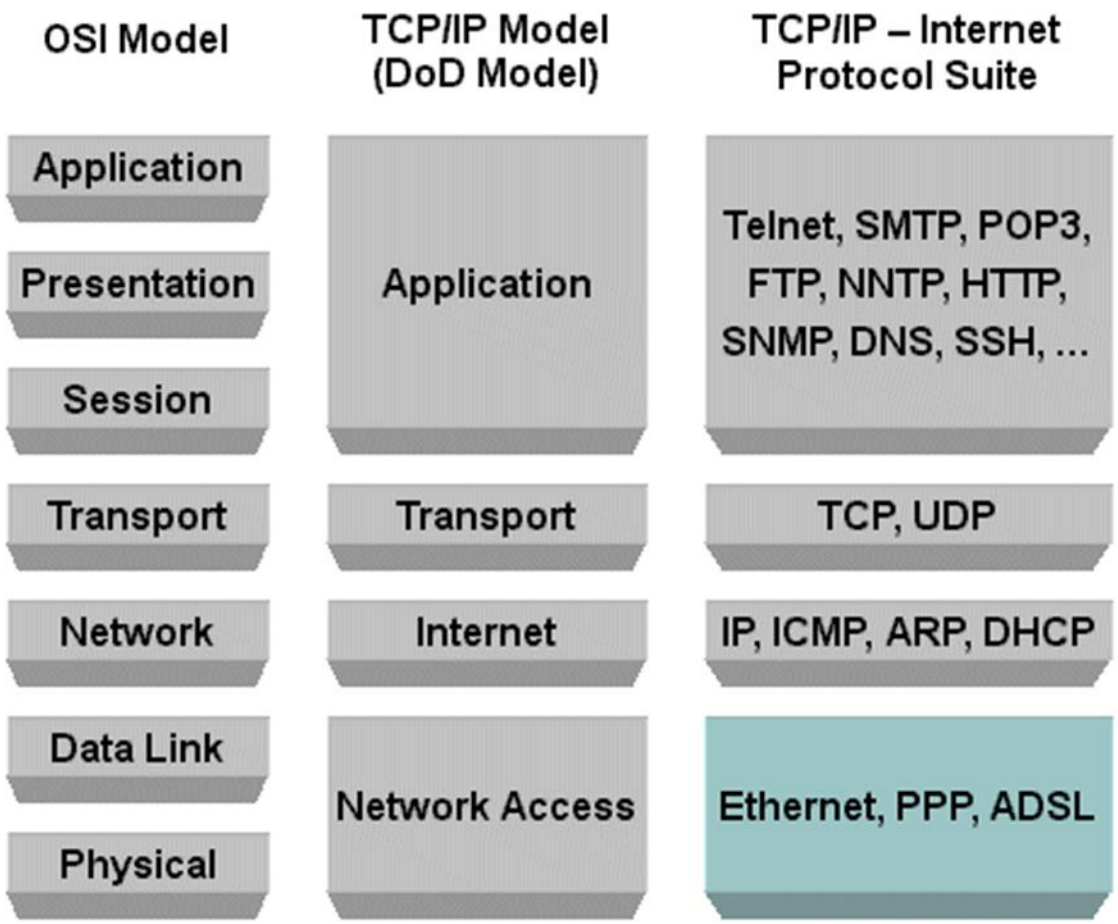


- TCP/IP Protocol Suite
- The **TCP/IP protocol suite** is the computer networking model and set of communications protocols used on the Internet and similar computer networks.
- TCP/IP provides end-to-end connectivity specifying how data should be packetized, addressed, transmitted, routed and received at the destination.
- Often also called the *Internet model*, it was originally also known as the **DoD model**, because the development of the networking model was funded by DARPA, an agency of the United States Department of Defense.
- It is a hierarchical model, i.e. There are multiple layers and higher layer protocols are supported by lower layer protocols.
- It existed even before the OSI model was developed.
- Originally had four layers (bottom to top):
  1. Host to Network Layer/Network Access Layer/Network Interface Layer/Link Layer
  2. Internet Layer
  3. Transport Layer
  4. Application Layer

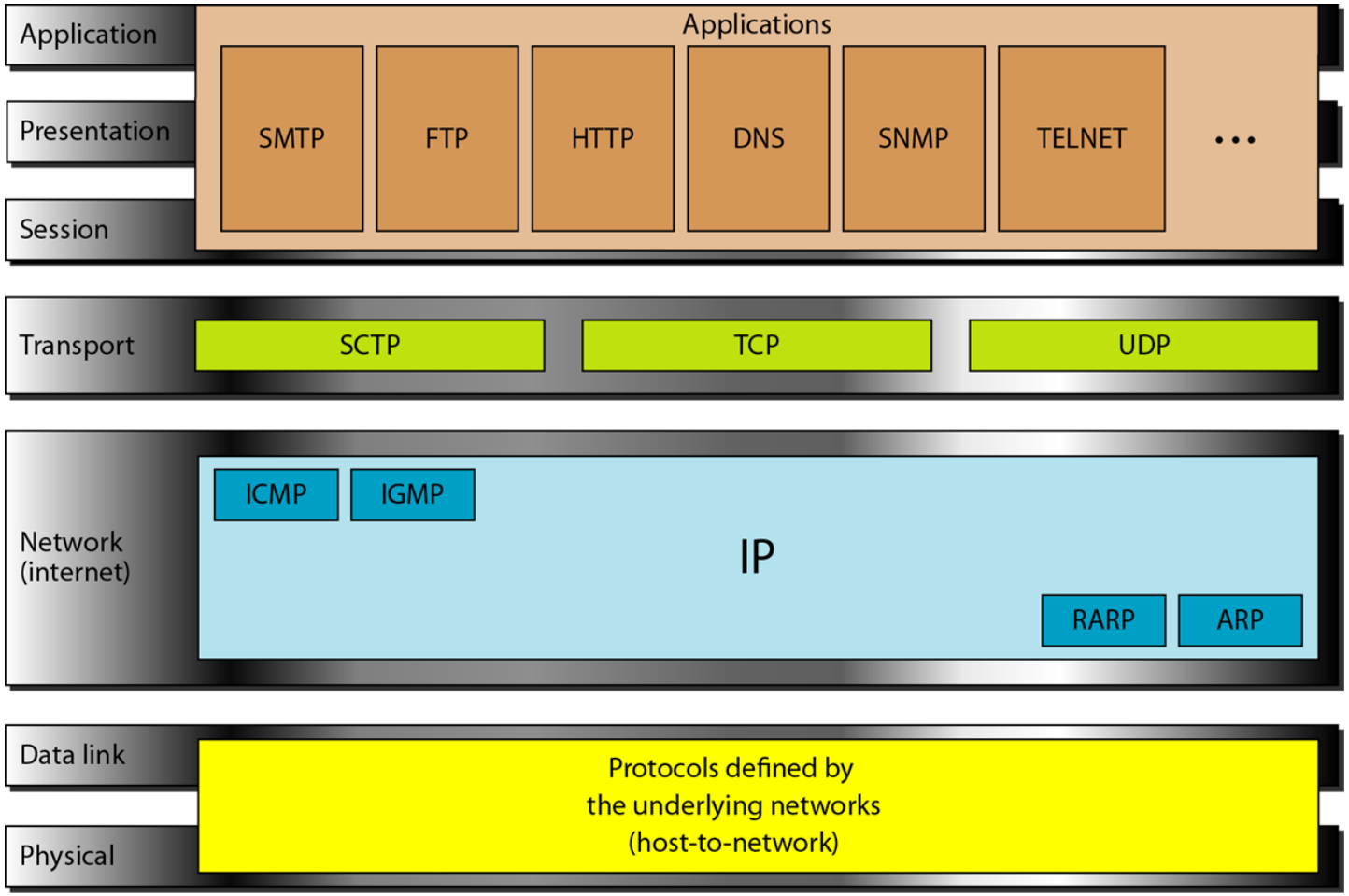
TCP/IP Protocol Suite

However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.

OSI and TCP/IP model



TCP/IP and OSI Model



Layer 1: Host to Network Layer

- This layer is a combination of protocols at the physical and data link layers.
- It supports all standard protocols used at these layers.

Layer 2: Network or Internet Layer

- Also called as the **Internetwork Layer (IP)**.
- It holds the IP protocol which is a network layer protocol and is responsible for source to destination transmission of data.
- The Internetworking Protocol (IP) is an **connection-less** and **unreliable protocol**.
- IP transports data by dividing it into **packets** called **datagrams** of same size. Each packet is independent of the other and can be transported across different routes and can arrive out of order at the receiver.
- IP is a combination of four protocols:
  1. ARP
  2. RARP
  3. ICMP
  4. IGM

Address Resolution Protocol (ARP)

- ARP is used to find the hardware address (physical address) of a host (device) from a known logical address (IP address).

Reverse Address Resolution Protocol (RARP)

- It is used by a device on the network to find its Internet address (logical address or IP address) when it knows its physical address (MAC address or hardware address).

Internet Control Message Protocol (ICMP)

- It is a signaling mechanism used to inform the sender about the datagram problems during the transit.
- It is used by intermediate devices like gateway router etc.
- The following are some common events and messages that ICMP relates to:
  - Destination Unreachable
  - Buffer Full
  - Hops/Time Exceeded
  - Ping
  - Traceroute

Internet Group Message Protocol (IGMP)

- It is a mechanism that allows to send the same message to a group of recipients

Layer 3: Transport Layer

- Transport layer protocols are responsible for transmission of data running on a process of one machine to the correct process running on another machine.
- The transport layer contains three protocols:
  1. TCP
  2. UDP
  3. SCTP

Transmission Control Protocol (TCP)

- TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted.
- It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data

User Datagram Protocol (UDP)

- UDP is a simple protocol used for process to process transmission.
- It is an unreliable, connectionless protocol for applications that do not require flow control or error control.
- It simply adds port address, checksum and length information to the data it receives from the upper layer.

Stream Control Transmission Protocol (SCTP)

- SCTP is a relatively new protocol added to the transport layer of TCP/IP protocol suite.
- It combines the features of TCP and UDP.
- It is used in applications like voice over Internet and has a much broader range of applications

Layer 4: Application Layer

- The Application Layer is a combination of Session, Presentation & Application Layers of OSI models.
- Many protocols are defined in this layer like File Transfer (FTP),Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Addressing in TCP/IP Suite

1. Physical Address
2. Logical Address
3. Port Address
4. Specific Address

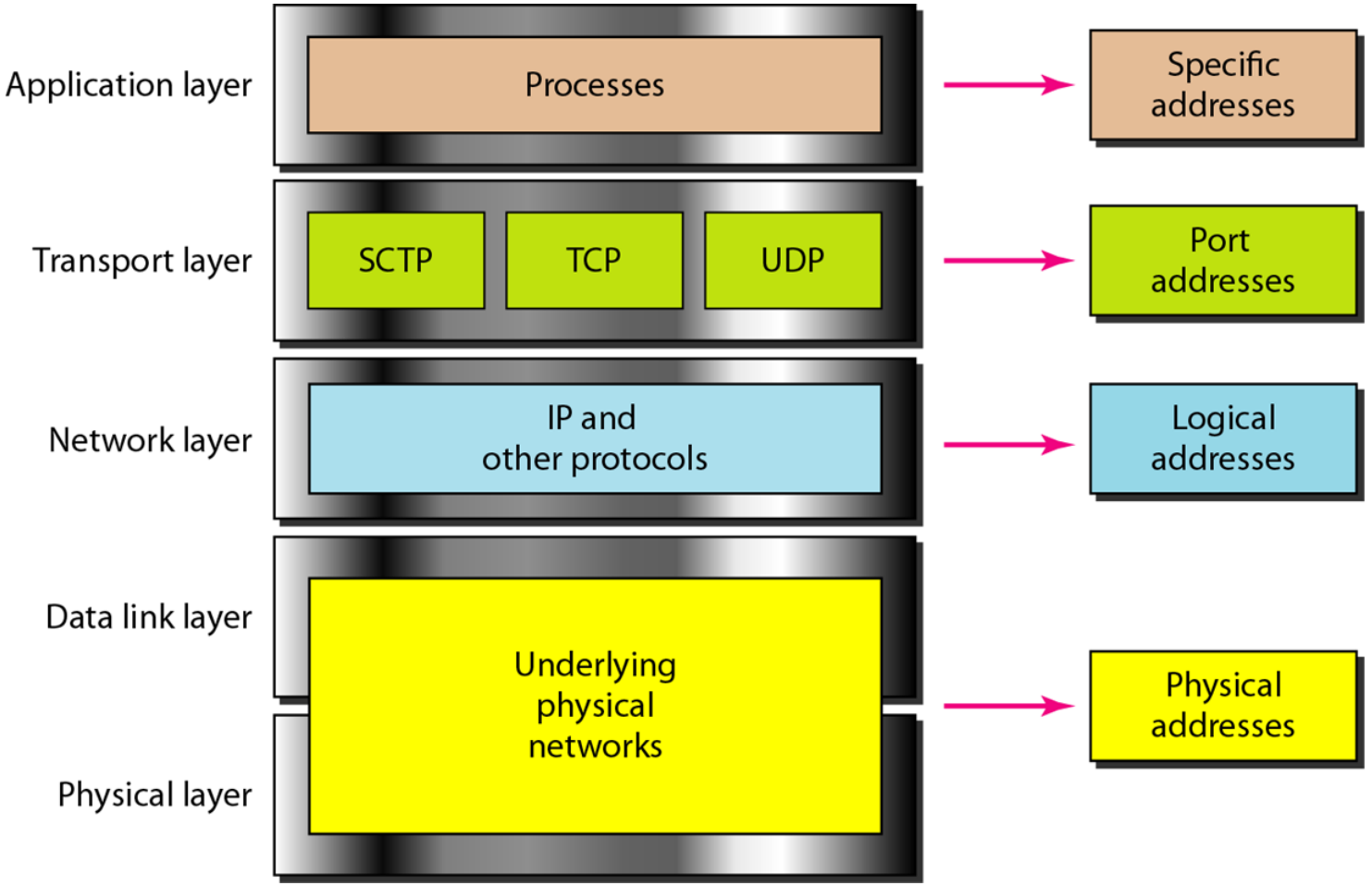
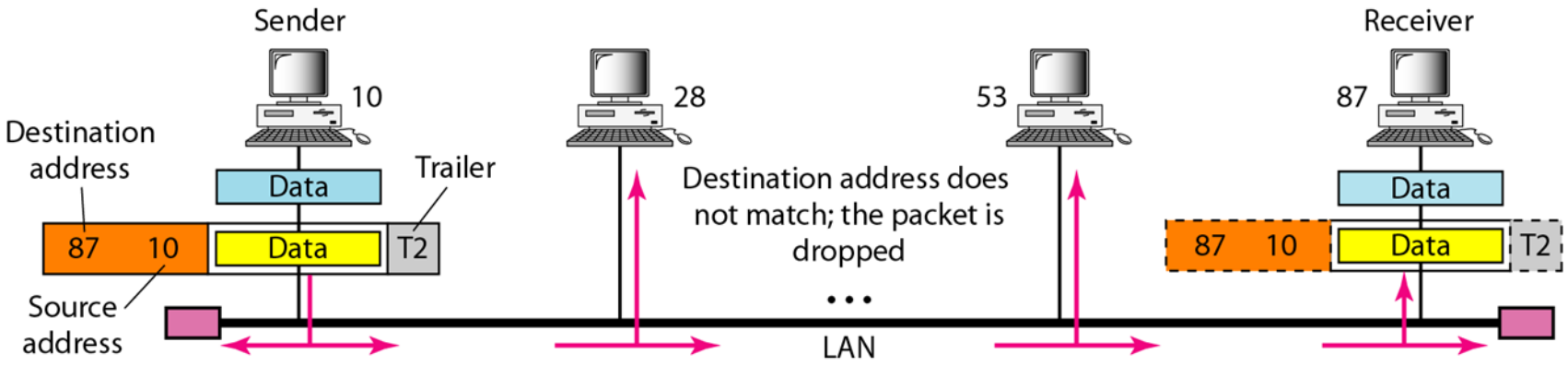


Figure: Relationship of layers and addresses in TCP/IP

Physical Address

- Physical Address is the lowest level of addressing, also known as link address.
- It is local to the network to which the device is connected and unique inside it.
- The physical address is usually included in the frame and is used at the data link layer.
- MAC is a type of physical address that is 6 byte (48 bit) in size and is imprinted on the Network Interface Card (NIC) of the device.
- The size of physical address may change depending on the type of network. Ex. An Ethernet network uses a 6 byte MAC address. Local Talk (Apple) use 1 byte dynamic address that changes each time the station comes up.

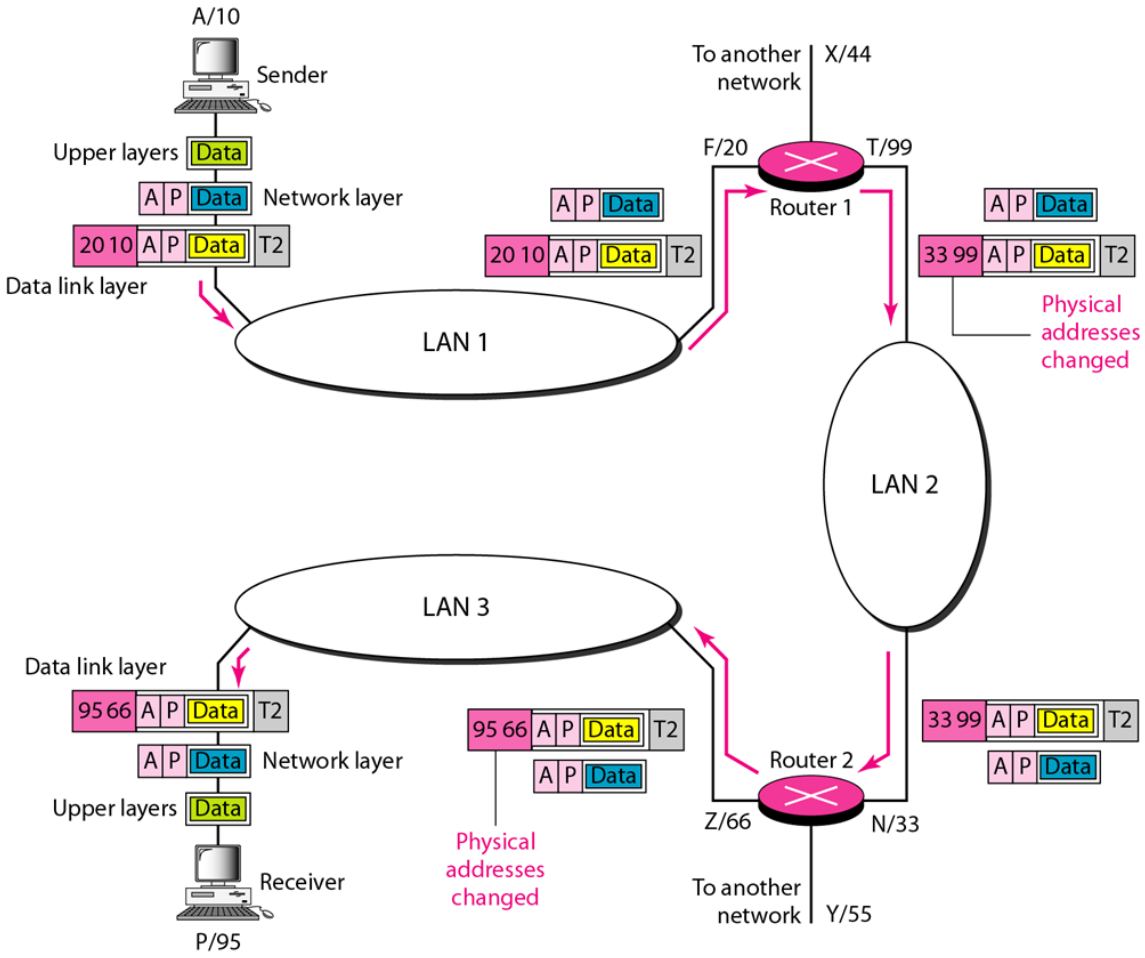
Physical Address



Logical Address

- Logical Address is also called as IP Address (Internet Protocol address).
- At the network layer, device i.e. computers and routers are identified universally by their IP Address.
- IP addresses are universally unique.
- Currently there are two versions of IP addresses being used:
  1. IPv4: 32 bit address, capable of supporting 2^{32} nodes
  2. IPv6: 128 bit address, capable of supporting 2^{128} nodes

IP Address

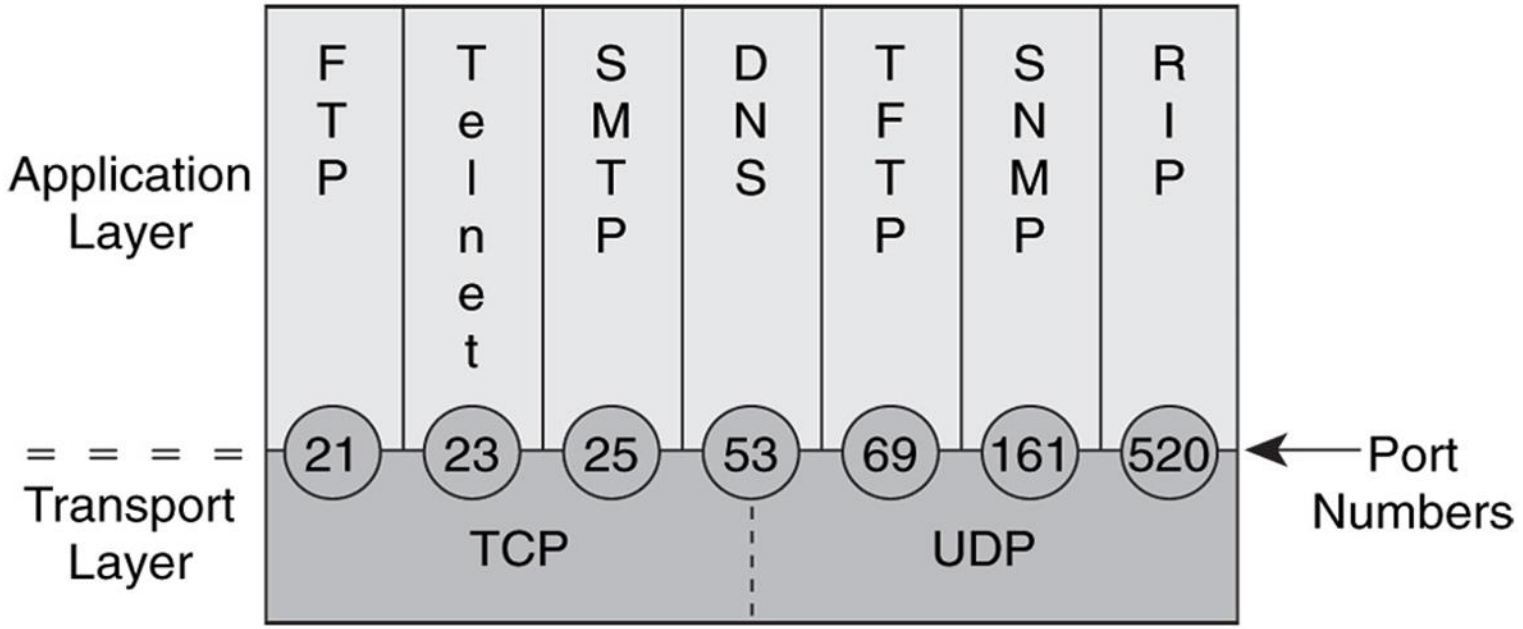

A/10
Sender
Upper layers
Data
A P Data
Network layer
20 10 A P Data T2
Data link layer
LAN 1
To another network
X/44
F/20
T/99
Router 1
A P Data
20 10 A P Data T2
33 99 A P Data T2
Physical addresses changed
LAN 2
LAN 3
Data link layer
95 66 A P Data T2
A P Data
Network layer
Upper layers
Data
Receiver
P/95
95 66 A P Data T2
A P Data
Physical addresses changed
Router 2
Z/66
N/33
33 99 A P Data T2
A P Data
To another network
Y/55

Note

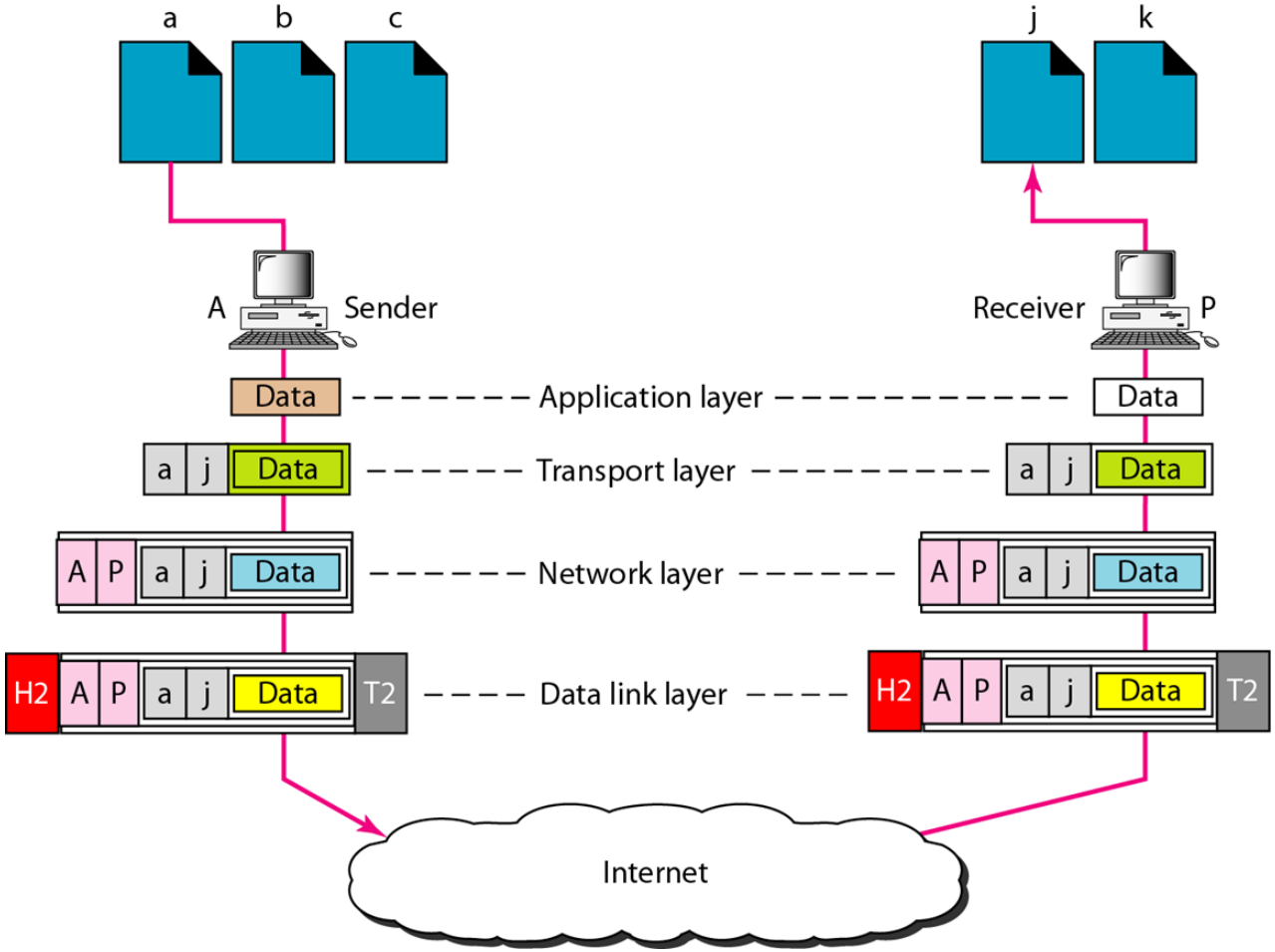
The physical addresses change from hop to hop, but the logical and port addresses usually remain the same.

Port Address

- A Port Address is the name or label given to a process. It is a 16 bit address.
- Ex. TELNET uses port address 23, HTTP uses port address 80



Port Address



Specific Address

- Some application have user friendly addresses and are called specific addresses.
- Examples: email address, URL (Universal Resource Locator)

Comparison of OSI Model and TCP/IP Model

- The OSI and TCP/IP models have many similarities:
- Both are based on layers' concept.
- Both have application layers, though they include different services.
- Both have comparable transport and network layers.
- Both use packet-switched instead of circuit-switched technology.
- Networking professionals need to know both models

Differences between OSI and TCP/IP

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.

Differences between OSI and TCP/IP

8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers