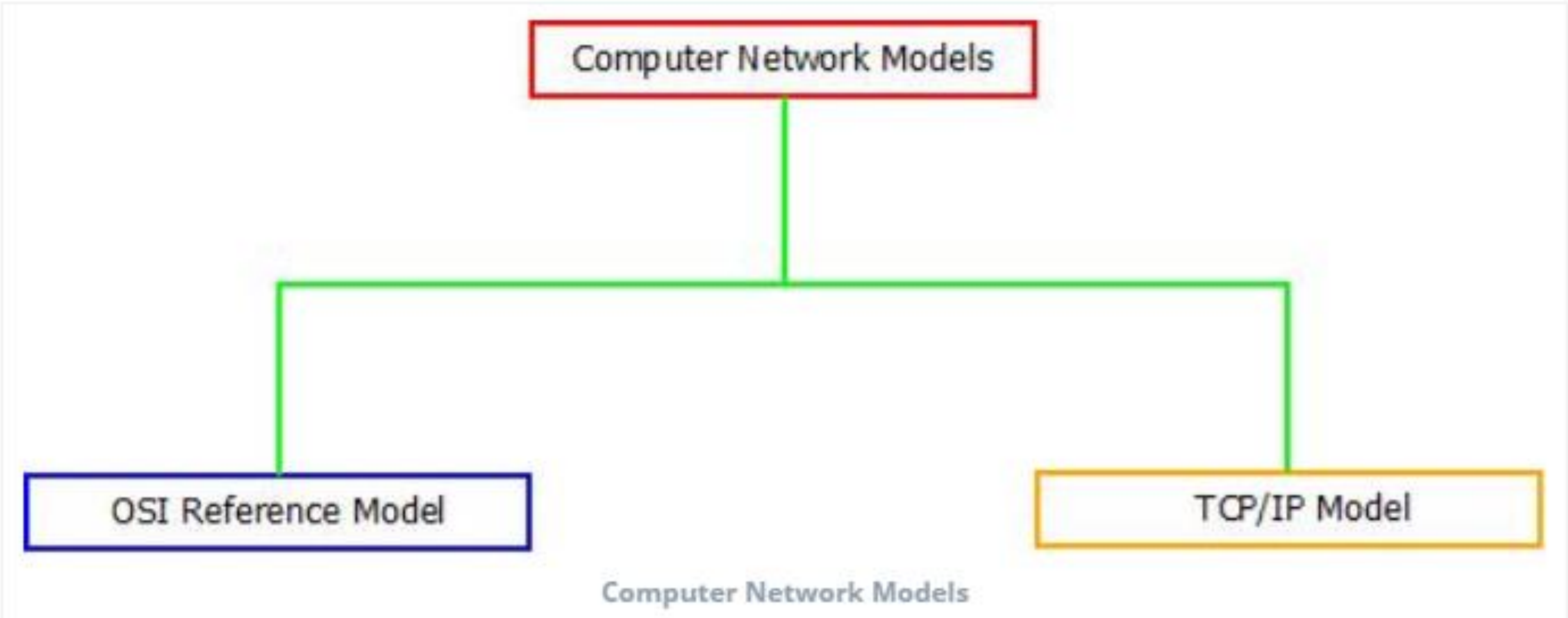
CAP275: Data Communiction and Networking
Unit-I: Network Models

Dr. Manmohan Sharma
School of Computer Applications
Lovely Professional University

Network Models

- For data communication to take place and two or more users can transmit data from one to other, a systematic approach is required.
- This approach enables users to communicate and transmit data through efficient and ordered path.
- It is implemented using models in computer networks and are known as computer network models.
- Computer network models are responsible for establishing a connection among the sender and receiver and transmitting the data in a smooth manner respectively.

- There are two computer network models on which the whole data communication process relies:
    - OSI Model
    - TCP/IP Model



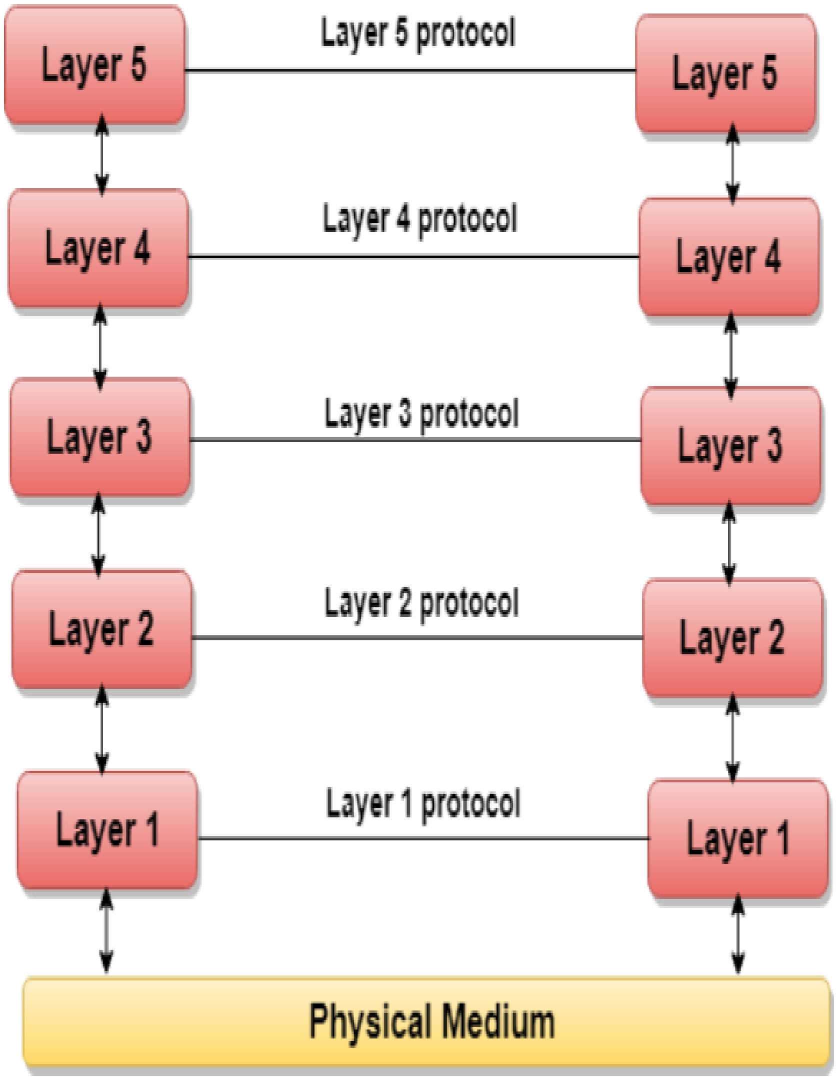
Computer Network Models

Layered Architecture

- The main aim of the layered architecture is to divide the design into small pieces.
- Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
- It provides modularity and clear interfaces, i.e., provides interaction between subsystems.
- It ensures the independence between layers by providing the services from lower to higher layer without defining how the services are implemented. Therefore, any modification in a layer will not affect the other layers.
- The number of layers, functions, contents of each layer will vary from network to network. However, the purpose of each layer is to provide the service from lower to a higher layer and hiding the details from the layers of how the services are implemented.

- The basic elements of layered architecture are services, protocols, and interfaces.
  - **Service:** It is a set of actions that a layer provides to the higher layer.
  - **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
  - **Interface:** It is a way through which the message is transferred from one layer to another layer.
- In a layer n architecture, layer n on one machine will have a communication with the layer n on another machine and the rules used in a conversation are known as a layer-n protocol.
- In case of layered architecture, no data is transferred from layer n of one machine to layer n of another machine. Instead, each layer passes the data to the layer immediately just below it, until the lowest layer is reached.

- Below layer 1 is the physical medium through which the actual communication takes place.
- In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.
- The data is passed from the upper layer to lower layer through an interface. A Layered architecture provides a clean-cut interface so that minimum information is shared among different layers. It also ensures that the implementation of one layer can be easily replaced by another implementation.
- A set of layers and protocols is known as network architecture.

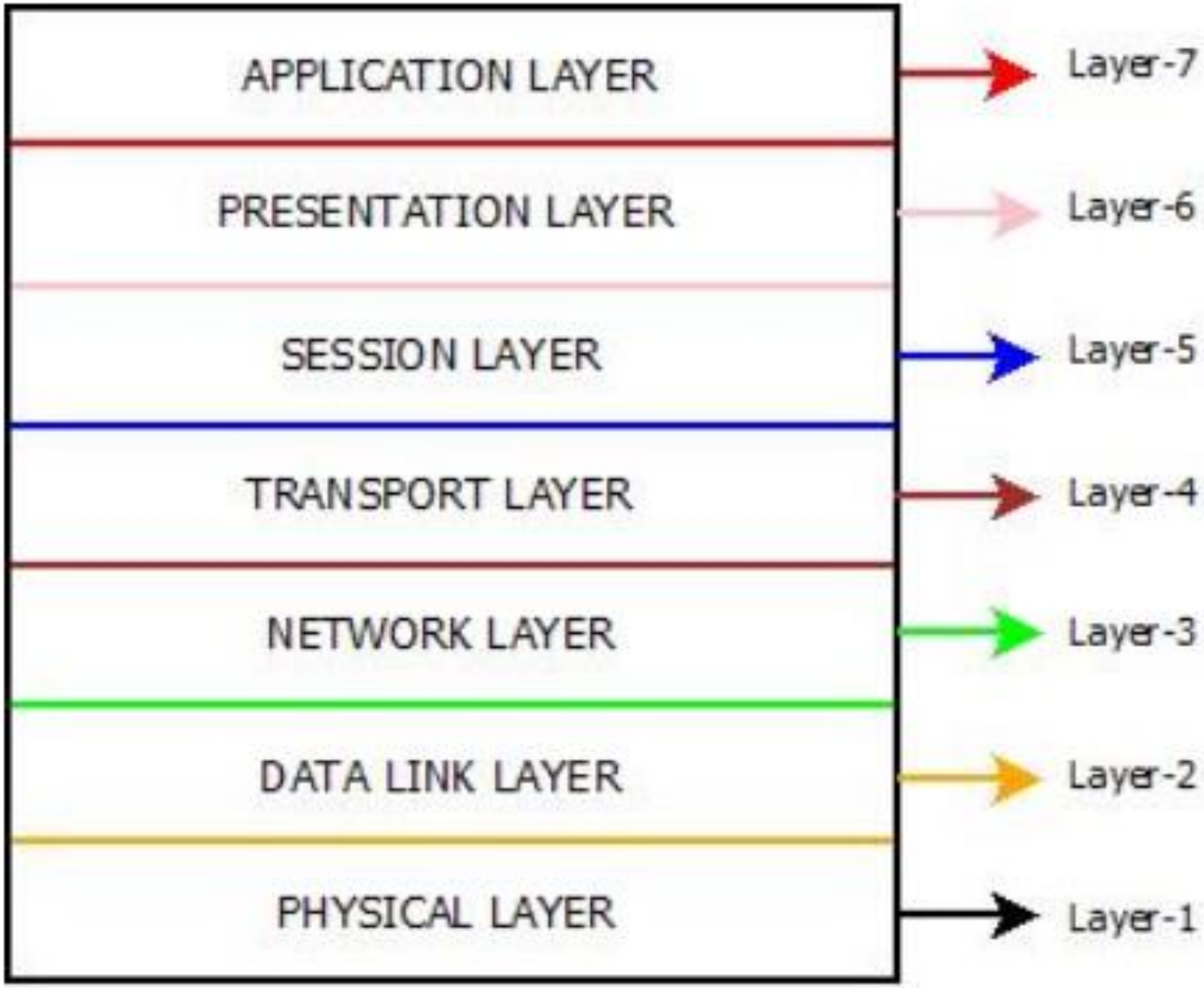


Why do we require Layered architecture?

- **Divide-and-conquer approach:** Divide-and-conquer approach makes a design process in such a way that the unmanageable tasks are divided into small and manageable tasks. In short, we can say that this approach reduces the complexity of the design.
- **Modularity:** Layered architecture is more modular. Modularity provides the independence of layers, which is easier to understand and implement.
- **Easy to modify:** It ensures the independence of layers so that implementation in one layer can be changed without affecting other layers.
- **Easy to test:** Each layer of the layered architecture can be analyzed and tested individually.

OSI Reference Model

- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.



APPLICATION LAYER → Layer-7

PRESENTATION LAYER → Layer-6

SESSION LAYER → Layer-5

TRANSPORT LAYER → Layer-4

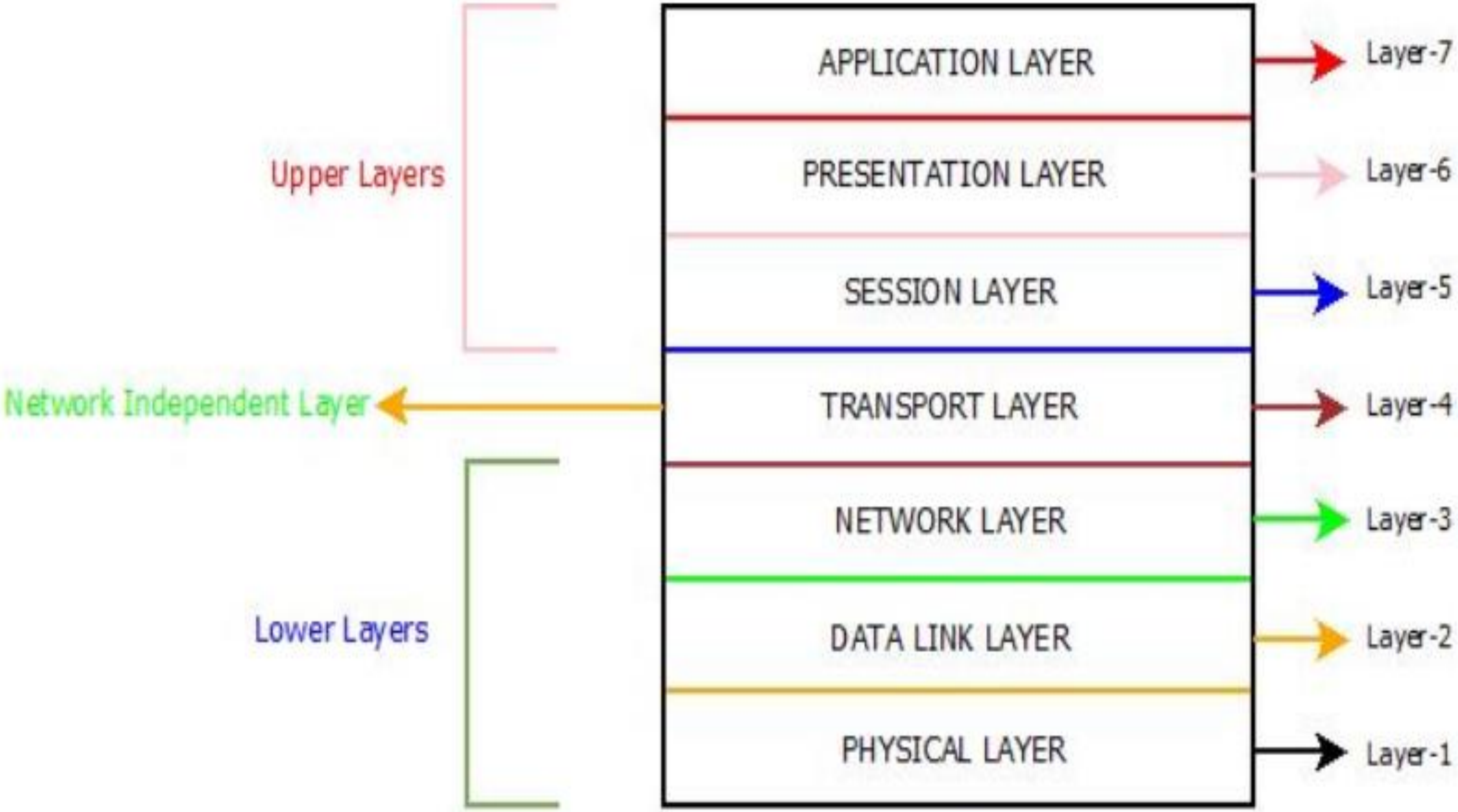
NETWORK LAYER → Layer-3

DATA LINK LAYER → Layer-2

PHYSICAL LAYER → Layer-1

The OSI Reference Model

- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.



Upper Layers

Network Independent Layer

Lower Layers

APPLICATION LAYER — Layer-7

PRESENTATION LAYER — Layer-6

SESSION LAYER — Layer-5

TRANSPORT LAYER — Layer-4

NETWORK LAYER — Layer-3

DATA LINK LAYER — Layer-2

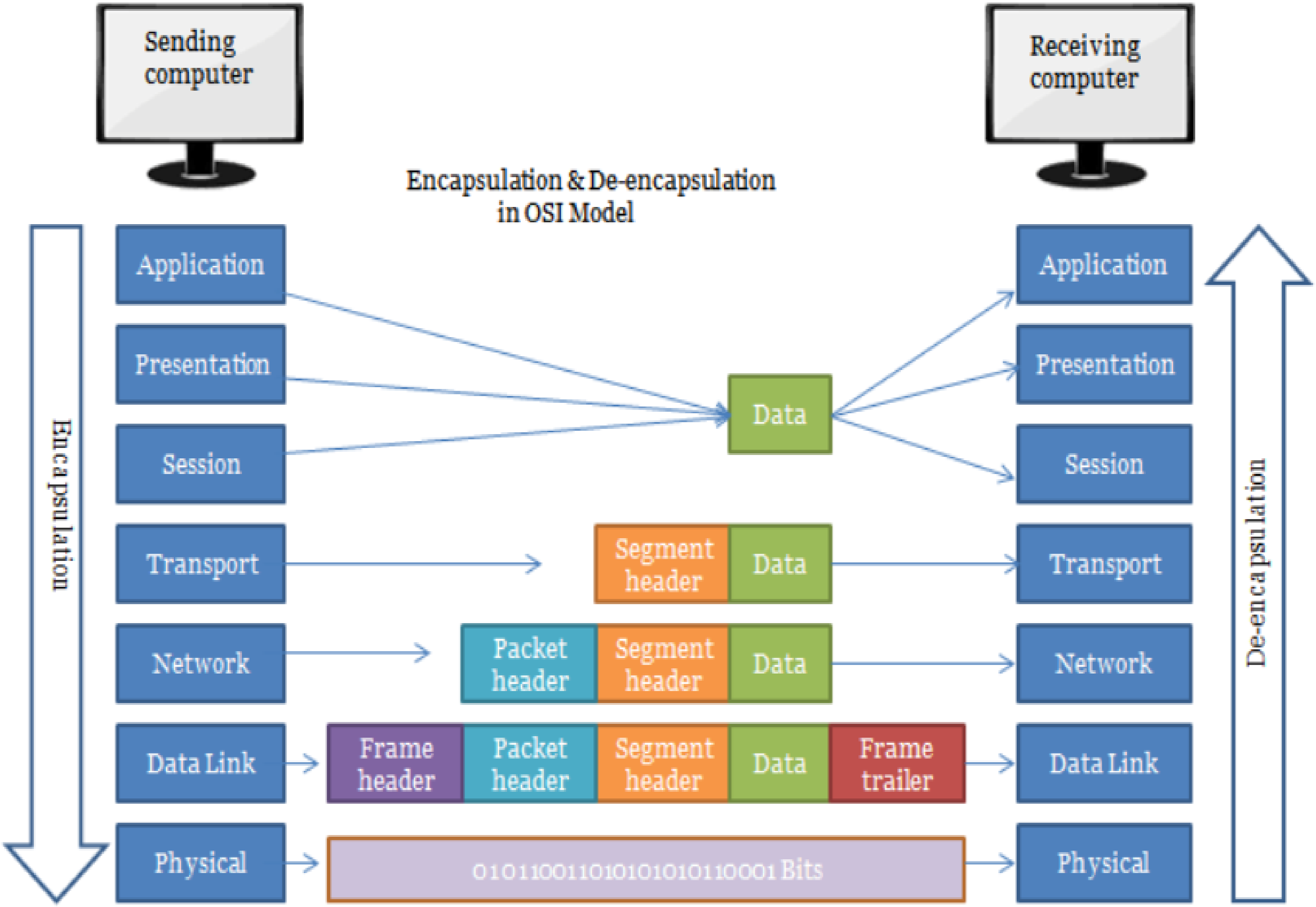
PHYSICAL LAYER — Layer-1

The OSI Reference Model
(Layer categorization)

Functions of the OSI Layers

- **Application Layer**: This layer is responsible for providing interface to the application user. This layer encompasses protocols which directly interact with the user.
- **Presentation Layer**: This layer defines how data in the native format of remote host should be presented in the native format of host.
- **Session Layer**: This layer maintains sessions between remote hosts. For example, once user/password authentication is done, the remote host maintains this session for a while and does not ask for authentication again in that time span.
- **Transport Layer**: This layer is responsible for Process to process delivery between hosts.
- **Network Layer**: This layer is responsible for address assignment and uniquely addressing hosts in a network.
- **Data Link Layer**: This layer is responsible for reading and writing data from and onto the line. Link errors are detected at this layer.
- **Physical Layer**: This layer defines the hardware, cabling wiring, power output, pulse rate etc.

	Layer	Responsibility of	PDU (Protocol Data Unit)	Data Flow
7	Application Layer	Host	Data	
6	Presentation Layer	Host	Data	
5	Session Layer	Host	Data	
4	Transport Layer	Host	Segment	Process to Process
3	Network Layer	Network	Packet	End to End
2	Data Link Layer	Network	Frame	Hop to Hop
1	Physical Layer	Network	Bits and Bytes	



Sending computer

Receiving computer

Encapsulation & De-encapsulation in OSI Model

Encapsulation

Application

Presentation

Session

Transport

Network

Data Link

Physical

Data

Segment header

Data

Packet header

Segment header

Data

Frame header

Packet header

Segment header

Data

Frame trailer

010110011010101010110001 Bits

Application

Presentation

Session

Transport

Network

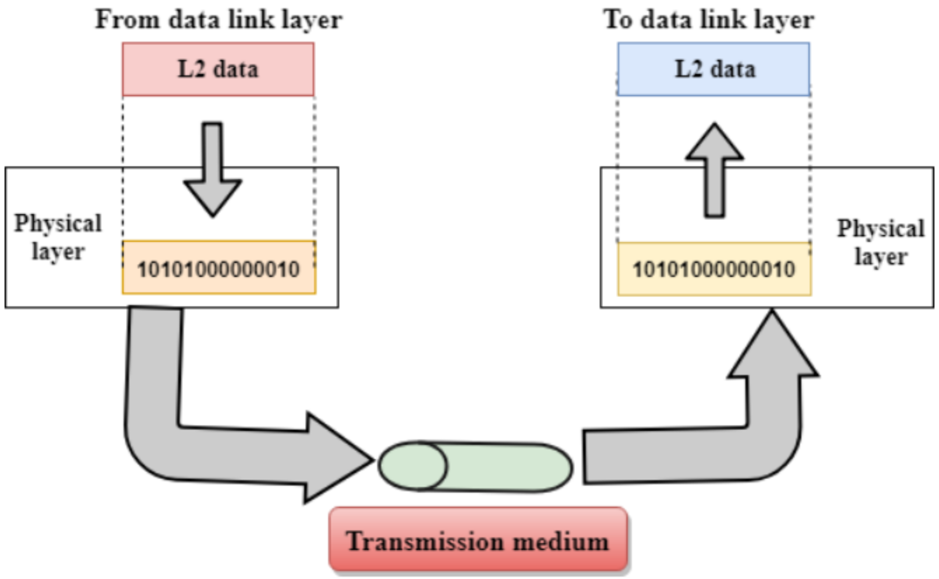
Data Link

Physical

De-encapsulation

Physical layer

- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

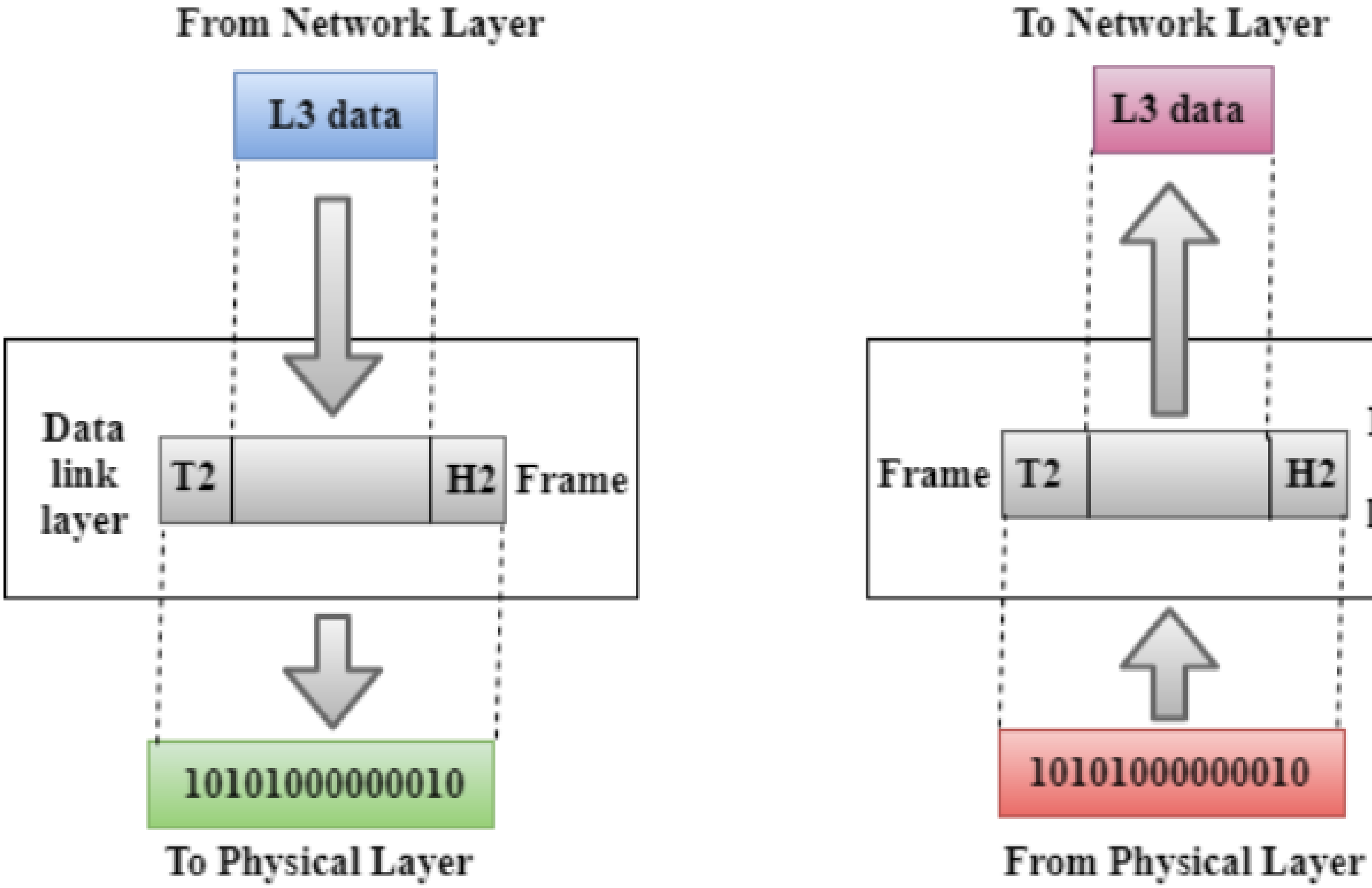


Functions of a Physical layer

- **Line Configuration:** It defines the way how two or more devices can be connected physically.
- **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- **Topology:** It defines the way how network devices are arranged.
- **Signals:** It determines the type of the signal used for transmitting the information.

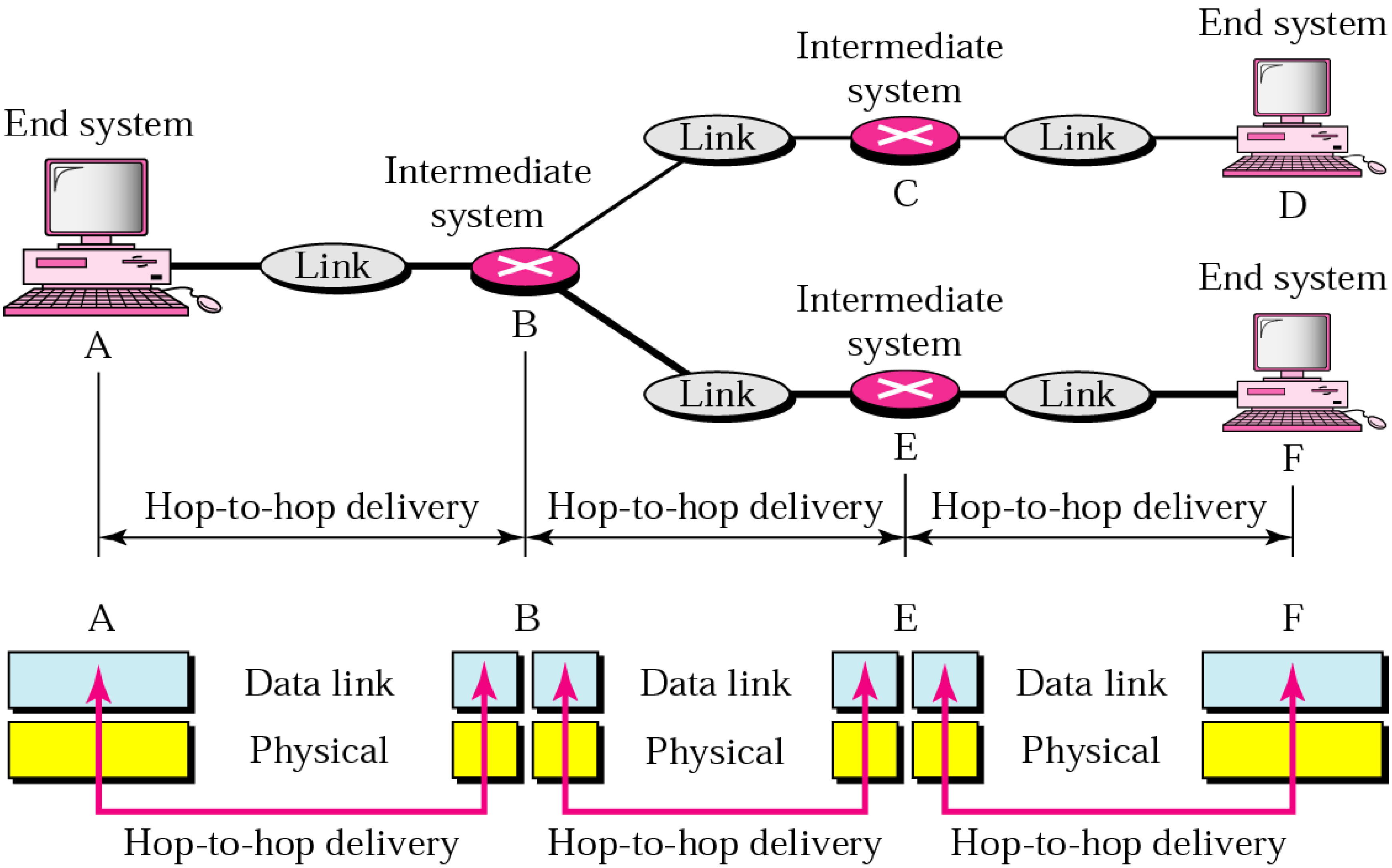
Data-Link Layer

- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
    - **Logical Link Control Layer**
        - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
        - It identifies the address of the network layer protocol from the header.
        - It also provides flow control.
    - **Media Access Control Layer**
        - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
        - It is used for transferring the packets over the network.


From Network Layer
L3 data
Data link layer
T2
H2
Frame
10101000000010
To Physical Layer
To Network Layer
L3 data
Frame
T2
H2
Data link layer
10101000000010
From Physical Layer

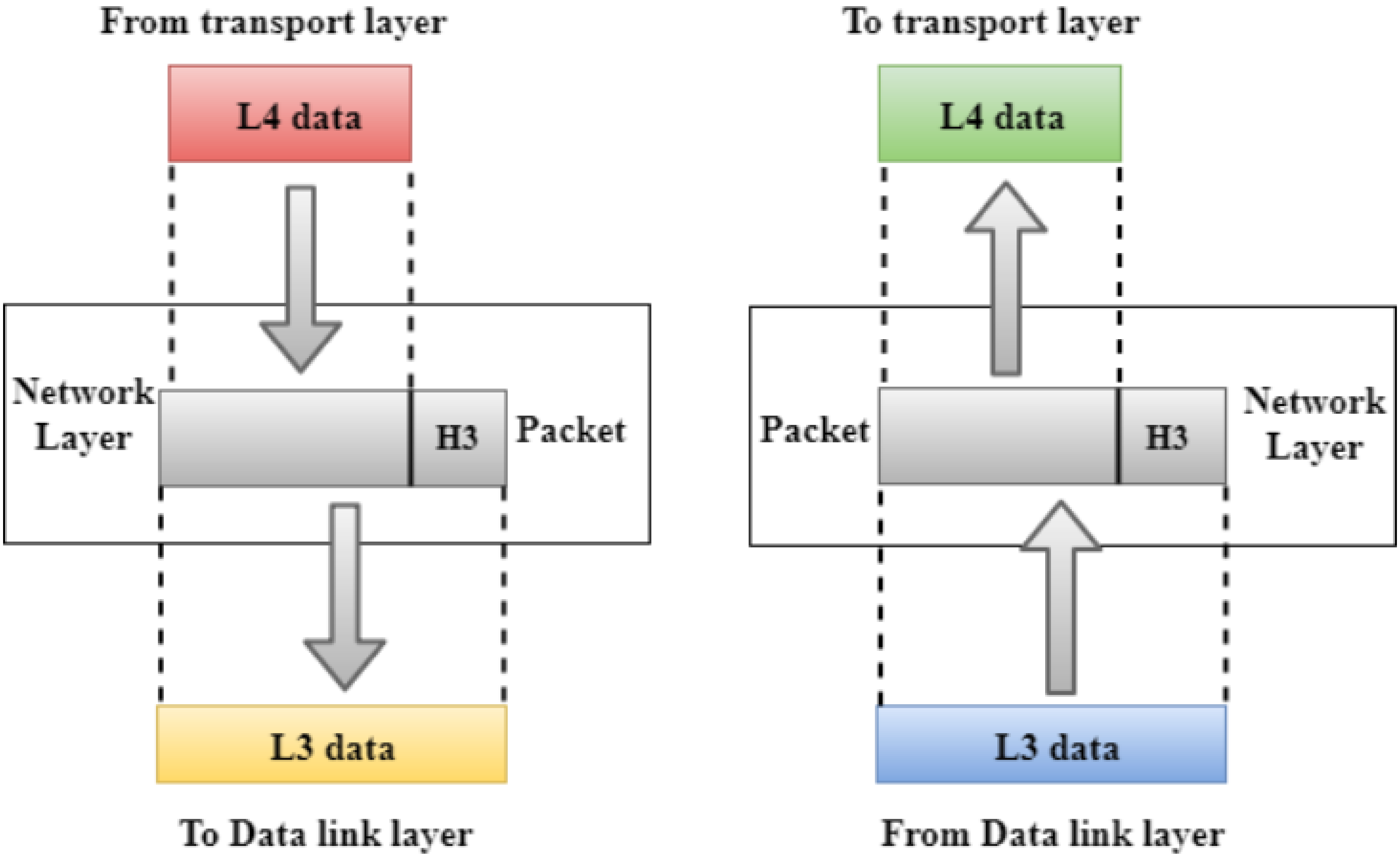
Functions of the Data-link layer

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.
- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.


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

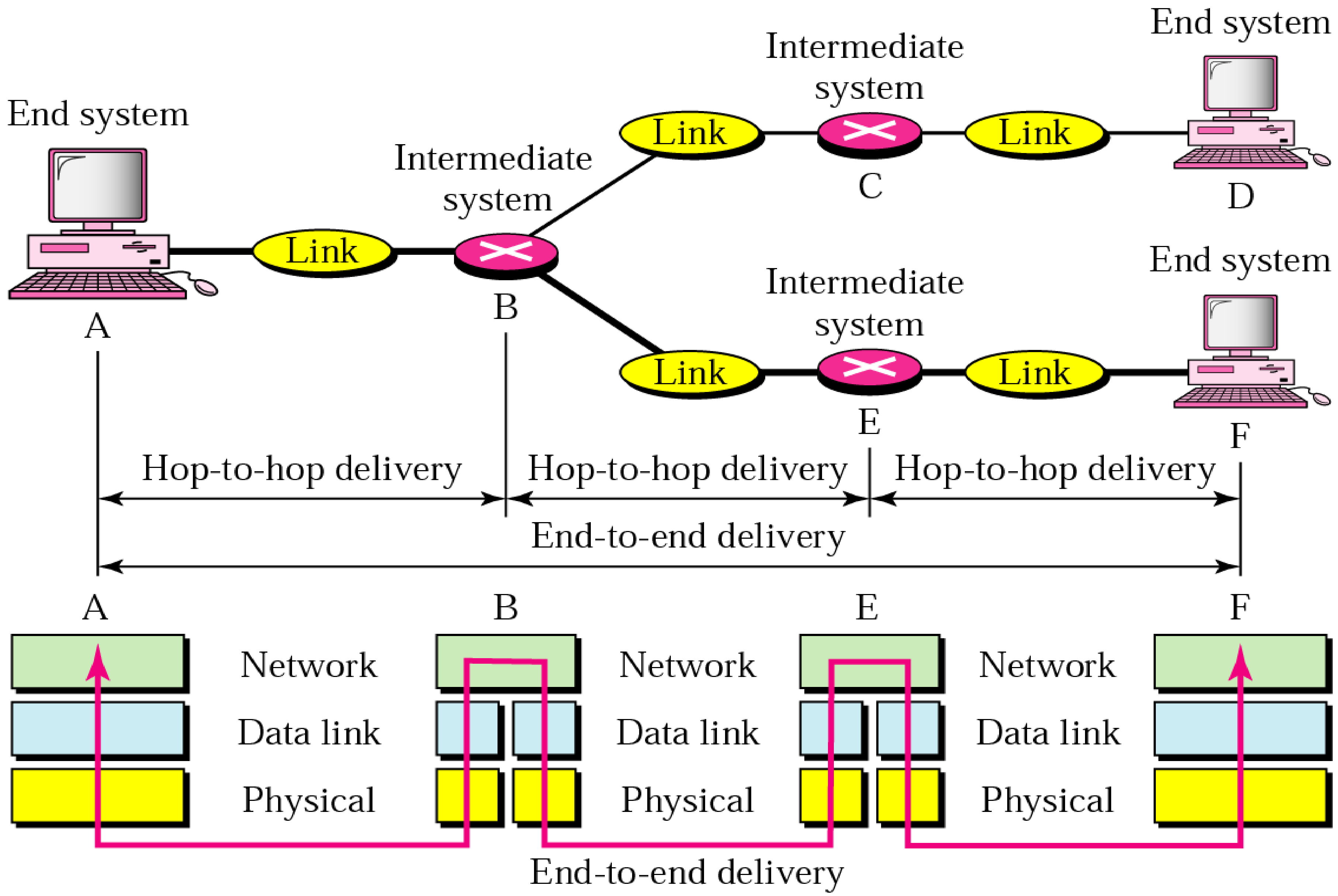
Network Layer

- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.


From transport layer
L4 data
Network Layer
H3
Packet
L3 data
To Data link layer
To transport layer
L4 data
Packet
H3
Network Layer
L3 data
From Data link layer

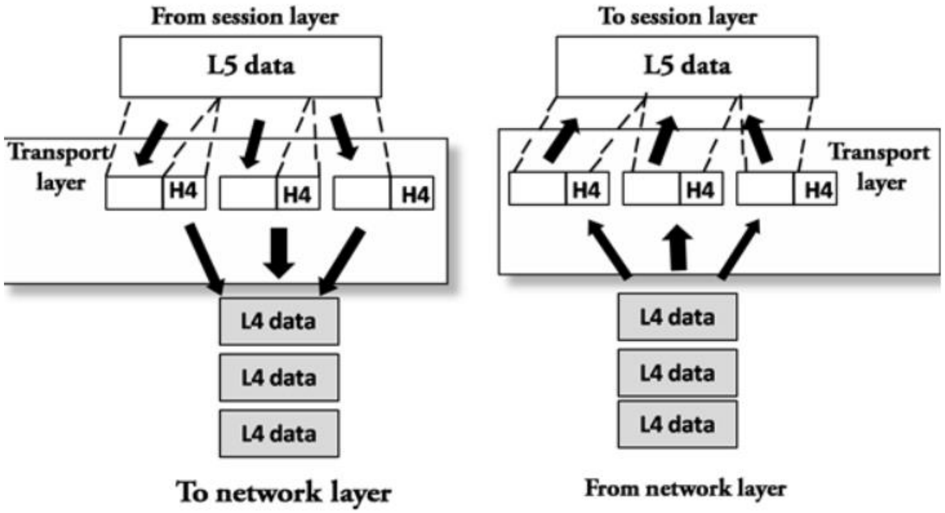
Functions of Network Layer

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the segments from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).


End system
End system
Intermediate system
Intermediate system
Link
Link
Link
Link
Link
Link
A
B
C
D
End system
Intermediate system
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

Transport Layer

- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an process to process layer as it provides a point-to-point connection between source and destination to deliver the data reliably.



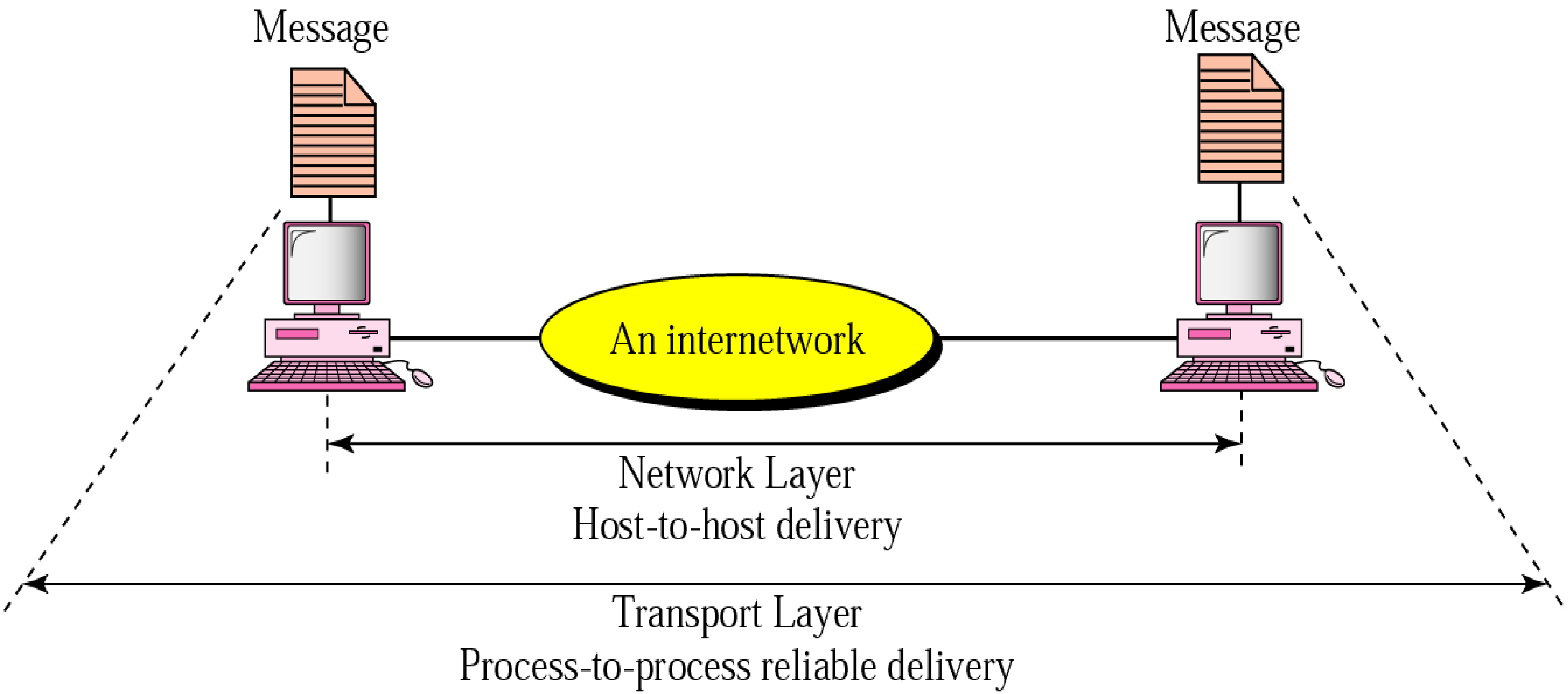
The two protocols used in this layer are:

- **Transmission Control Protocol**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.
  - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.



Message

Message

An internetwork

Network Layer

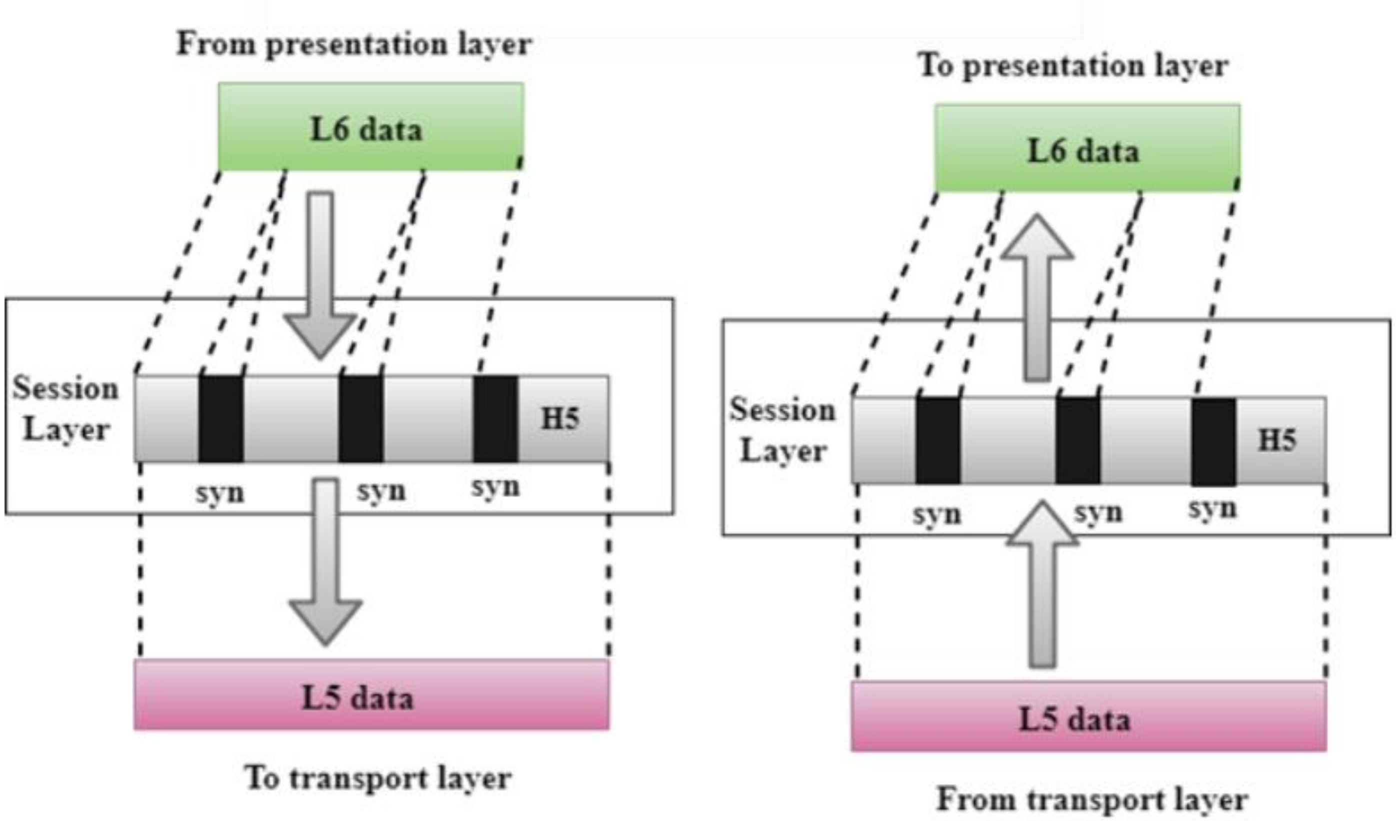
Host-to-host delivery

Transport Layer

Process-to-process reliable delivery

Session Layer

- It is a layer 5 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

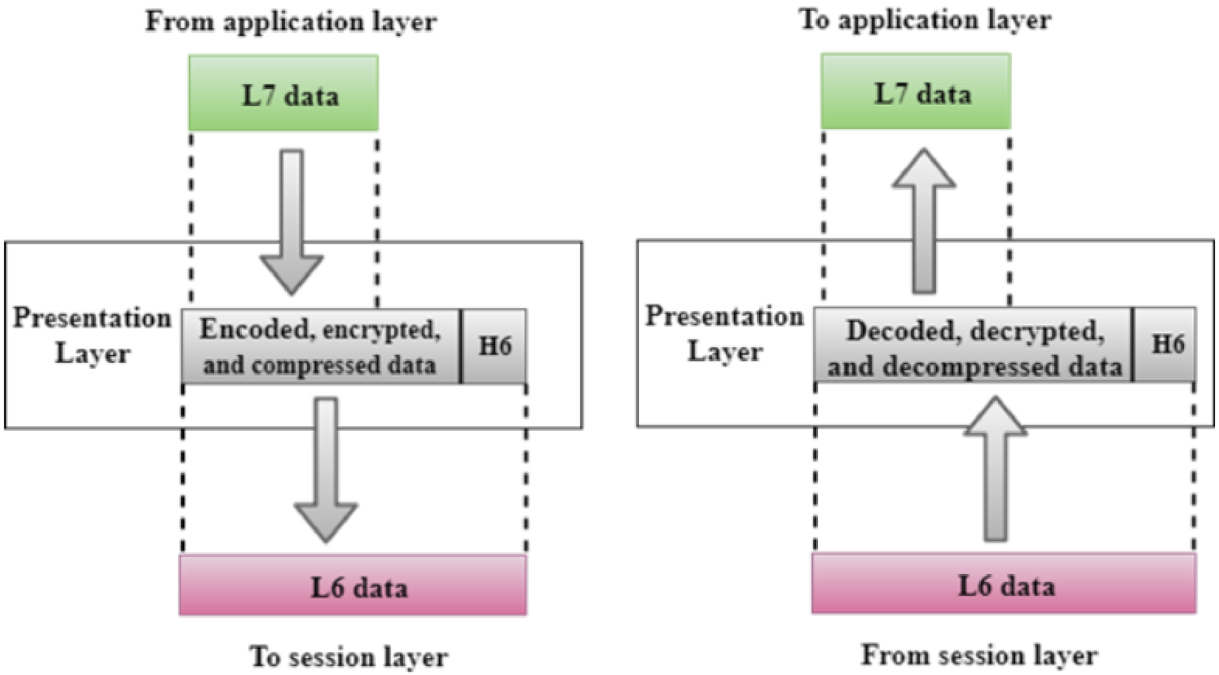


Functions of Session layer

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

Presentation Layer

- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

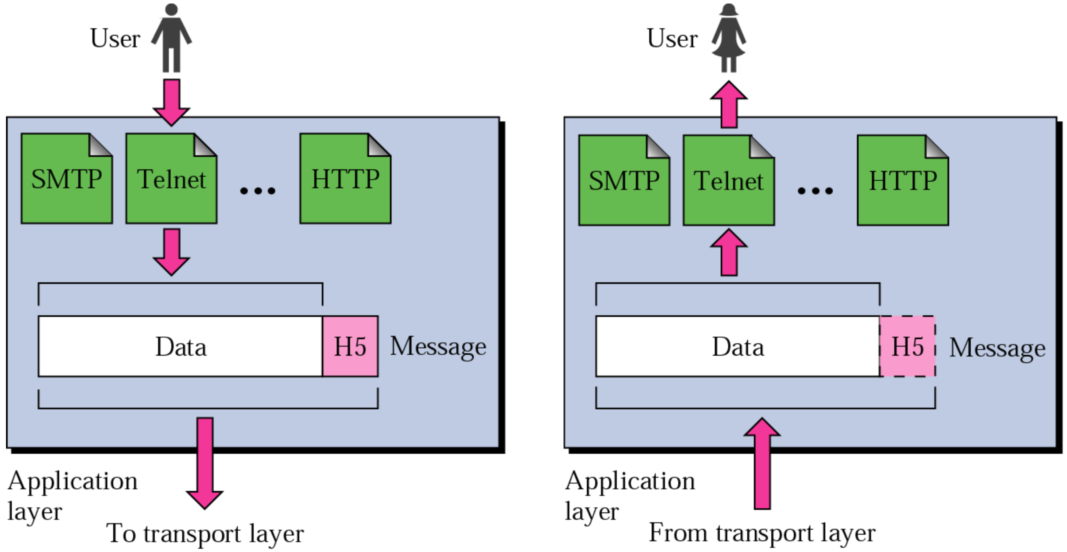


Functions of Presentation layer

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

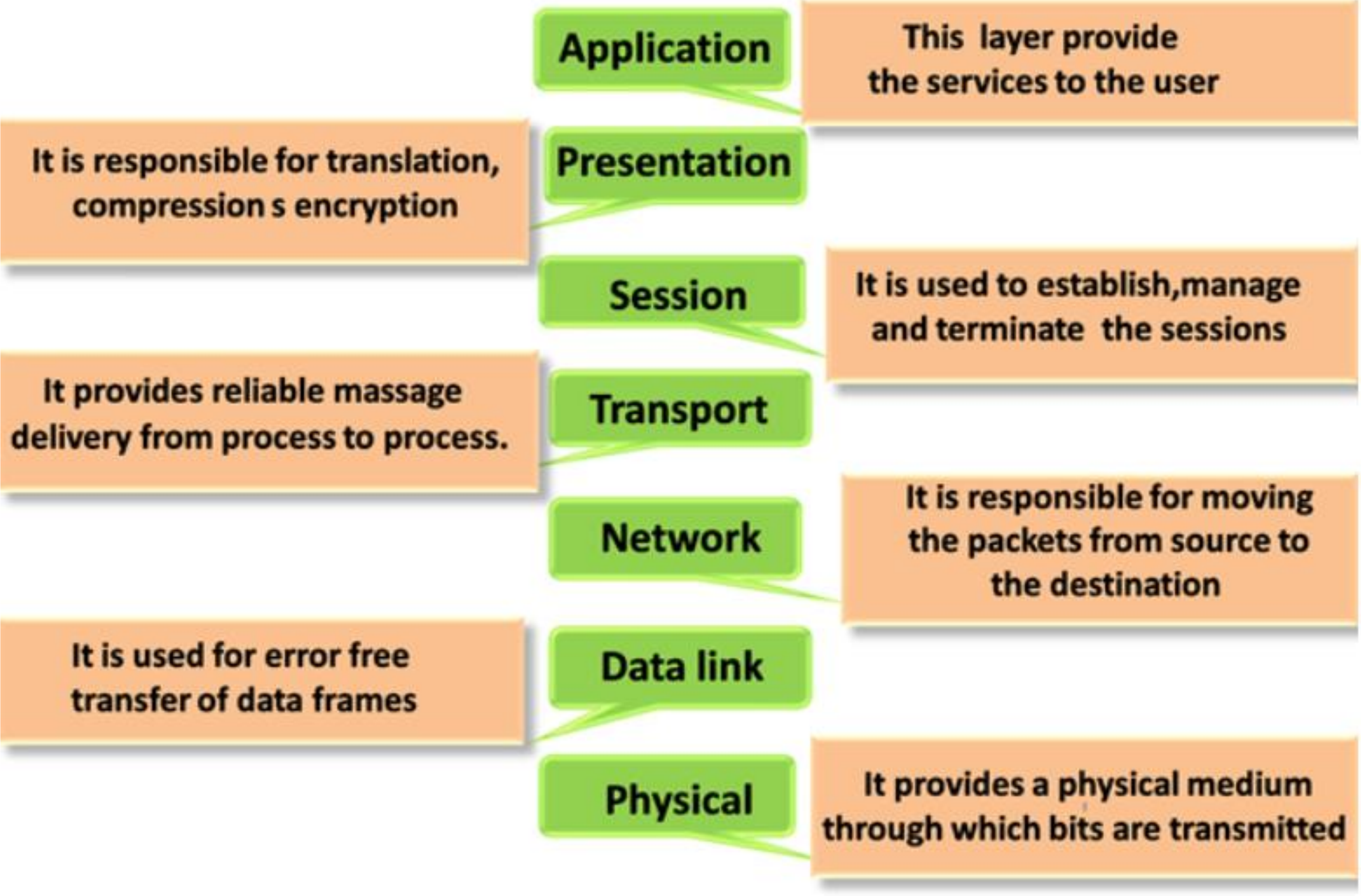
Application Layer

- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.



Functions of Application layer

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- **Directory services:** An application provides the distributed database sources and is used to provide that global information about various objects.



Application

This layer provide the services to the user

Presentation

It is responsible for translation, compression s encryption

Session

It is used to establish,manage and terminate the sessions

Transport

It provides reliable massage delivery from process to process.

Network

It is responsible for moving the packets from source to the destination

Data link

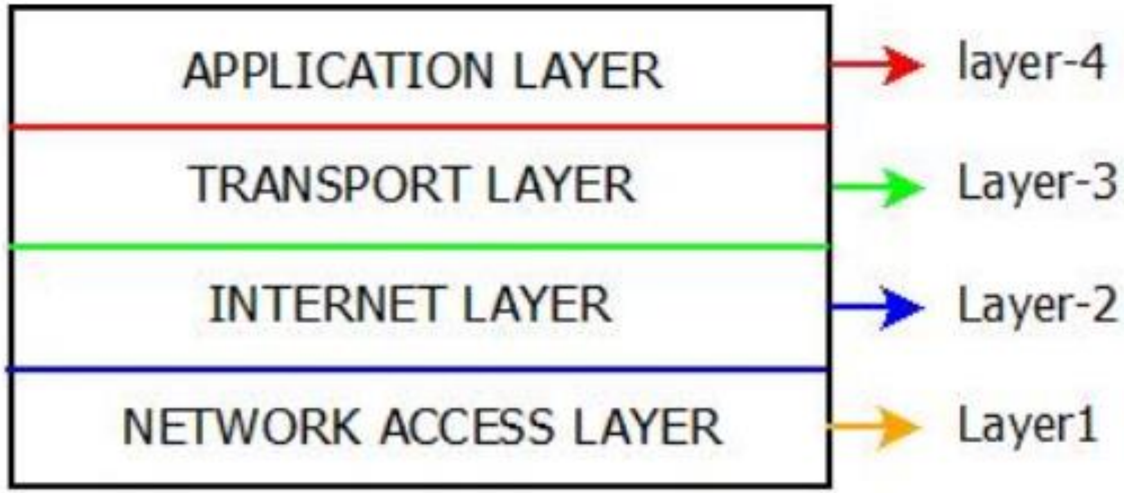
It is used for error free transfer of data frames

Physical

It provides a physical medium through which bits are transmitted

TCP/IP model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.



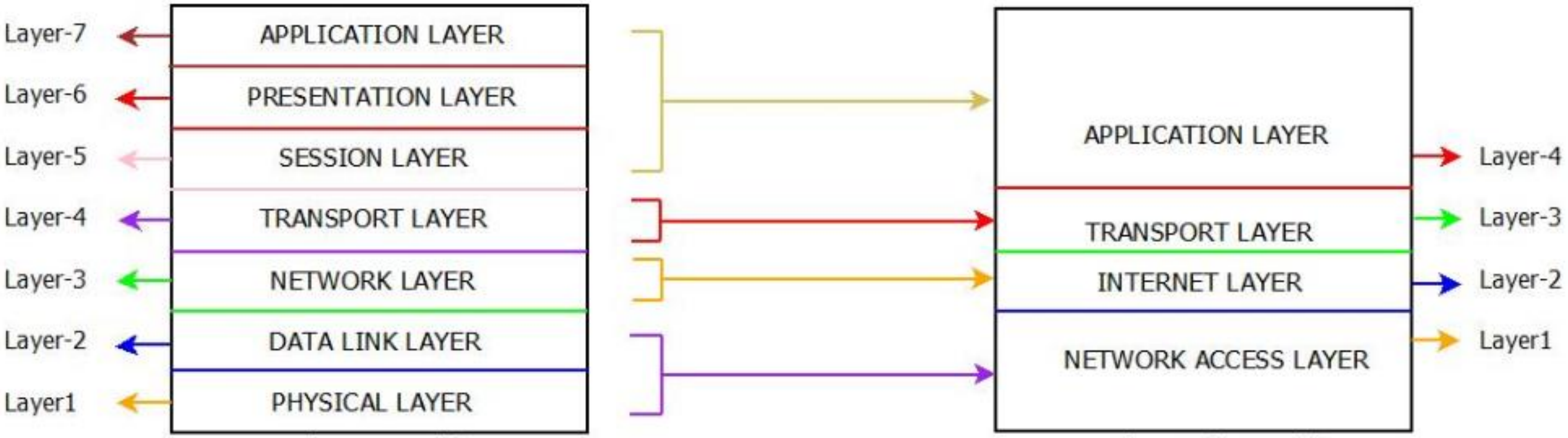
APPLICATION LAYER → layer-4

TRANSPORT LAYER → Layer-3

INTERNET LAYER → Layer-2

NETWORK ACCESS LAYER → Layer1

The TCP/IP Model



Layer-7 ← APPLICATION LAYER

Layer-6 ← PRESENTATION LAYER

Layer-5 ← SESSION LAYER

Layer-4 ← TRANSPORT LAYER

Layer-3 ← NETWORK LAYER

Layer-2 ← DATA LINK LAYER

Layer1 ← PHYSICAL LAYER

APPLICATION LAYER → Layer-4

TRANSPORT LAYER → Layer-3

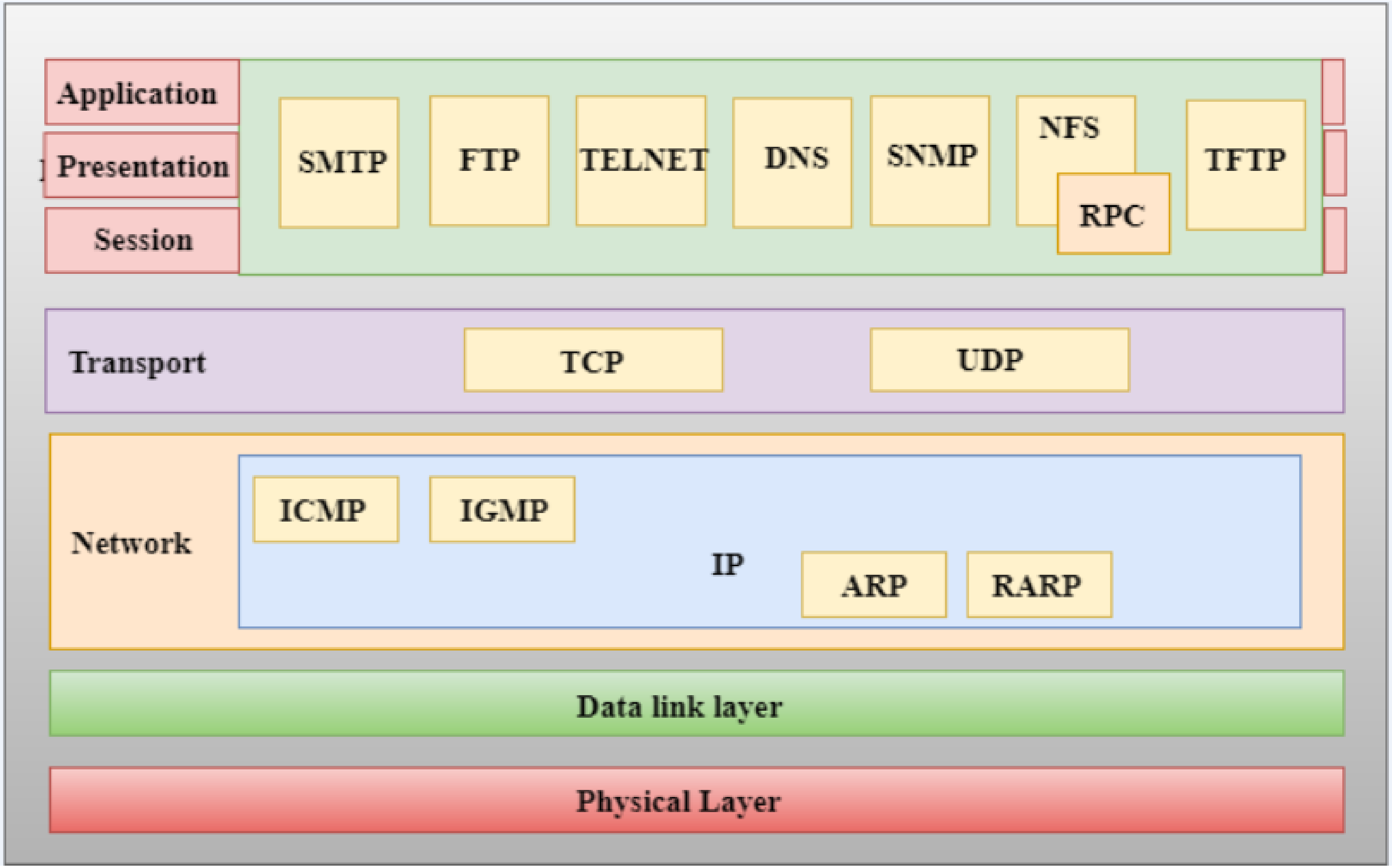
INTERNET LAYER → Layer-2

NETWORK ACCESS LAYER → Layer1

The OSI Model

The TCP/IP Model

Functions of TCP/IP layer



Application

Presentation

Session

SMTP

FTP

TELNET

DNS

SNMP

NFS

RPC

TFTP

Transport

TCP

UDP

Network

ICMP

IGMP

IP

ARP

RARP

Data link layer

Physical Layer

Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- Following protocols are used at this layer:
  - Internet Protocol (IP)
  - Address Resolution Protocol (ARP)
  - Internet Control Message Protocol (ICMP)

Internet Protocol (IP)

- IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.
- Responsibilities of this protocol are:
  - **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
  - **Host-to-host communication:** It determines the path through which the data is to be transmitted.
  - **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
  - **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU).
    - If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network.
    - Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
  - **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

Address Resolution Protocol (ARP)

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol:**
  - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
  - **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- An ICMP protocol mainly uses two terms:
  - **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
  - **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

Transport Layer

- The transport layer is responsible for error-free, end-to-end delivery of data from the source host to the destination host. It corresponds to the transport layer of the OSI model.
- The functions of the transport layer are:
  - It facilitates the communicating hosts to carry on a conversation.
  - It provides an interface for the users to the underlying network.
  - It can provide for a reliable connection. It can also carry out error checking, flow control, and verification.
- The protocols used at transport layer are:
  - User Datagram Protocol (UDP)
  - Transmission Control Protocol (TCP)
  - Stream Control Transmission Protocol (SCTP)

User Datagram Protocol (UDP)

- It provides connectionless service and end-to-end delivery of transmission.
- It is an unreliable protocol as it discovers the errors but not specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
- UDP consists of the following fields:
  - **Source port address:** The source port address is the address of the application program that has created the message.
  - **Destination port address:** The destination port address is the address of the application program that receives the message.
  - **Total length:** It defines the total number of bytes of the user datagram in bytes.
  - **Checksum:** The checksum is a 16-bit field used in error detection.
- UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.

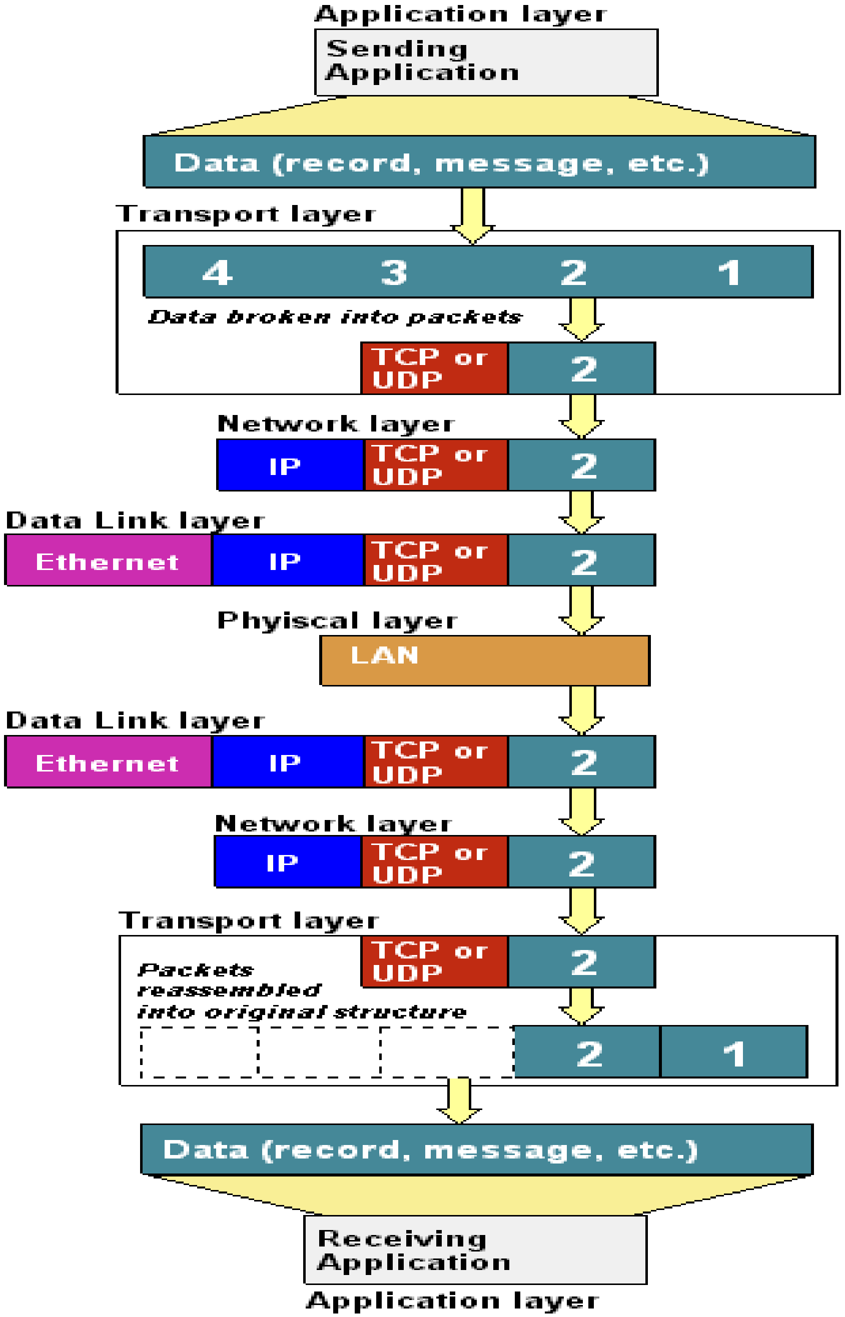
Transmission control protocol (TCP)

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames.
    - Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

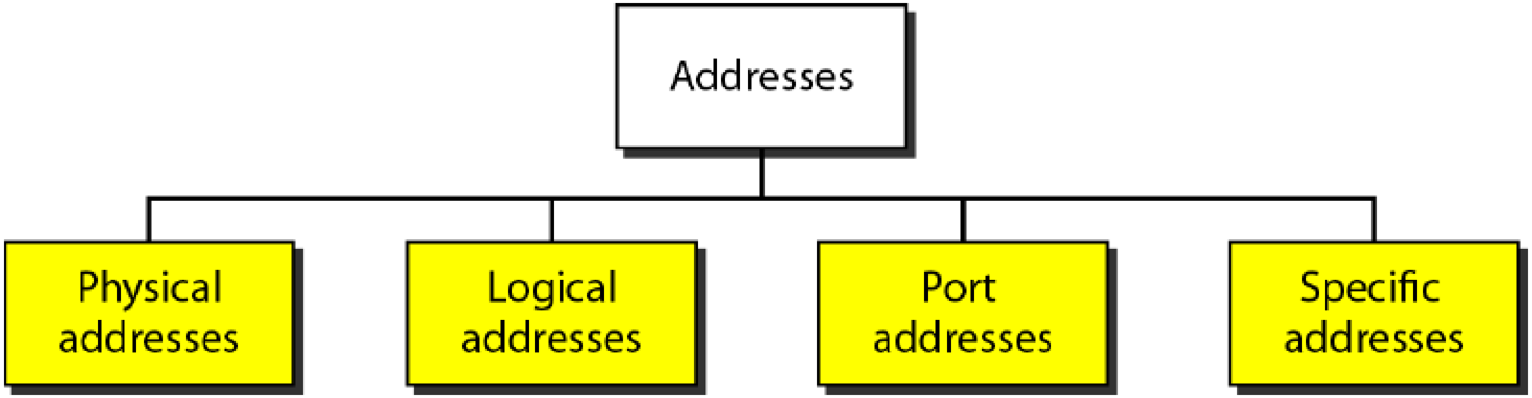
- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system.
  - For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

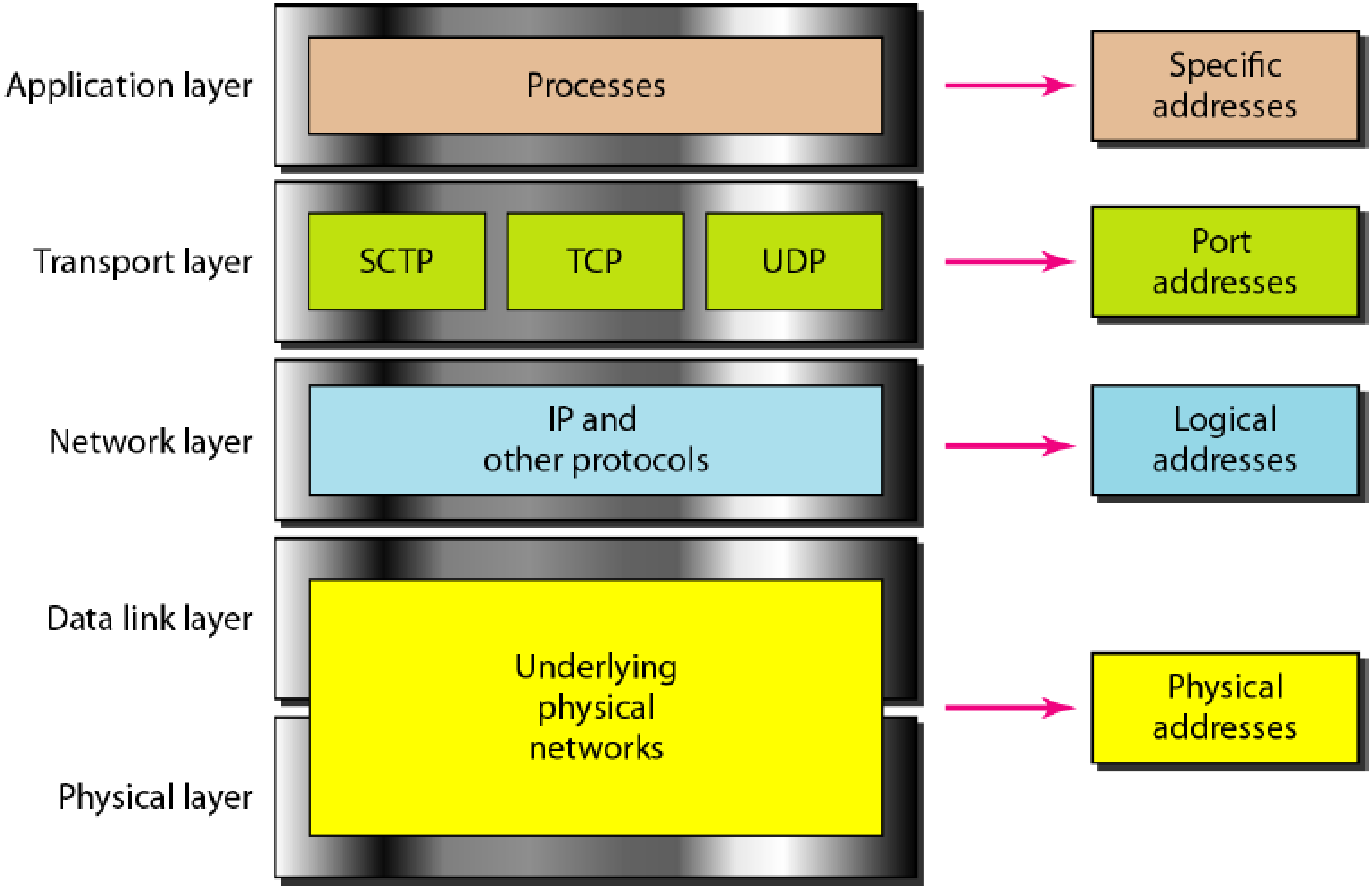
- Following are the main protocols used in the application layer:
  - **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
  - **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
  - **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
  - **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
  - **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
  - **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.


Application layer
Sending Application
Data (record, message, etc.)
Transport layer
4
3
2
1
Data broken into packets
TCP or UDP
2
Network layer
IP
TCP or UDP
2
Data Link layer
Ethernet
IP
TCP or UDP
2
Phyiscal layer
LAN
Data Link layer
Ethernet
IP
TCP or UDP
2
Network layer
IP
TCP or UDP
2
Transport layer
TCP or UDP
2
Packets reassembled into original structure
2
1
Data (record, message, etc.)
Receiving Application
Application layer

Addressing Mechanisms

- Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.

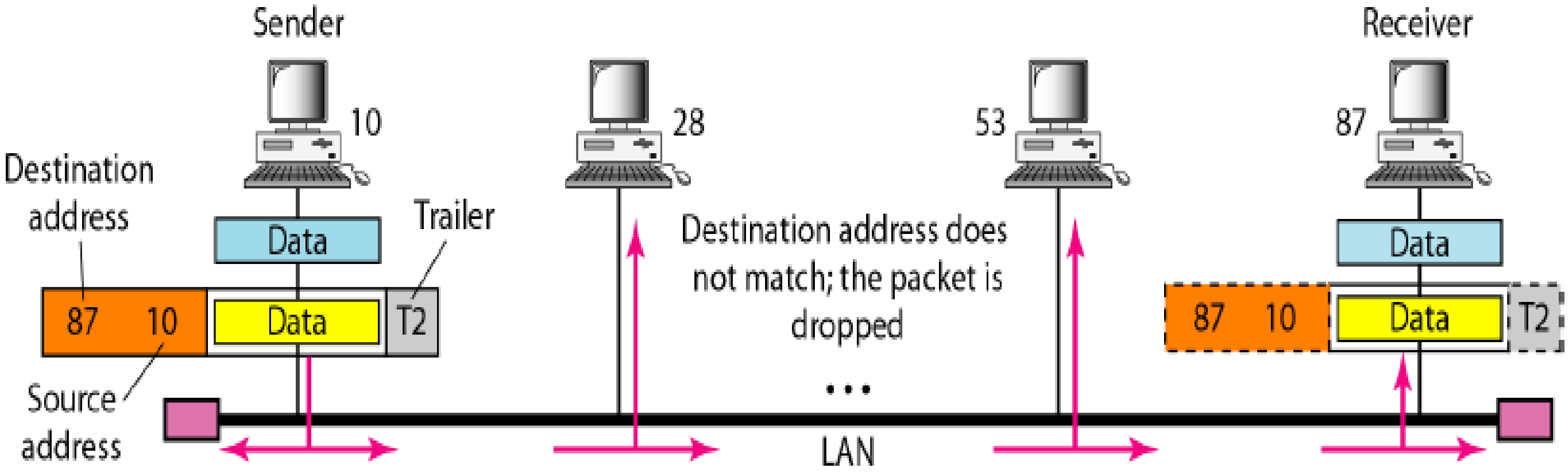



Application layer
Transport layer
Network layer
Data link layer
Physical layer
Processes
SCTP
TCP
UDP
IP and other protocols
Underlying physical networks
Specific addresses
Port addresses
Logical addresses
Physical addresses

Physical Address

- The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN.
- The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address.
- Physical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (to be received by all systems in the network.
  - 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: A 6-byte (12 hexadecimal digits) physical address 07:01:02:01:2C:4B

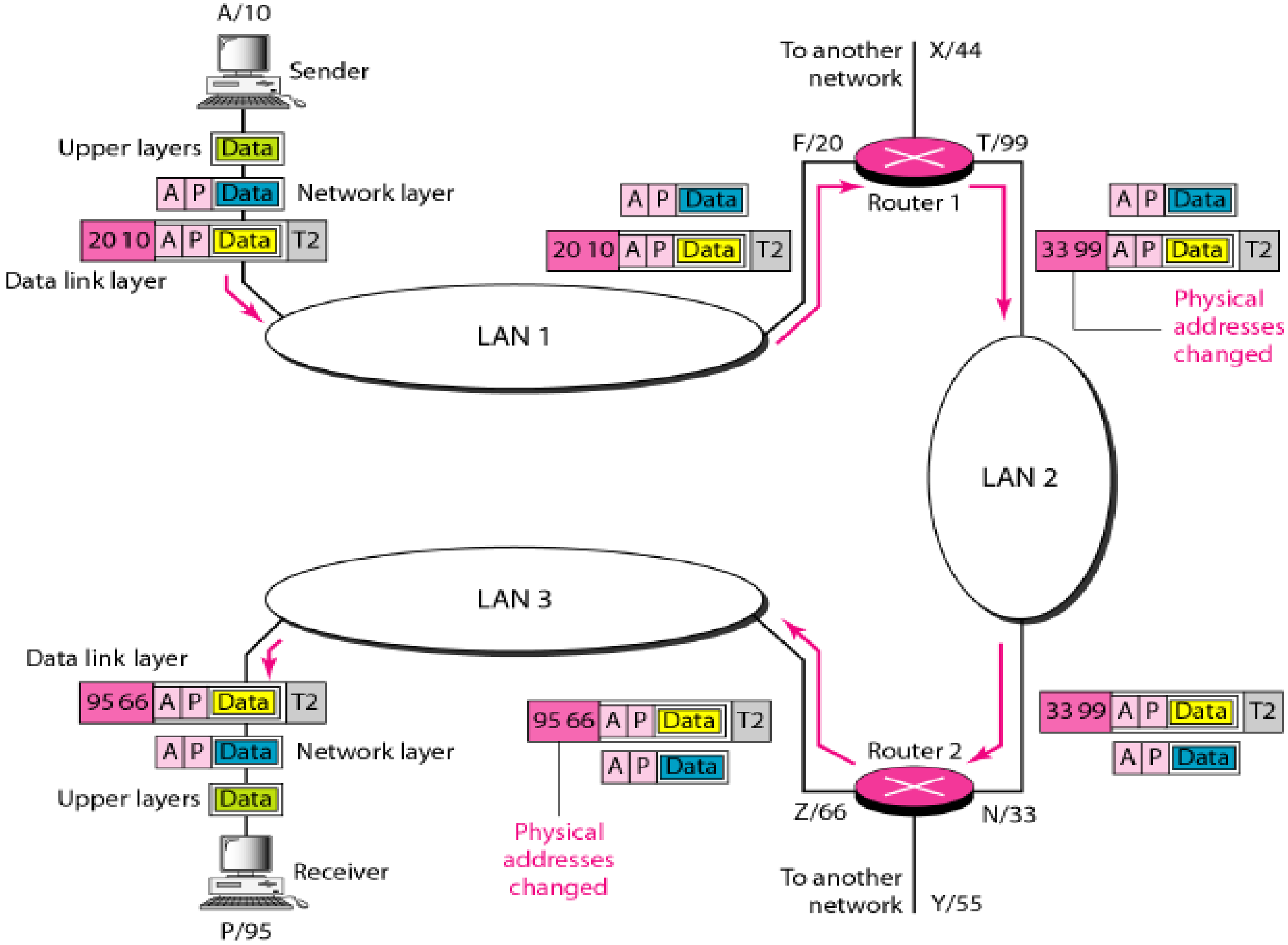
- In Figure a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). As the figure shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver.



Logical Address

- Logical addresses are used by networking software to allow packets to be independent of the physical connection of the network, that is, to work with different network topologies and types of media.
- A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. An internet address in IPv4 in decimal numbers **132.24.75.9**
- No two publicly addressed and visible hosts on the Internet can have the same IP address.
- The physical addresses will change from hop to hop, but the logical addresses remain the same.
- The logical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (all systems in the network). There are limitations on broadcast addresses.

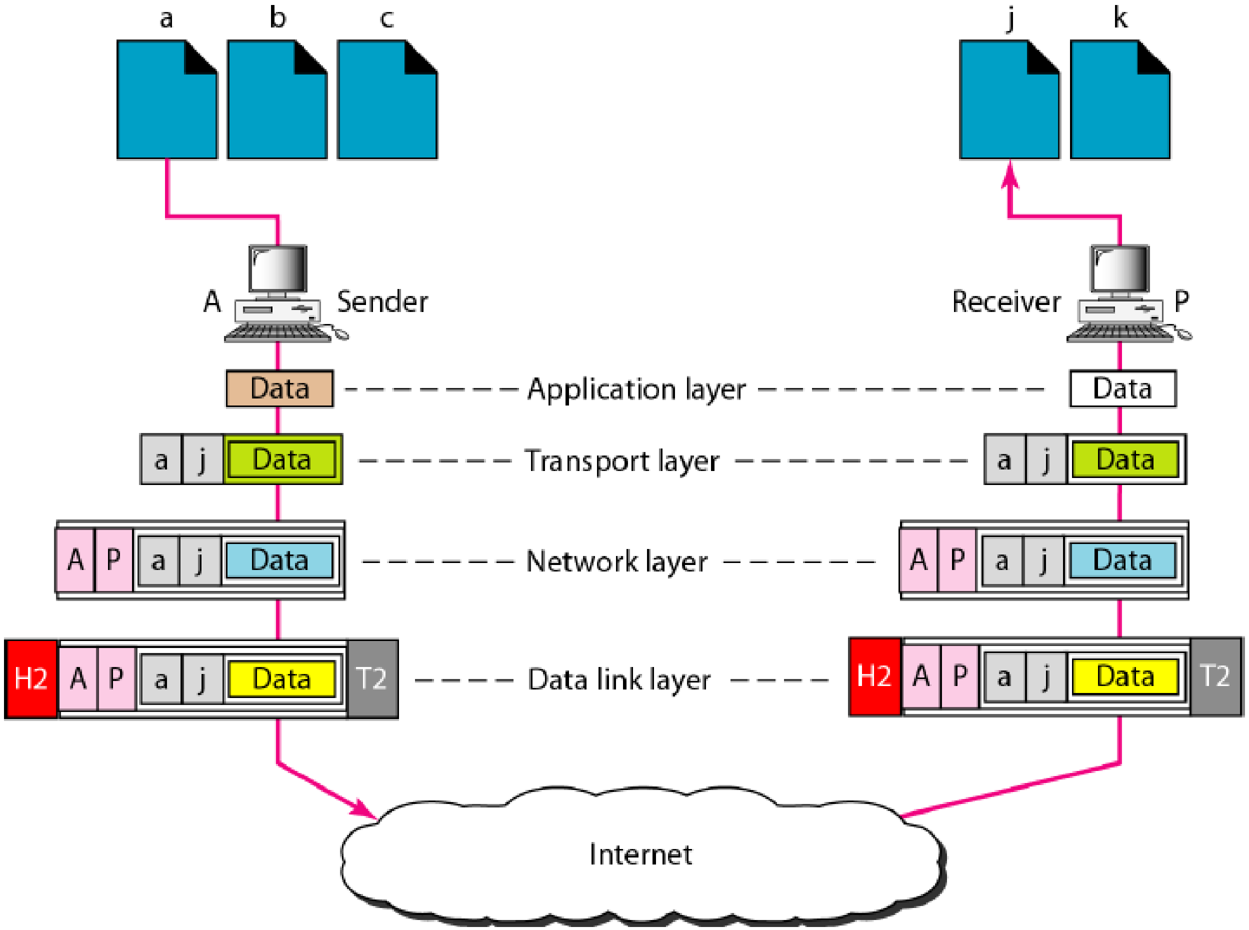
- Figure shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however,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

- There are many application running on the computer. Each application run with a port no.(logically) on the computer.
- A port number is part of the addressing information used to identify the senders and receivers of messages.
- Port numbers are most commonly used with TCP/IP connections.
- These port numbers allow different applications on the same computer to share network resources simultaneously.
- The physical addresses change from hop to hop, but the logical and port addresses usually remain the same.
- Example: a port address is a 16-bit address represented by one decimal number **753**

- 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.



Application-Specific Addresses

- Some applications have user-friendly addresses that are designed for that specific application.
- Examples include the e-mail address (for example, xyz@gmail.com) and the Universal Resource Locator (URL) (for example, www.gmail.com). The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web.