Chapter 2: Network Models

Network Models

- Computer networks are created by different entities. Standards are needed so that these heterogeneous networks can communicate with one another.
- The two best-known standards are:
    - the OSI model and
    - the Internet model
- The OSI (Open Systems Interconnection) model defines a seven-layer network; the Internet model defines a five-layer network.

THE INTERNET

- Count the ways you've used the Internet recently. Perhaps you've sent electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule-all by using the Internet.
- Or maybe you researched a medical topic, booked a hotel reservation, chatted with a fellow Trekkie, or comparison-shopped for a car.
- The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.
- The Internet is a structured, organized system. We begin with a brief history of the Internet. We follow with a description of the Internet today.

A Brief History

- A network is a group of connected communicating devices such as computers and printers.
- An internet (note the lowercase letter i) is two or more networks that can communicate with each other.
- The most notable internet is called the Internet.
- In the mid-1960s, mainframe computers in research organizations were standalone devices. Computers from different manufacturers were unable to communicate with one another.
- The Advanced Research Projects Agency (ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.

A Brief History

- In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers.
- By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the *Network Control Protocol (NCP) provided communication* between the hosts.

A Brief History

- In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the Internetting Projec1.
- Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of packets.
- This paper on Transmission Control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway.

A Brief History

- Shortly thereafter, authorities made a decision to split TCP into two protocols: Transmission Control Protocol (TCP) and Internetworking Protocol (IP).
- IP would handle datagram routing while TCP would be responsible for higher-level functions such as segmentation, reassembly, and error detection. The internetworking protocol became known as TCPIIP.

The Internet Today

- The Internet today is not a simple hierarchical structure. It is made up of many wide- and local-area networks joined by connecting devices and switching stations.
- It is difficult to give an accurate representation of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed.

Protocol

- All parties involved in a communication must agree in a set of rules to be used when exchanging messages.
- Thus, the set of rules which both the sender and the receiver all comply with is called protocol.
- The sending device cannot just send the data and expect the receiving device to receive and further interpret it correctly.
- When the sender sends a message it may consist of text, number, images, etc. which are converted into bits and grouped into blocks to be transmitted and often certain additional information called control information is also added to help the receiver interpret the data.
- A Protocol is defined as a set of rules that governs data communications.
- A protocol defines what is to be communicated, how it is to be communicated and when it is to be communicated.

Elements of a Protocol

- There are three key elements of a protocol:
- A. Syntax: It means the structure or format of the data. It is the arrangement of data in a particular order.
- B. Semantics: It tells the meaning of each section of bits and indicates the interpretation of each section.
- It also tells what action/decision is to be taken based on the interpretation.
- C. Timing: It tells the sender about the readiness of the receiver to receive the data. It tells the sender at what rate the data should be sent to the receiver to avoid overwhelming the receiver.

Standards in Networking

- Standards are necessary in networking to ensure interconnectivity and interoperability between various networking hardware and software components.
- Without standards we would have proprietary products creating isolated islands of users which cannot interconnect.
- Standards provide guidelines to product manufacturers and vendors to ensure national and international interconnectivity.
- Data communications standards are classified into two categories:

Standards in Networking

- 1. De facto Standard: These are the standards that have been traditionally used and mean by fact or by convention
- These standards are not approved by any organized body but are adopted by widespread use.
- 2. De jure standard: It means by law or by regulation.
- These standards are legislated and approved by a body that is officially recognized.

Standards in Networking

- Standard Organizations for Networking
- Standards are created by standards creation committees, forums, and government regulatory agencies.
- <u>Examples of Standard Creation Committees :</u>
- 1. International Organization for Standardization(ISO)
- 2. International Telecommunications Union – Telecommunications Standard (ITU-T)
- 3. American National Standards Institute (ANSI)
- 4. Institute of Electrical & Electronics Engineers (IEEE)
- 5. Electronic Industries Associates (EIA)
- 6. Internet Research Task Force (IETF)

Layered Task

- i. The main objective of a computer network is to be able to transfer the data from sender to receiver.
- This task can be done by breaking it into small sub tasks, each of which are well defined.
- ii. Each subtask will have its own process or processes to do and will take specific inputs and give specific outputs to the subtask before or after it.
- In more technical terms we can call these sub tasks as layers.
- iii. In general, every task or job can be done by dividing it into sub task or layers.
- Consider the example of sending a letter where the sender is in City A and receiver is in city B.
- iv. The process of sending letter is shown below:

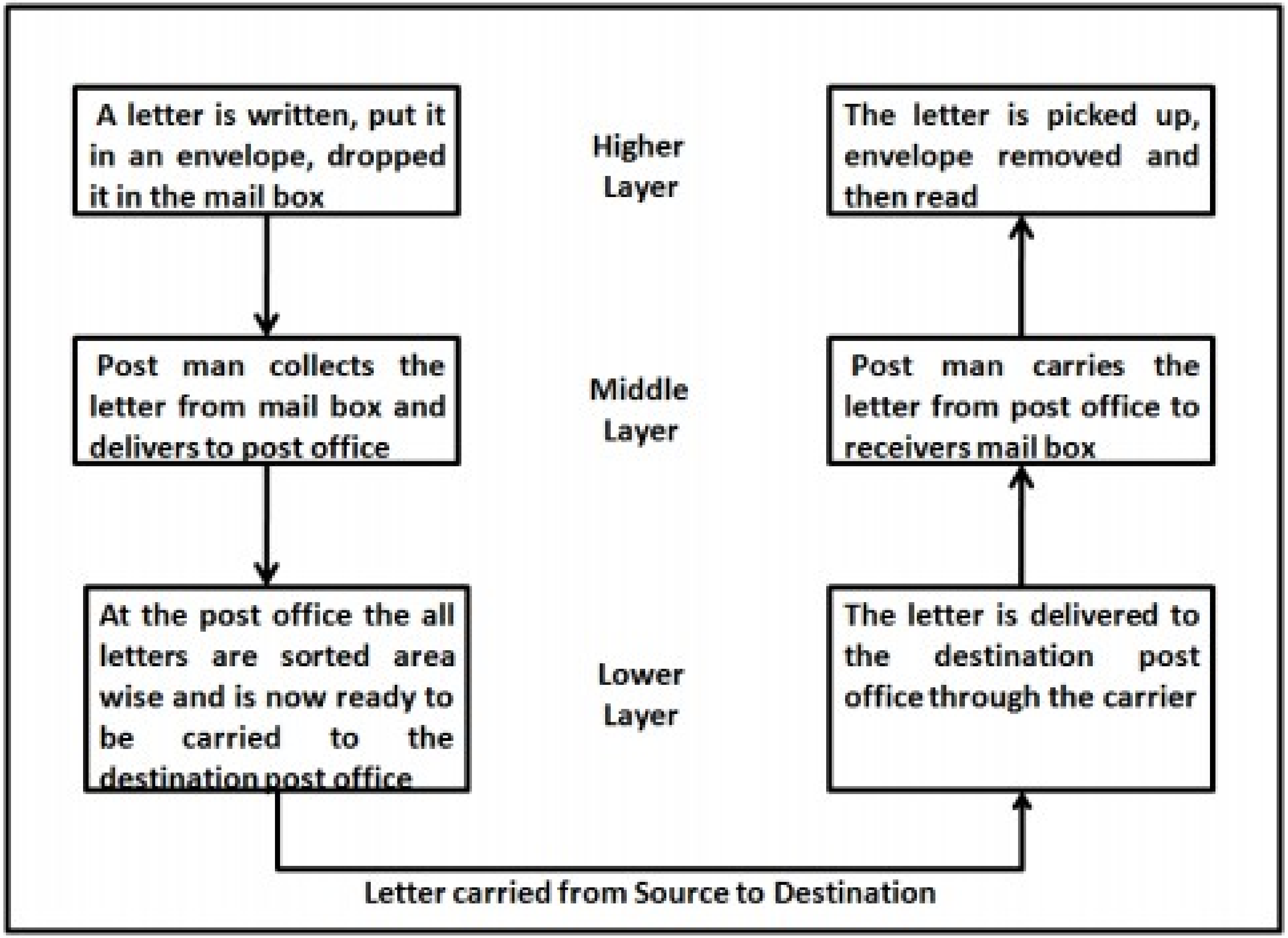


Fig: Concept of layer task: sending a letter

Layered Task

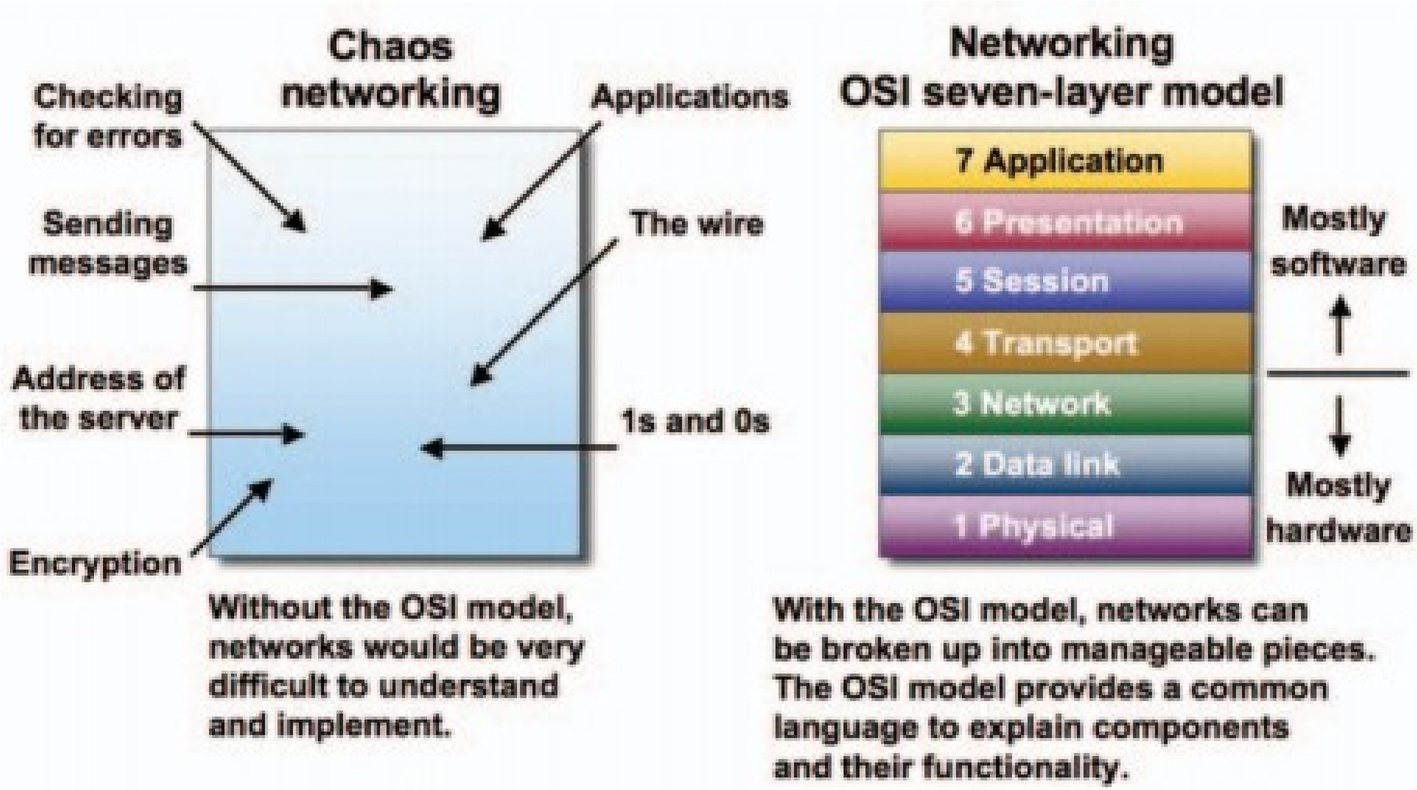
- v. The above figure shows
  - a. Sender, Receiver & Carrier
  - b. Hierarchy of layers
- vi. At the sender site, the activities take place in the following descending order:
  - a. Higher Layer: The sender writes the letter along with the sender and receivers address and put it in an envelope and drop it in the mailbox.
  - b. Middle Layer: The letter is picked up by the post man and delivered to the post office
  - c. Lower Layer: The letters at the post office are sorted and are ready to be transported through a carrier.
- vii. During transition the letter may be carried by truck, plane or ship or a combination of transport modes before it reaches the destination post office.

Layered Task

- viii. At the Receiver site, the activities take place in the following ascending order:
  - a. Lower Layer: The carrier delivers the letter to the destination post office
  - b. Middle Layer: After sorting, the letter is delivered to the receivers mail box
  - c. Higher Layer: The receiver picks up the letter, opens the envelope and reads it.
- ix. Hierarchy of layers: The activities in the entire task are organized into three layers. Each activity at the sender or receiver side occurs in a particular order at the hierarchy.
- x. The important and complex activities are organized into the Higher Layer and the simpler ones into middle and lower layer.

Why to have a model?

- The purpose of the OSI reference model is to guide technology vendors and developers so the digital communications products and software programs they create can interoperate and to promote a clear framework that describes the functions of a networking or telecommunications system that's in use.



Layered Architecture of OSI Model

- The OSI model has 7 layers each with its own dedicated task.
- A message sent from Device A to Device B passes through all layers at A from top to bottom then all layers at B from bottom to top as shown in the figure below.
- At Device A, the message is sent from the top layer i.e. Application Layer A then all the layers till it reaches its physical layer and then it is transmitted through the transmission medium.
- At Device B, the message received by the physical layer passes through all its other layers and moves upwards till it reaches its Application Layer.

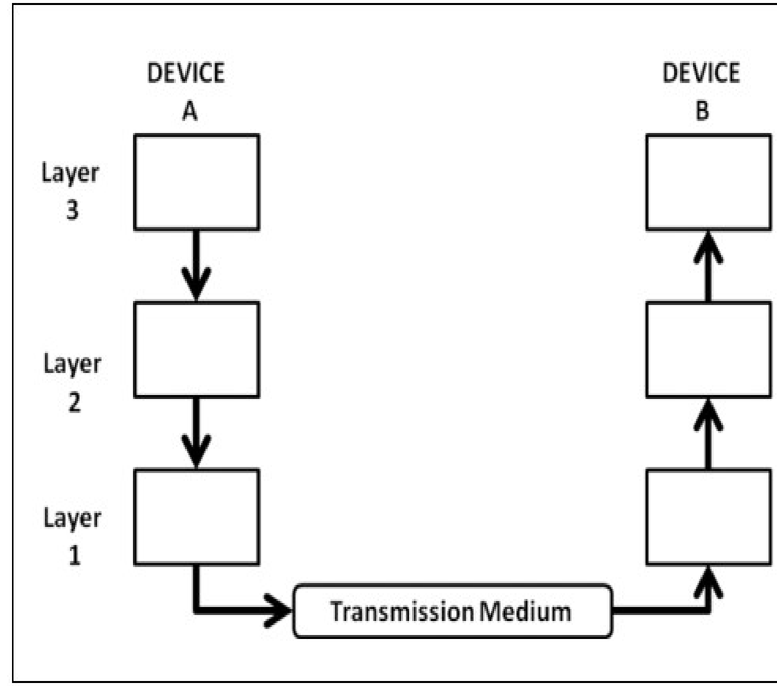


Fig: Flow of Data from Device A to Device B through various layers

Layered Architecture of OSI Model

- As the message travels from device A to device B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model as shown be

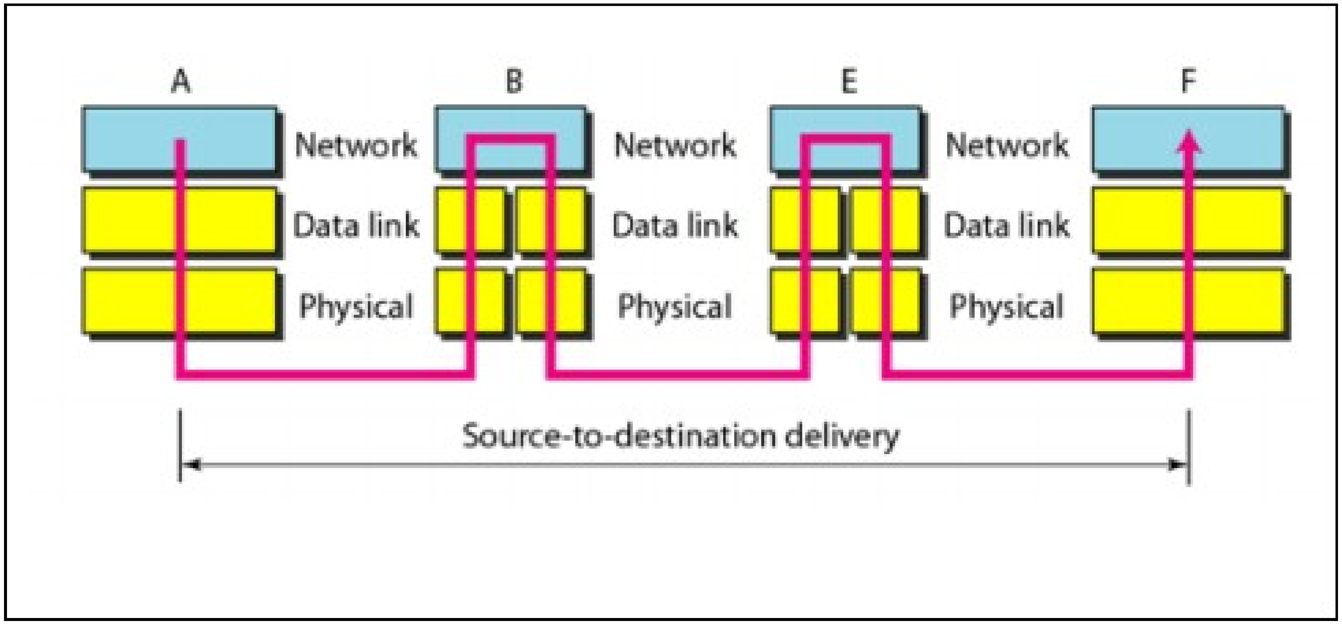


Fig: Data Transfer through Intermediate nodes

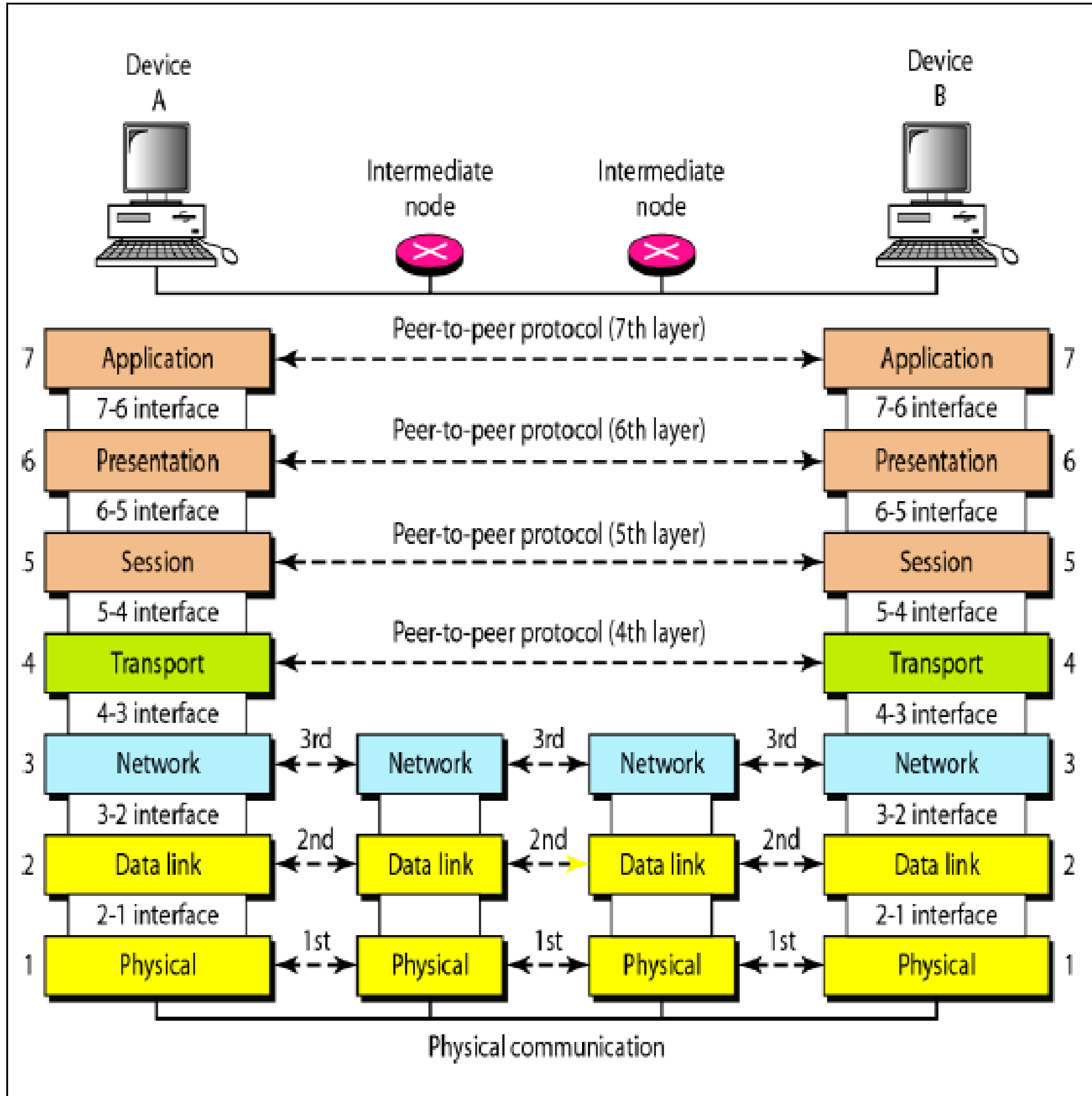
- The Data Link layer determines the next node where the message is supposed to be forwarded and the network layer determines the final recipient.

Communication & Interfaces

- For communication, 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.
- Each layer in the receiving device removes the information added at the corresponding layer and sends the obtained data to the layer above it.
- Every Layer has its own distinct function or services.
- On every sending device, each layer calls upon the service offered by the layer below it.
- On every receiving device, each layer calls upon the service offered by the layer above it.
- Between two devices, the layers at corresponding levels communicate with each other i.e. layer 2 at receiving end can communicate and understand data from layer 2 of sending end.
- This is called peer –to – peer communication.

- For this communication to be possible between every two adjacent layers there is an interface.
- An interface defines the service that a layer must provide.
- Every layer has an interface to the layer above and below it as shown in the figure.

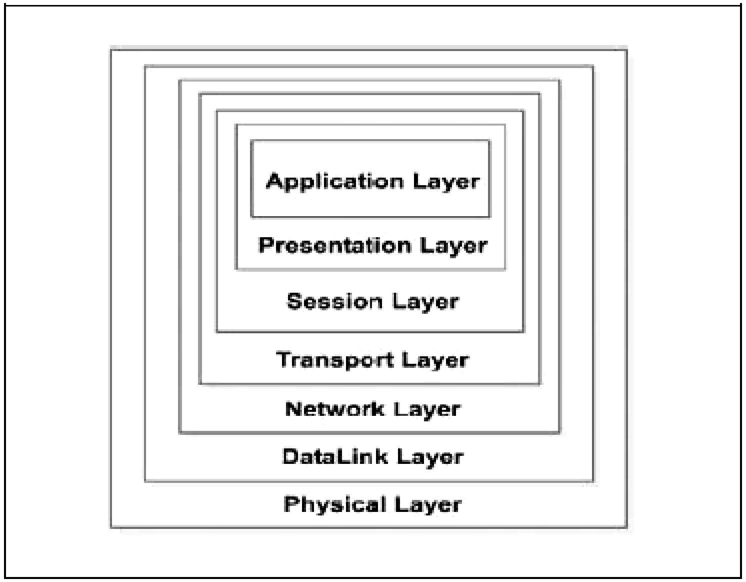
Fig: Communication & Interfaces in the OSI model



Encapsulation of Data

- As shown in the figure above the data at layer 7 i.e. the Application layer along with the header added at layer 7 is given to layer 6, the Presentation layer.
- This layer adds Its header and passed the whole package to the layer below.
- The corresponding layers at the receiving side removes the corresponding header added at that layer and sends the remaining data to the above layer.
- The above process is called encapsulation.

Fig: Encapsulation



The OSI Model

- Open Systems Interconnection (OSI).
- Developed by the International Organization for Standardization (ISO).
- Model for understanding and developing computer-to-computer communication architecture that is flexible, robust and interoperable.
- It is not a protocol.
- Developed in the 1980s.
- Divides network architecture into seven layers.

OSI cont.

- Each layer performs a subset of the required communication functions
- Each layer relies on the next lower layer to perform more primitive functions
- Each layer provides services to the next higher layer
- Changes in one layer should not require changes in other layers
- Layer 1,2,3 are the network support layer, deals with the physical aspects of moving data from one device to another.
- Layer 5,6,7 are the user support layer, allow the interoperability among unrelated software.
- Layer 4 ensures that what the lower layer have transmitted is in a form that the upper layers can use.

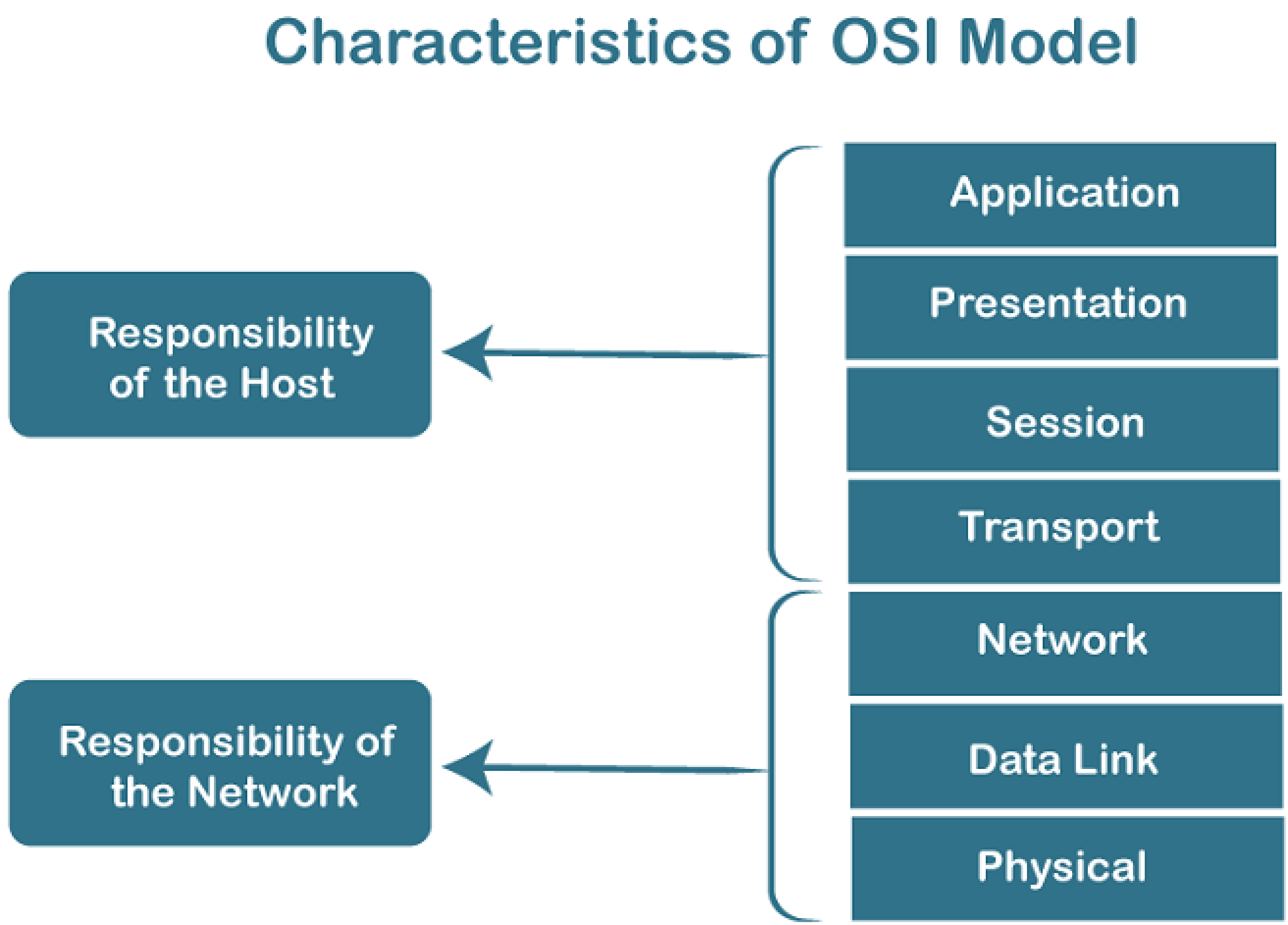
OSI layer

- Application layer
- Presentation layer
- Session layer
- Transport layer
- Network layer
- Data Link layer
- Physical layer

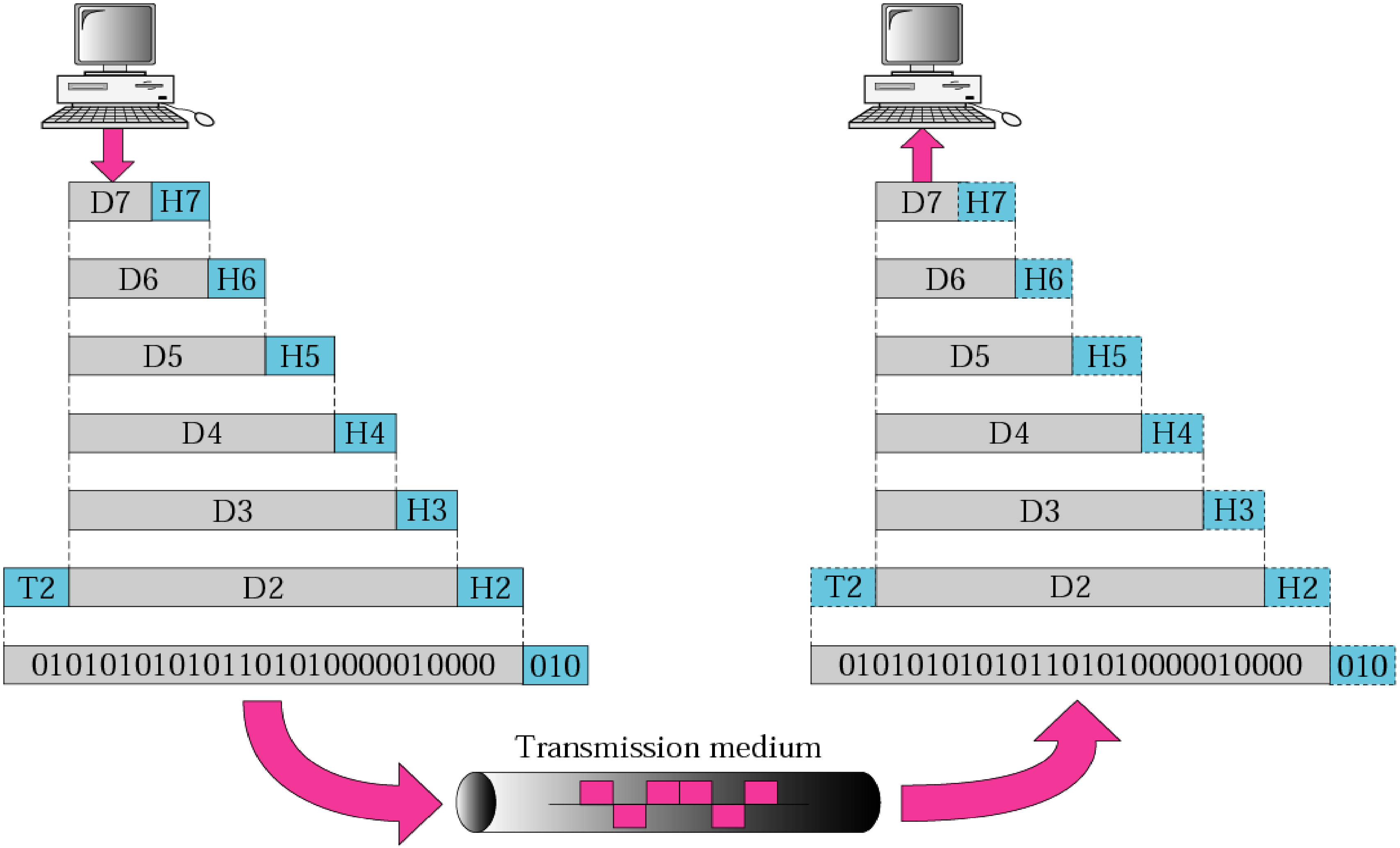
Protocol Data Units (PDU)

- At each layer, protocols are used to communicate with other layers.
- Control information is added to user data at each layer.
- For example, the transport layer may fragment user data.
- Each fragment has a transport header added:
  - Destination Address
  - Sequence number
  - Error detection code
- This creates a *transport protocol data unit (TPDU)*.

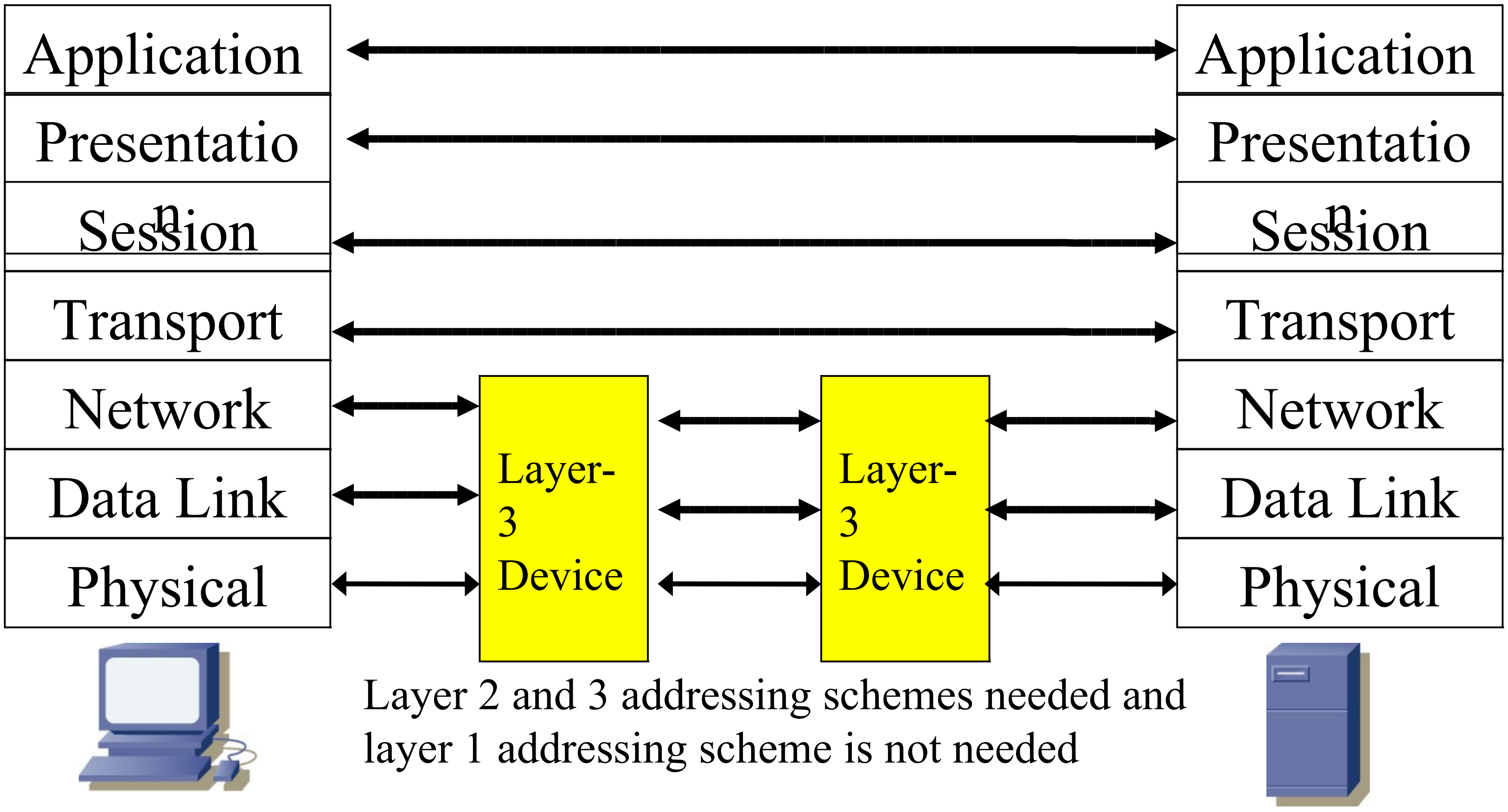
OSI layer


Characteristics of OSI Model
Responsibility of the Host
Responsibility of the Network
Application
Presentation
Session
Transport
Network
Data Link
Physical

An exchange using the OSI model



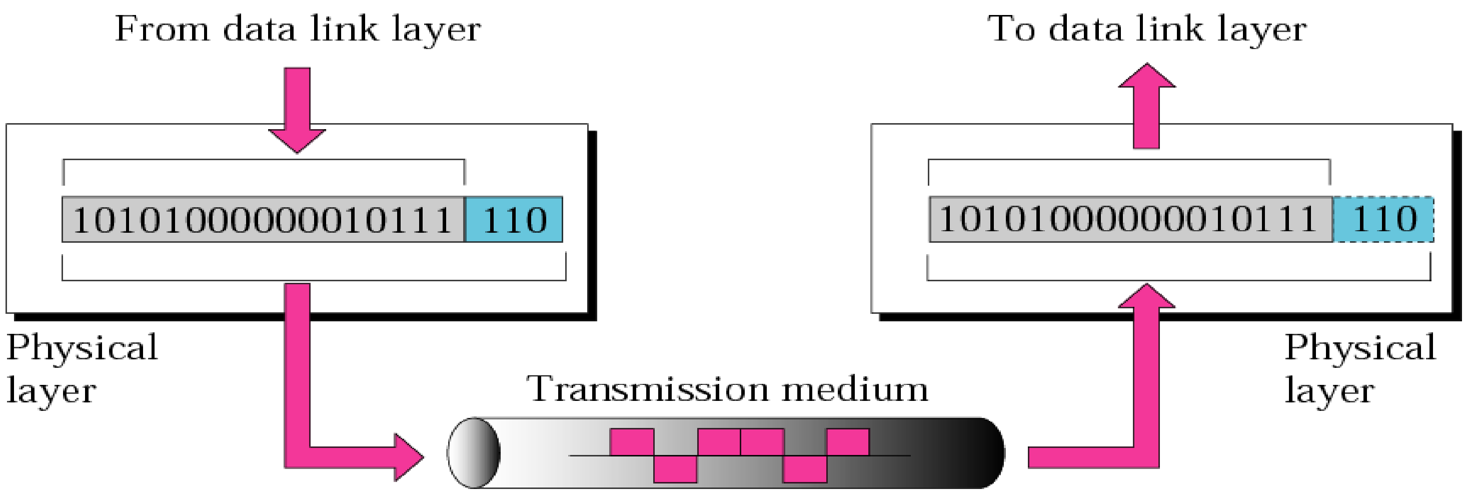
Layer 1,2,3

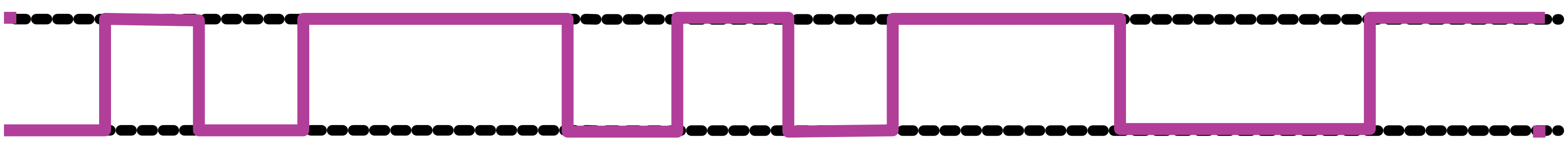

Application
Presentation
Session
Transport
Network
Data Link
Physical
Layer-3 Device
Layer-3 Device
Application
Presentation
Session
Transport
Network
Data Link
Physical
Layer 2 and 3 addressing schemes needed and layer 1 addressing scheme is not needed

Layer 1: Physical Layer

- **Physical Layer**
- **I.** The Physical Layer provides a standardized interface to physical transmission media, including :
- a. Mechanical specification of electrical connectors and cables, for example maximum cable length
- b. Electrical specification of transmission line
- c. Bit-by-bit or symbol-by-symbol delivery
- **II.** On the sender side, the physical layer receives the data from Data Link Layer and encodes it into signals to be transmitted onto the medium.
- On the receiver side, the physical layer receives the signals from the transmission medium decodes it back into data and sends it to the Data Link Layer as shown in the figure below:
- **III.** Interface
- The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.

Physical Layer cont.





Layer 1: Physical Layer

- **IV. Representation of bits**
- The physical layer is concerned with transmission of signals from one device to another which involves converting data (1's & 0's) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.
- **V. Data rate**
- The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.
- **VI. Synchronization of bits**
- To interpret correct and accurate data the sender and receiver have to maintain the same bit rate and also have synchronized clocks.
- **VII. Line configuration**
- The physical layer defines the nature of the connection .i.e. a point to point link, or a multi point link.

Layer 1: Physical Layer

- **VIII. Physical Topology**
- The physical layer defines the type of topology in which the device is connected to the network. In a mesh topology it uses a multipoint connection and other topologies it uses a point to point connection to send data.
- **IX. Transmission mode**
- The physical layer defines the direction of data transfer between the sender and receiver. Two devices can transfer the data in simplex, half duplex or full duplex mode
- **X. Main responsibility of the physical layer**
- Transmission of bits from one hop to the next.

Layer 2: Data Link layer

- **I.** The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
- **II. Framing:** 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 is shown in the figure below:
- **III. Physical Addressing** (inside / outside senders network)
  - a. The Data link layer appends the physical address in the header of the frame before sending it to physical layer.
  - b. The physical address contains the address of the sender and receiver.

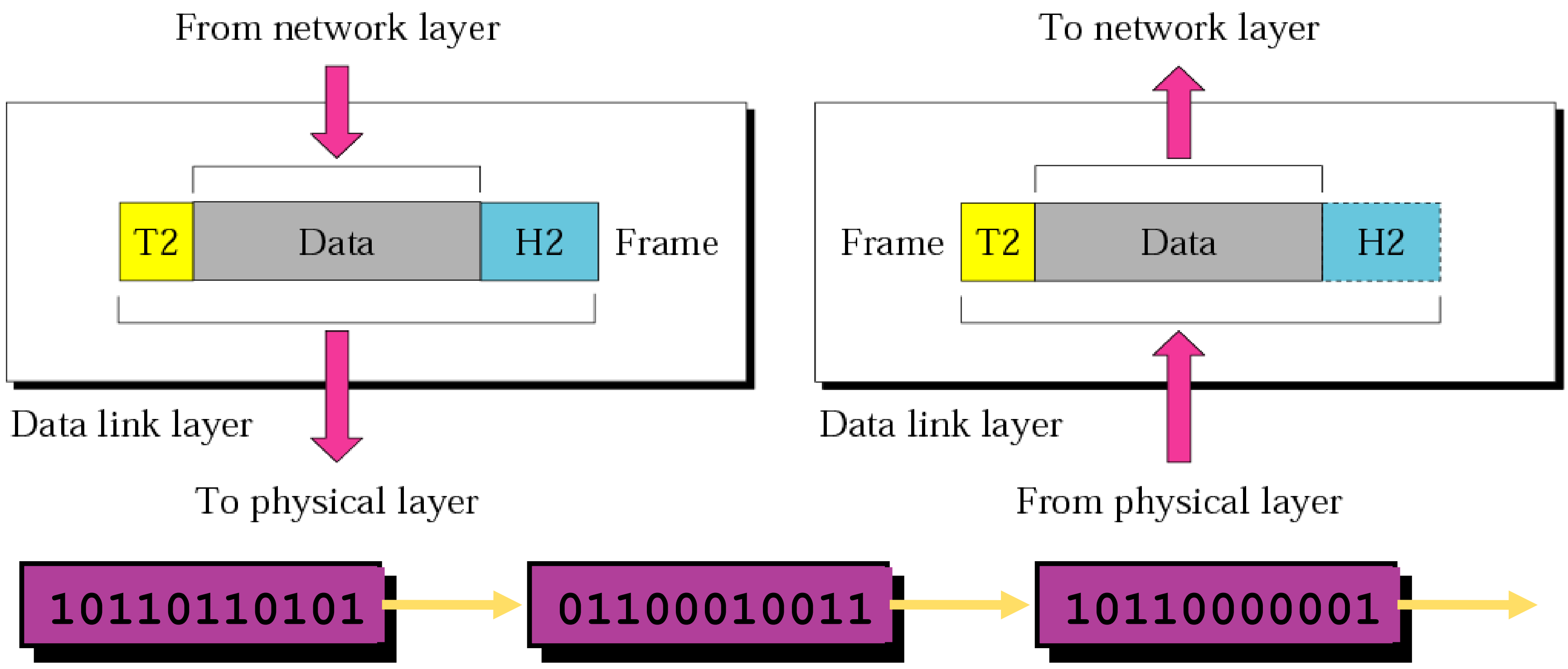
Layer 2: Data Link layer

- c. In case the receiver happens to be on the same physical network as the sender; the receiver address contains the receiver‘s physical address.
- d. In case the receiver is not directly connected to the sender, the physical address is the address of the next node where the data is supposed to be delivered.

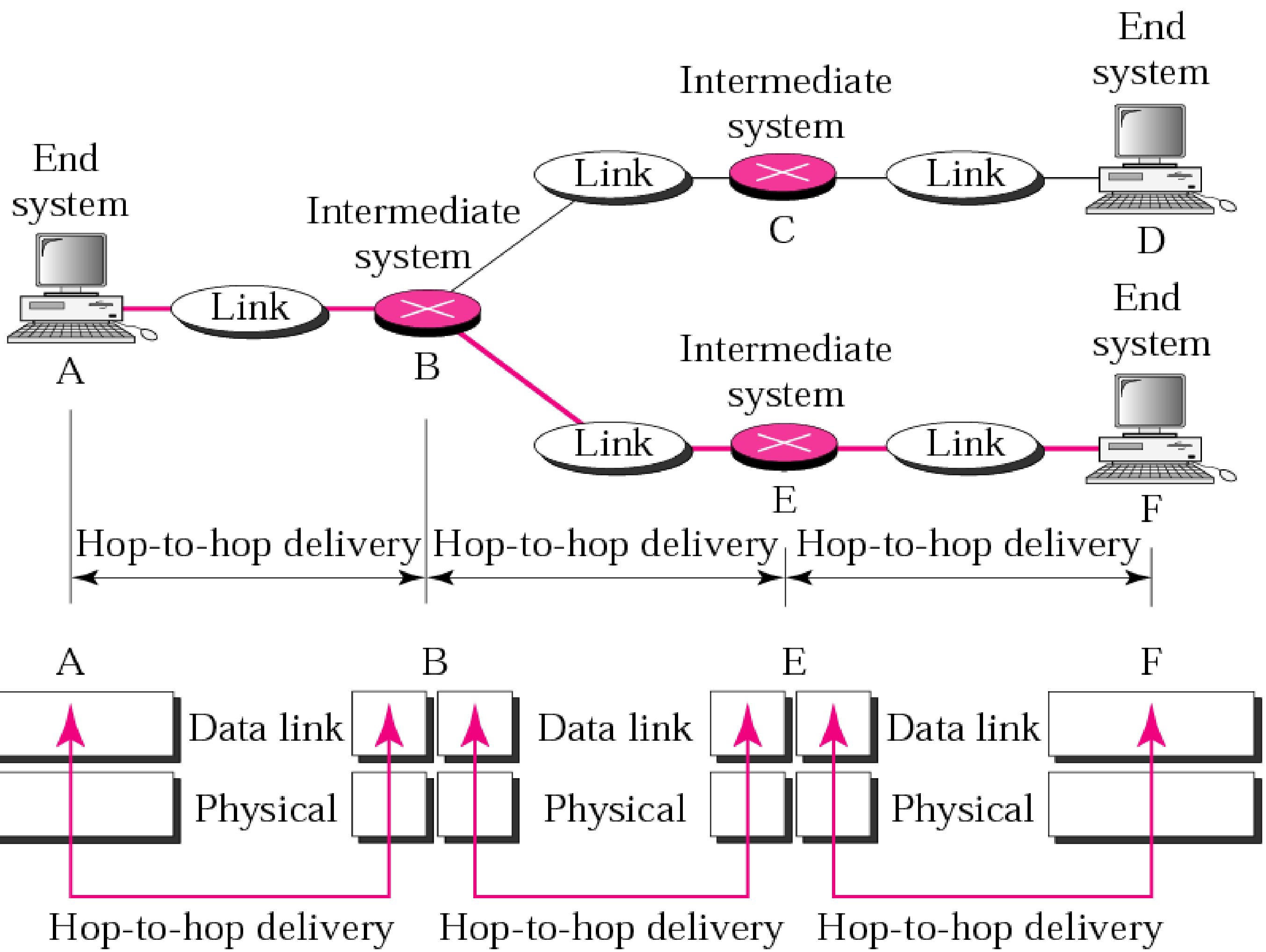
- **IV. Flow control**
- a. The data link layer makes sure that the sender sends the data at a speed at which the receiver can receive it else if there is an overflow at the receiver side the data will be lost.
- **b.** The data link layer imposes flow control mechanism over the sender and receiver to avoid overwhelming of the receiver.
- **V. Error control**
- **a.** The data link layer imposes error control mechanism to identify lost or damaged frames, duplicate frames and then retransmit them.
- **b.** Error control information is present in the trailer of a frame.

Data Link layer cont.

- **VI. Access Control**
- a. The data link layer imposes access control mechanism to determine which device has right to send data in an multipoint connection scenario.
- **VII. Main Responsibility**
- i. The main responsibility of the data link layer is hop to hop transmission of frames.



Hop-to-Hop delivery



Layer 3: Network Layer

- **I.** The network layer makes sure that the data is delivered to the receiver despite multiple intermediate devices.
- **II.** 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.

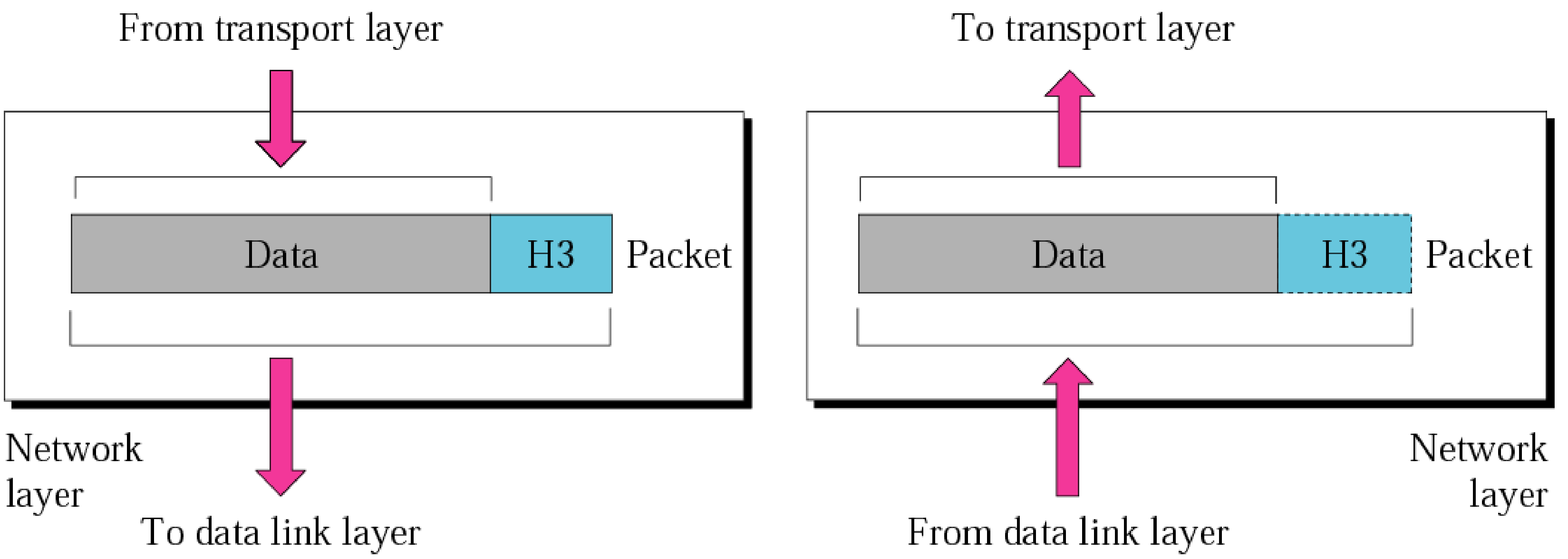
Layer 3: Network Layer

- **III.** The network layer is responsible for source to destination 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:
- a. Logical Addressing
- b. Routing
- **IV. Logical Addressing**
- The network layer uses logical address commonly known as IP address to recognize devices on the network.
- An IP address is a unique address which enables the network layer to identify devices outside the sender‘s network.
- The header appended by the network layer contains the actual sender and receiver IP address.
- At every hop the network layer of the intermediate node checks the IP address in the header, if it is not its own own IP address, the intermediate node concludes that it is not the final node and passes it to the data link layer.

Layer 3: Network Layer

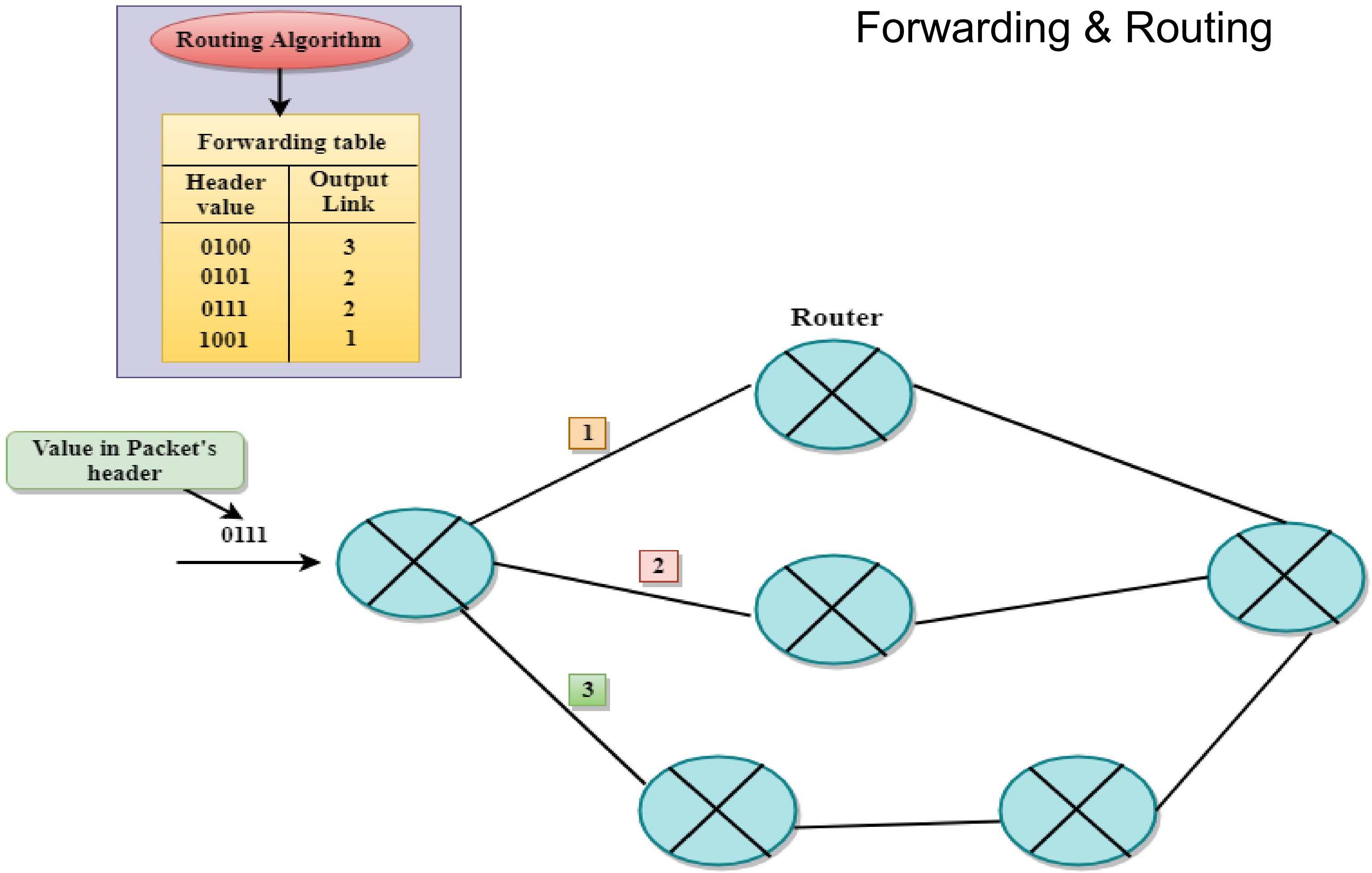
- **V. Routing**
- The network layer divides data into units called packets of equal size and gives a sequence number for rearranging on the receiving end.
- Each packet is independent of the other and may travel using different routes to reach the receiver hence may arrive out of turn at the receiver.
- Hence every intermediate node which encounters a packet tries to compute the best possible path for the packet which may depend on several factors such as congestion, number of hops, etc.
- This process of finding the best path is called as Routing. It is done using routing algorithms.
- **VI.** The Network layer does not perform any flow control or error control
- **VII. Main Responsibility**
- The main responsibility of Network Layer is transmission of packets from source to destination

Network Layer cont.



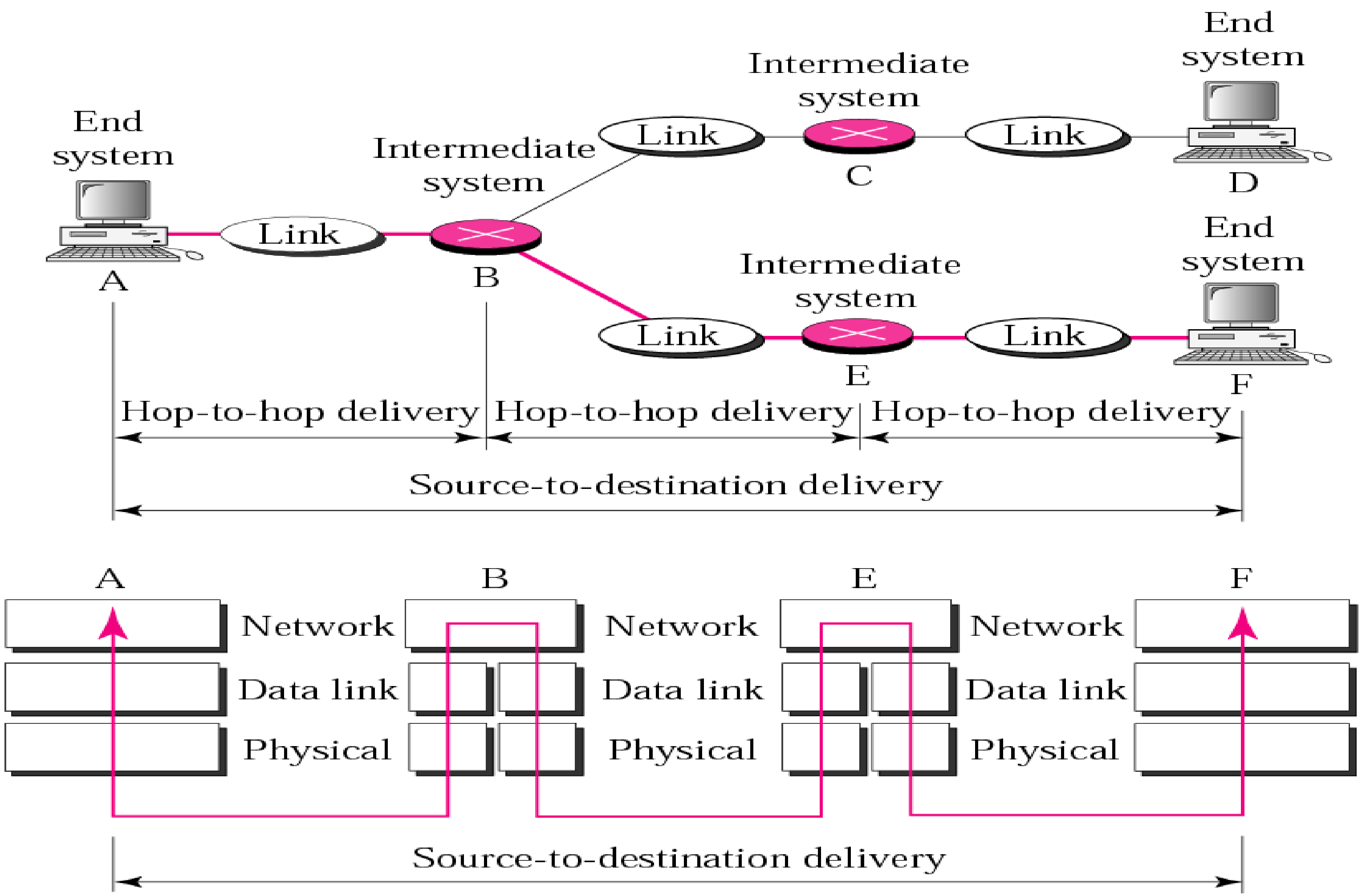
Network Layer cont.

Source to Destination Delivery with Forwarding & Routing



Routing algorithms determine the values in forwarding table

Source-to-Destination delivery

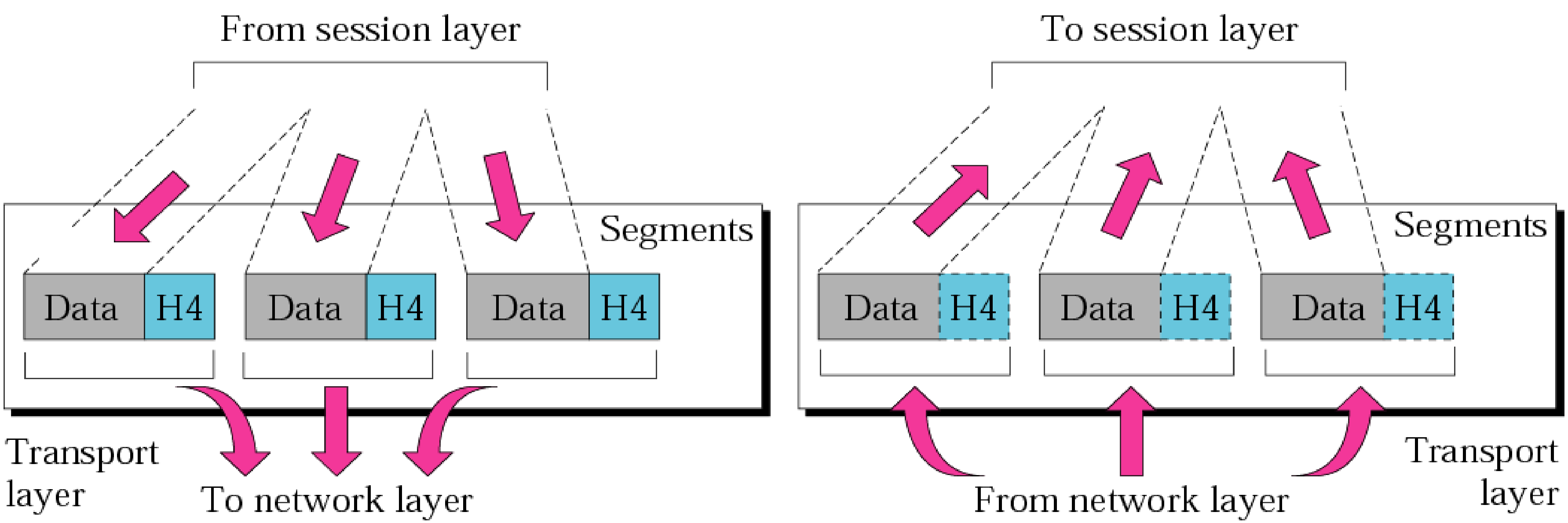


Layer 4: Transport Layer

- **I.** A logical address at network layer facilitates the transmission of data from source to destination device, which may be having multiple processes communicating with each other.
- Hence it is important to deliver the data from the correct process on the sender to the correct process on the receiver.
- The transport layer takes care of process to process delivery of data and makes sure that it is intact and in order.
- **II.** At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer.
- At the receiving side, the transport layer receives packets from the network layer, converts and arranges into proper sequence of segments and sends it to the session layer.

Transport Layer cont.

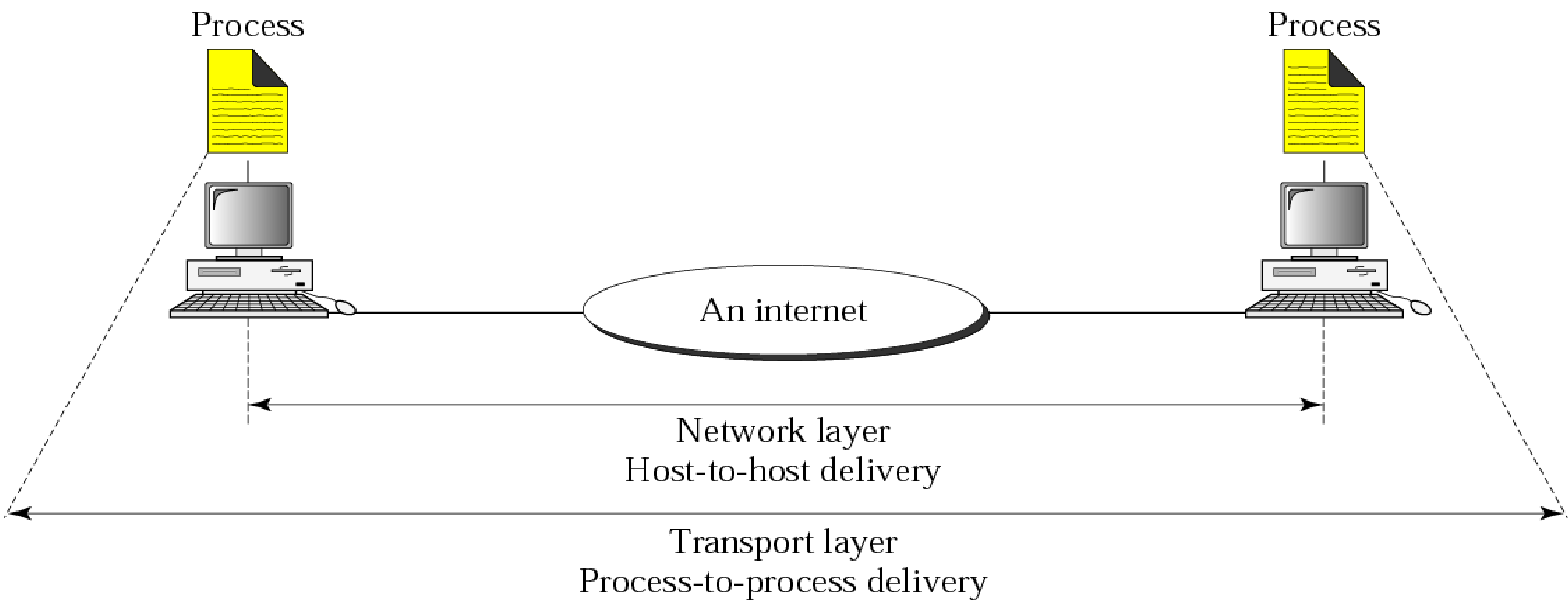
- **III.** To ensure process to process delivery the transport layer makes use of **port address** to identify the data from the sending and receiving process.
- A Port Address is the name or label given to a process. It is a 16 bit address.
- Ex. TELNET uses port address 23, HTTP uses port address 80. Port address is also called as Service Point Address.



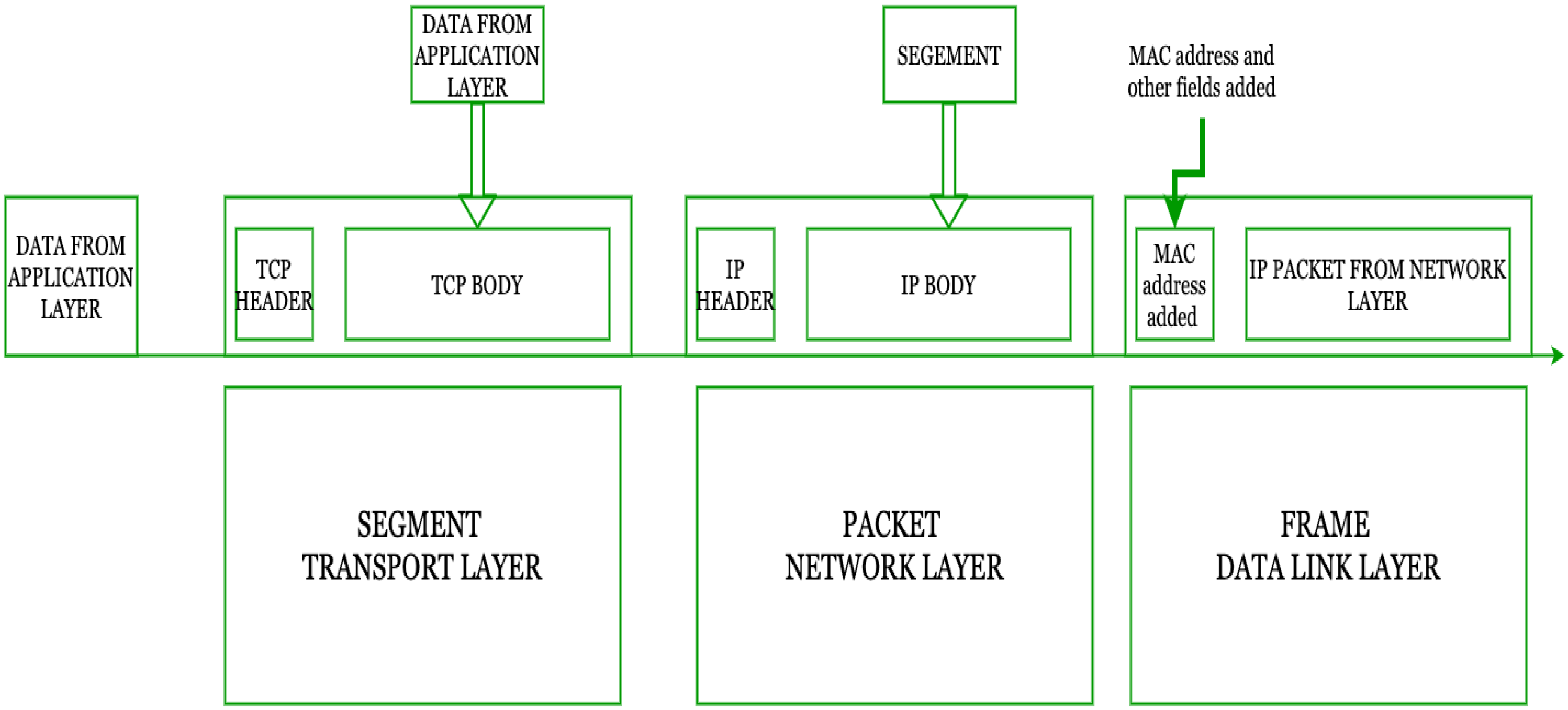
Transport Layer cont.

- **IV.** The data can be transported in a connection oriented or connectionless manner.
- If the connection is connection oriented then all segments are received in order else they are independent of each other and are received out of order and have to be rearranged.
- **V.** The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers.
- This numbering enables the receiving transport layer to rearrange the segments in proper order.
- **VI. Flow Control & Error control:** the transport layer also carries out flow control and error control functions; but unlike data link layer these are end to end rather than node to node.
- **VII. Main Responsibility**
- The main responsibility of the transport layer is process to process delivery of the entire message.

Reliable process-to-process delivery of a message



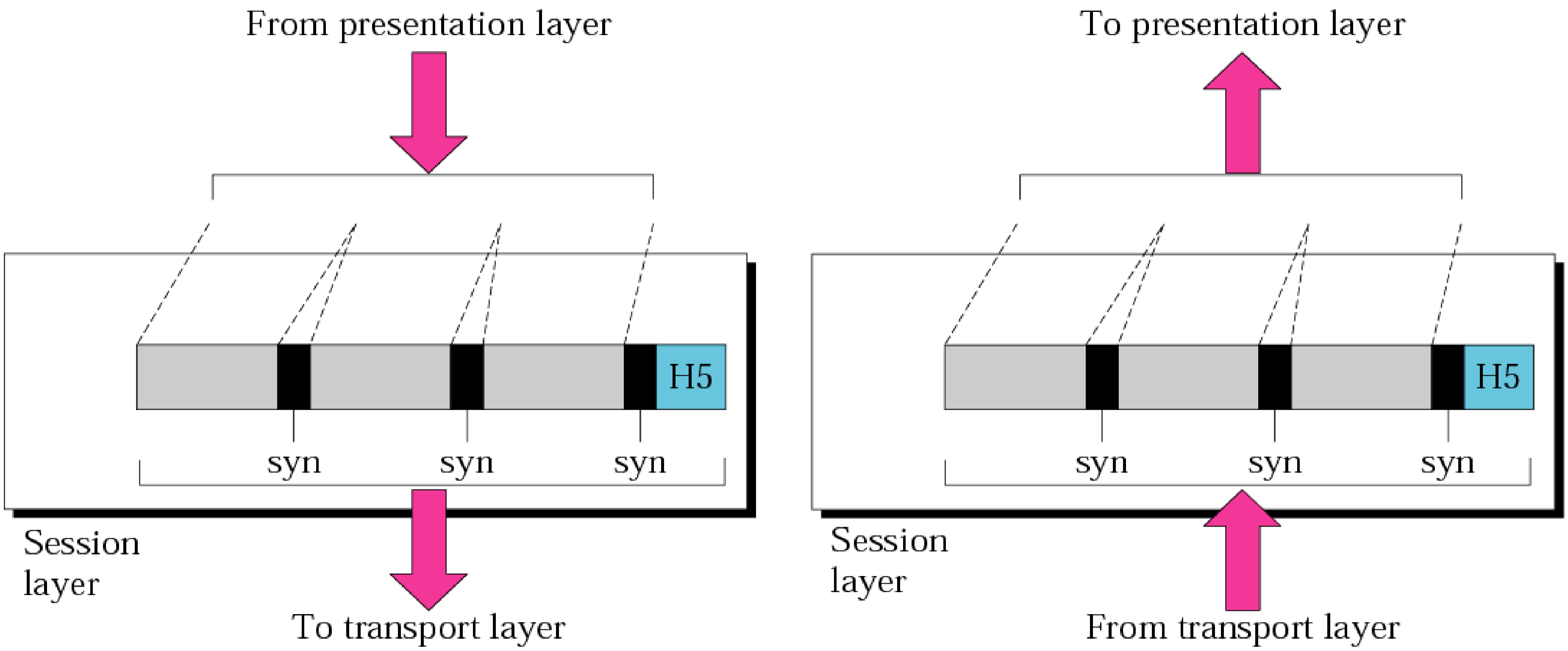
Fragment-Packet-Frame



Layer 5: Session Layer

- **I.** The session layer establishes a session between the communicating devices called dialogue and synchronizes their interaction.
- It is the responsibility of the session layer to establish and synchronize the dialogues. It is also called the network dialogue controller.
- **II.** 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.
- **III.** The checkpoints or synchronization points is a way of informing the status of the data transfer.
- **Ex**. A checkpoint after first 500 bits of data will ensure that those 500 bits are not sent again in case of retransmission at 650th bit.
- **IV.** Main responsibility of session layer is dialog control and synchronization

Session Layer cont.

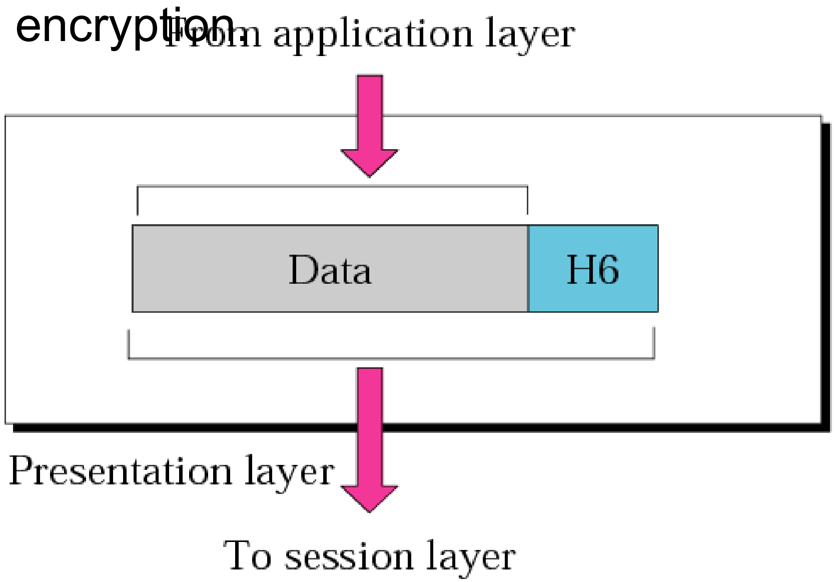


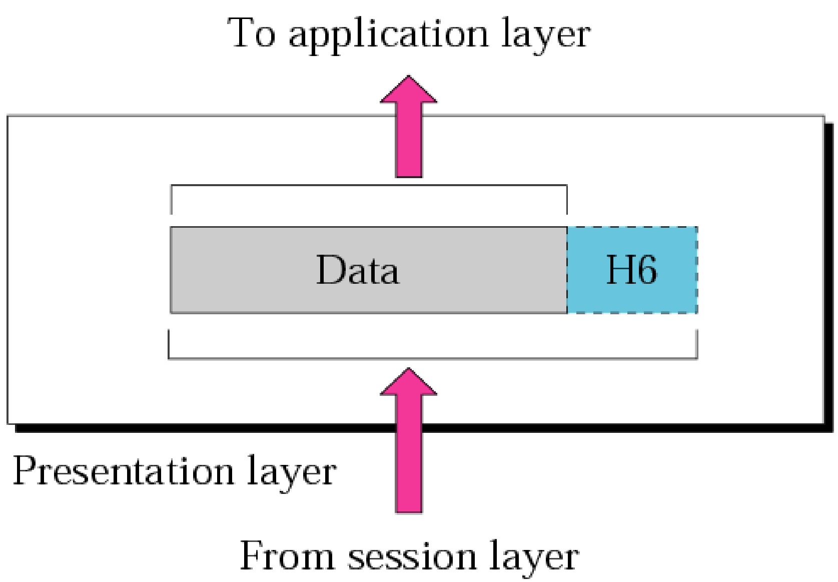
Layer 6 :Presentation Layer

- **I.** The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.
- **II.** 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.
- **III. Translation**
- The sending and receiving devices may run on different platforms (hardware, software and operating system).
- Hence it is important that they understand the messages that are used for communicating with using some translation service.

Presentation Layer cont.

- **IV. Compression**
- Compression ensures faster data transfer. The data compressed at sender has to be decompressed at the receiving end.
- **V. Encryption**
- It is the process of transforming the original message to change its meaning before sending it. The reverse process called decryption has to be performed at the receiving end to recover the encrypted message.
- **VI. Main responsibility**
- The main responsibility of the Presentation layer is translation, compression and encryption.

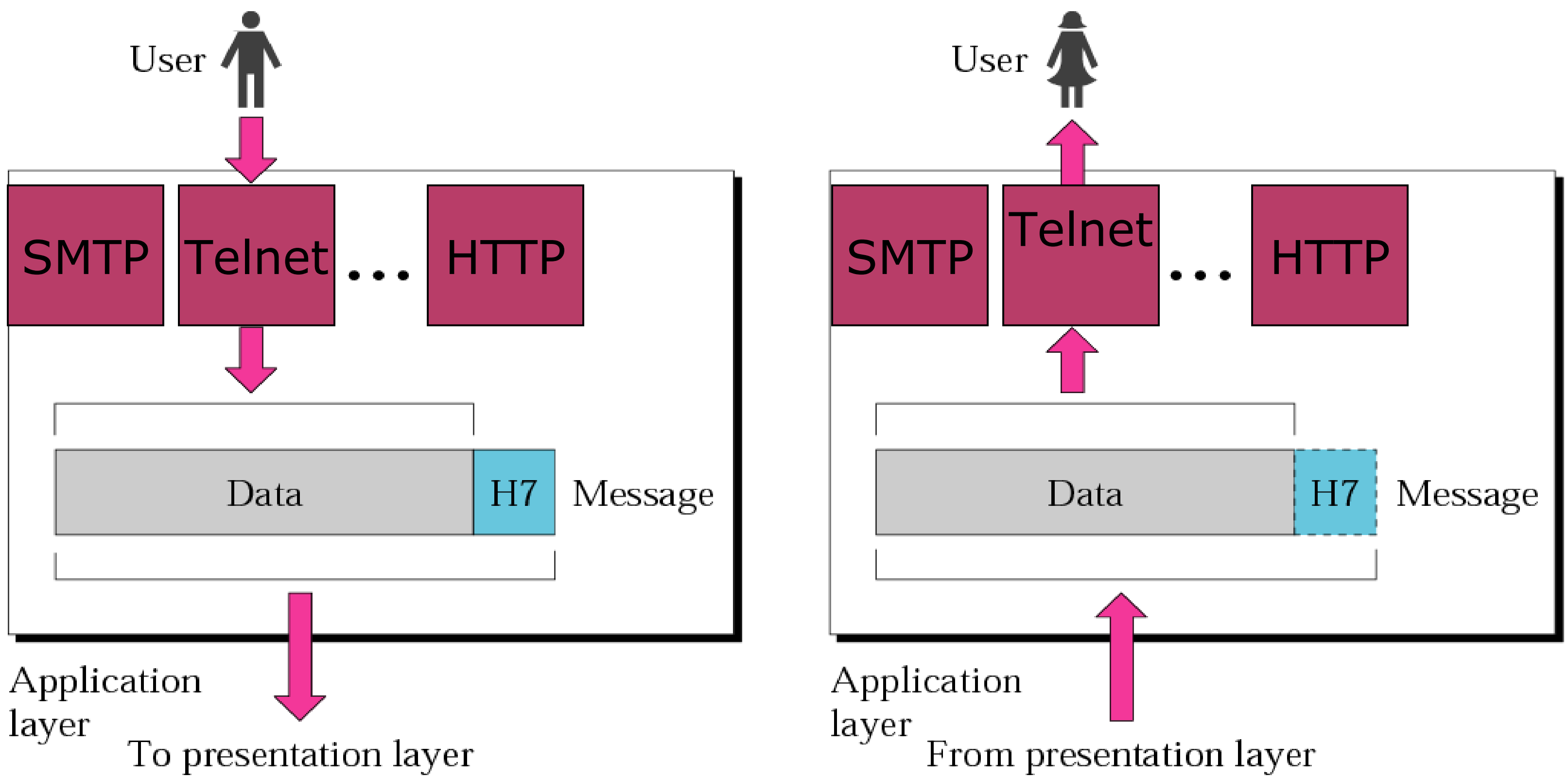




Layer 7: Application Layer

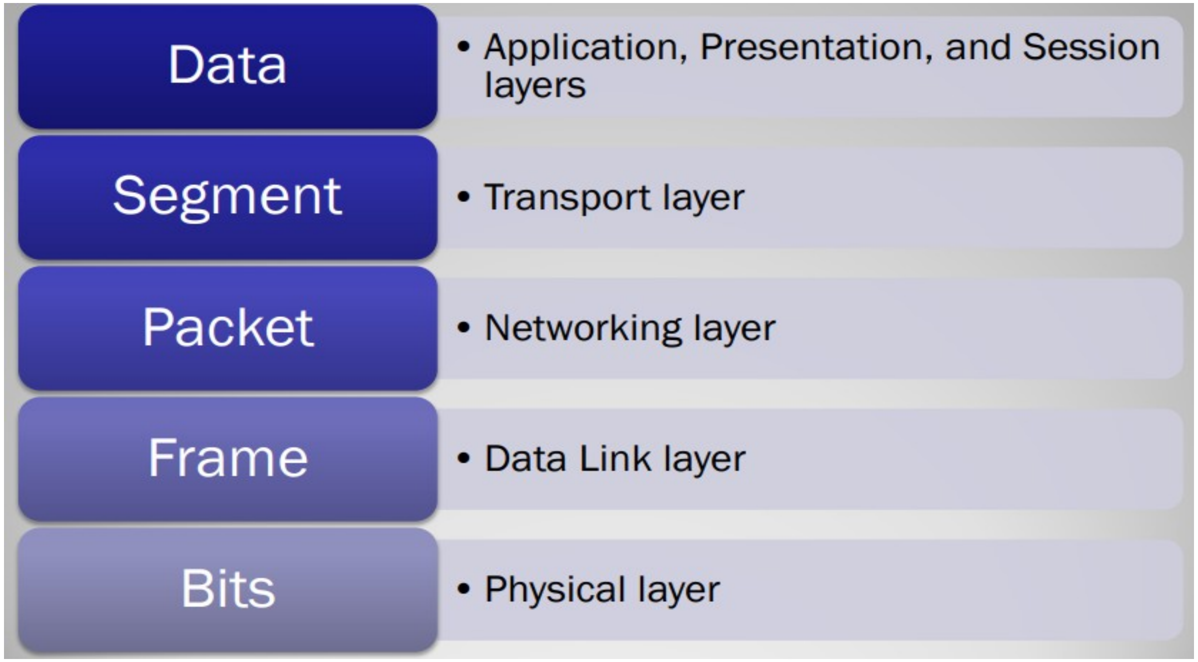
- **I.** The application layer enables the user to communicate its data to the receiver by providing certain services. For ex. Email is sent using X.400 service.
- **II. X500** is a directory service used to provide information and access to distributed objects
- **III. X400** is services that provides basis for mail storage and forwarding
- **IV. FTAM** (File transfer, access and management) provides access to files stored on remote computers and mechanism for transfer and manage them locally.
- **V. Main Responsibility**: Main Responsibility of Application layer is to provide access to network resources.

Application Layer cont.

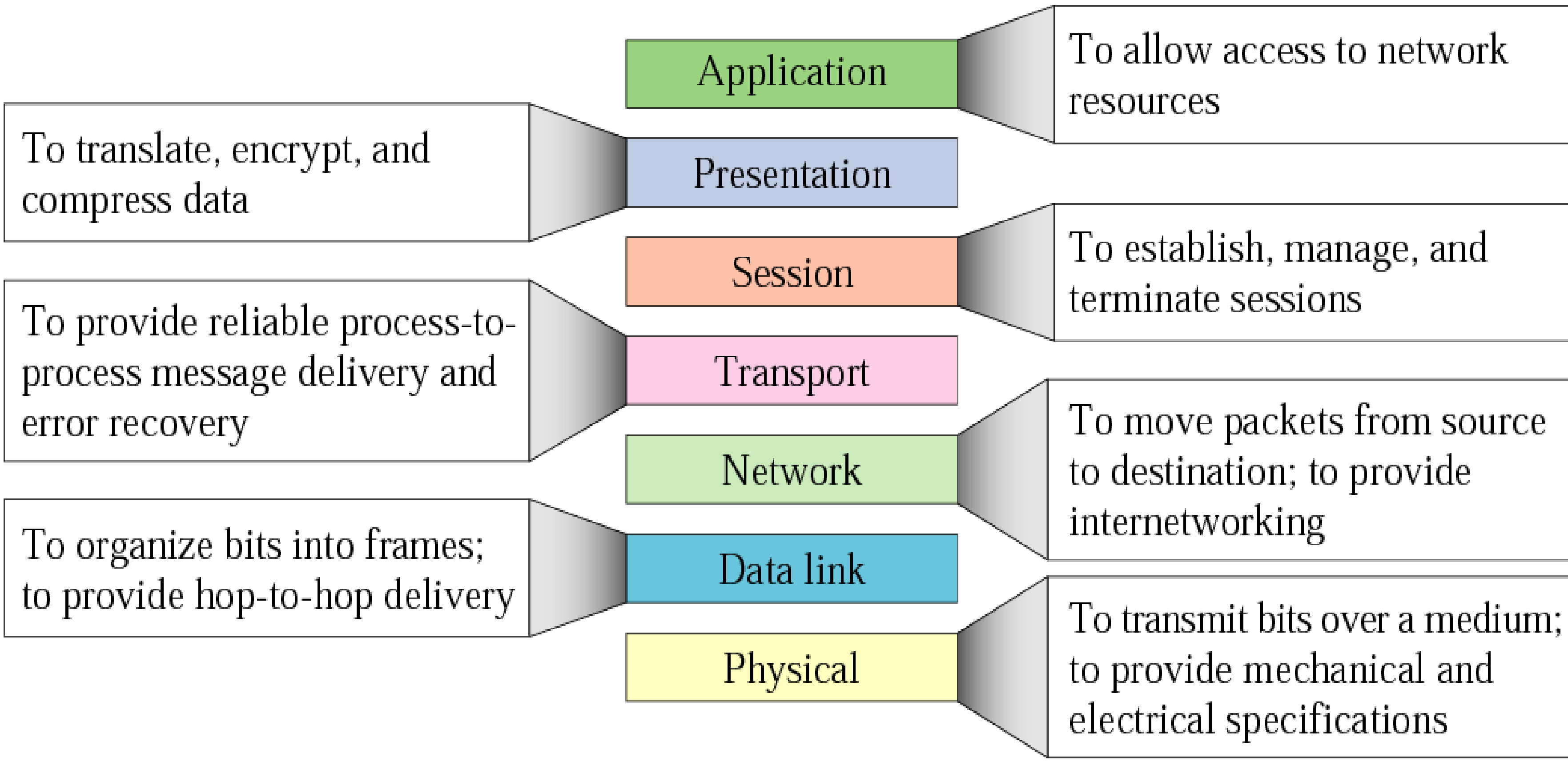


Conclusion

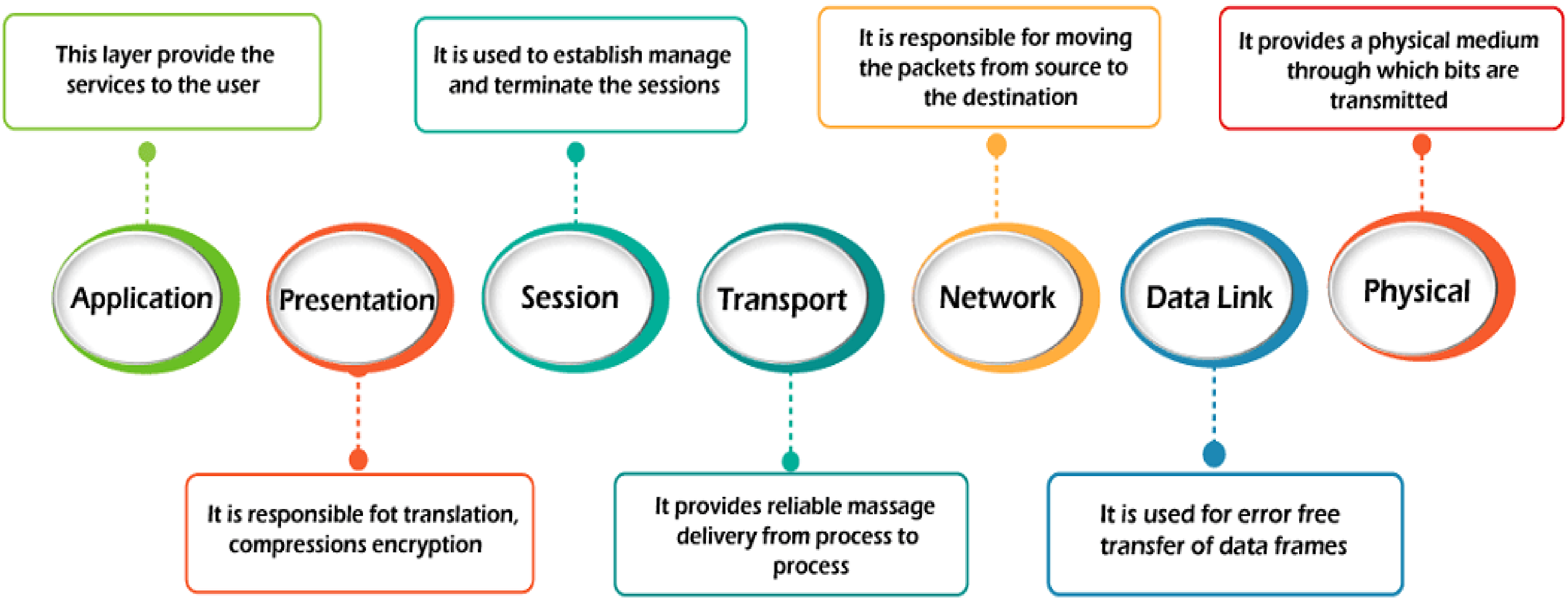
- The process of moving data between layers of the OSI Model.
- **Encapsulation:**
- Data > segment >packet > frame >bits
- **De-encapsulation:**
- Bits > frame >packet > segment> data
- Following figure shows how data is referred to at different layers in the OSI model.



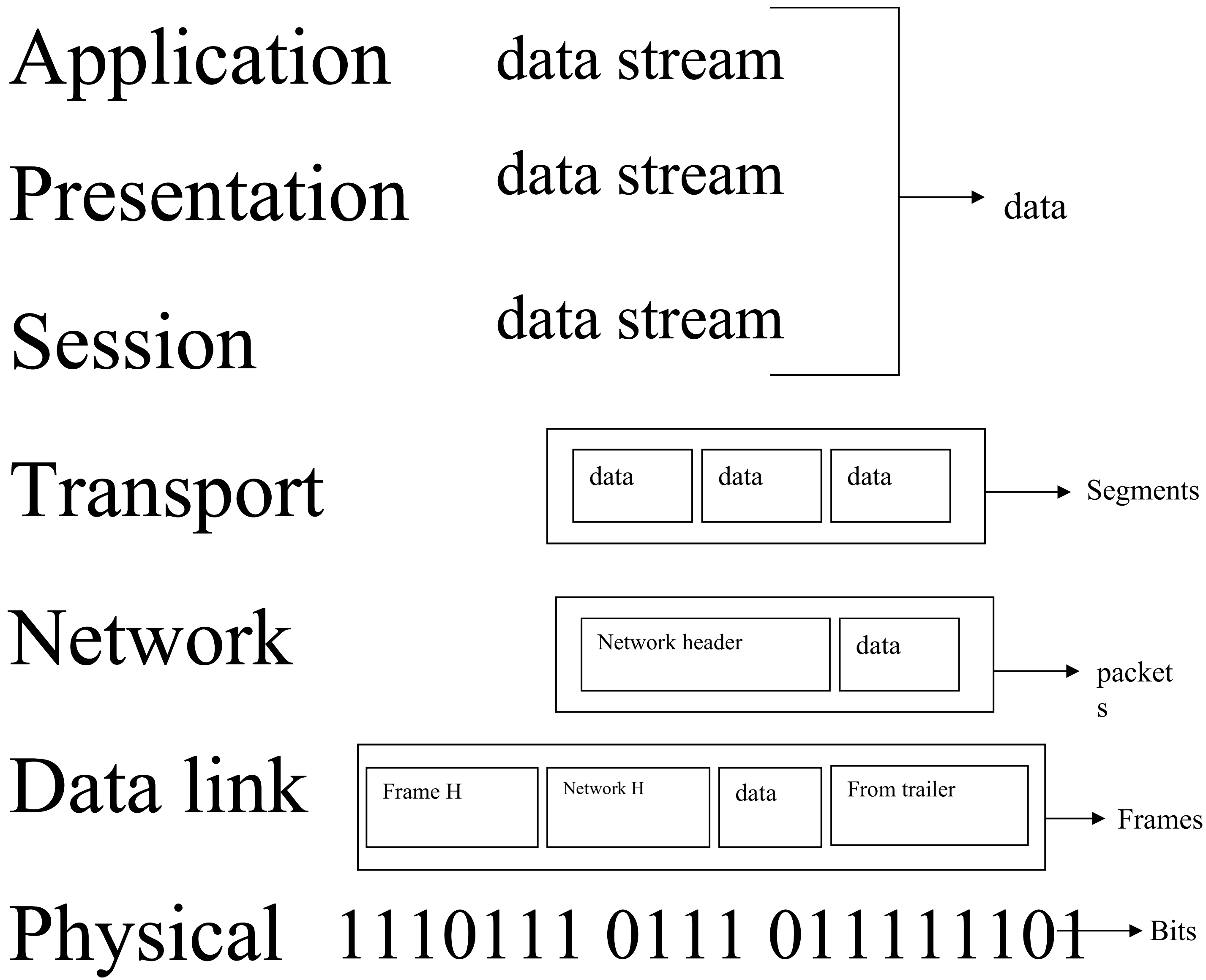
Summary


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

Summary


This layer provide the services to the user
It is used to establish manage and terminate the sessions
It is responsible for moving the packets from source to the destination
It provides a physical medium through which bits are transmitted
Application
Presentation
Session
Transport
Network
Data Link
Physical
It is responsible fot translation, compressions encryption
It provides reliable massage delivery from process to process
It is used for error free transfer of data frames

Summary (Format of Data)



TCP/IP Protocol Suite

- **The <u>TCP/IP protocol suite</u> is a hierarchical protocol , made of five layers:**
- TCP/IP model is a collection of protocols often called a protocol suite. It offers a rich variety of protocols from which we can choose from.
- It is also called as the TCP/IP protocol suite. It is a collection of protocols.
- It is a hierarchical model, i.e. There are multiple layers. It existed even before the OSI model was developed.
    - Physical layer
    - Data link layer
    - Network layer
    - Transport layer
    - Application layer.
- The figure for TCP/IP model is as follows:

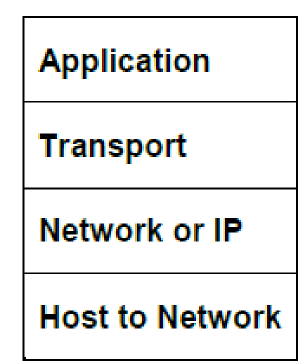
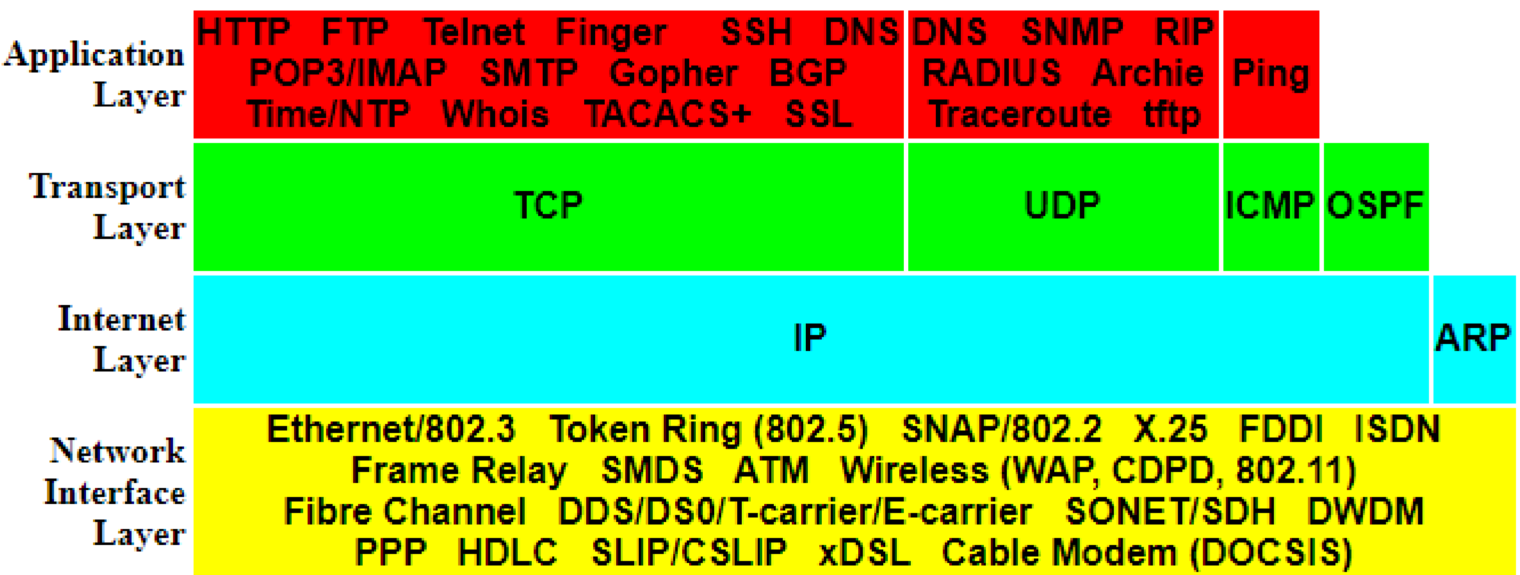


Fig: Layers of TCP/IP Reference Model

The TCP/IP Model

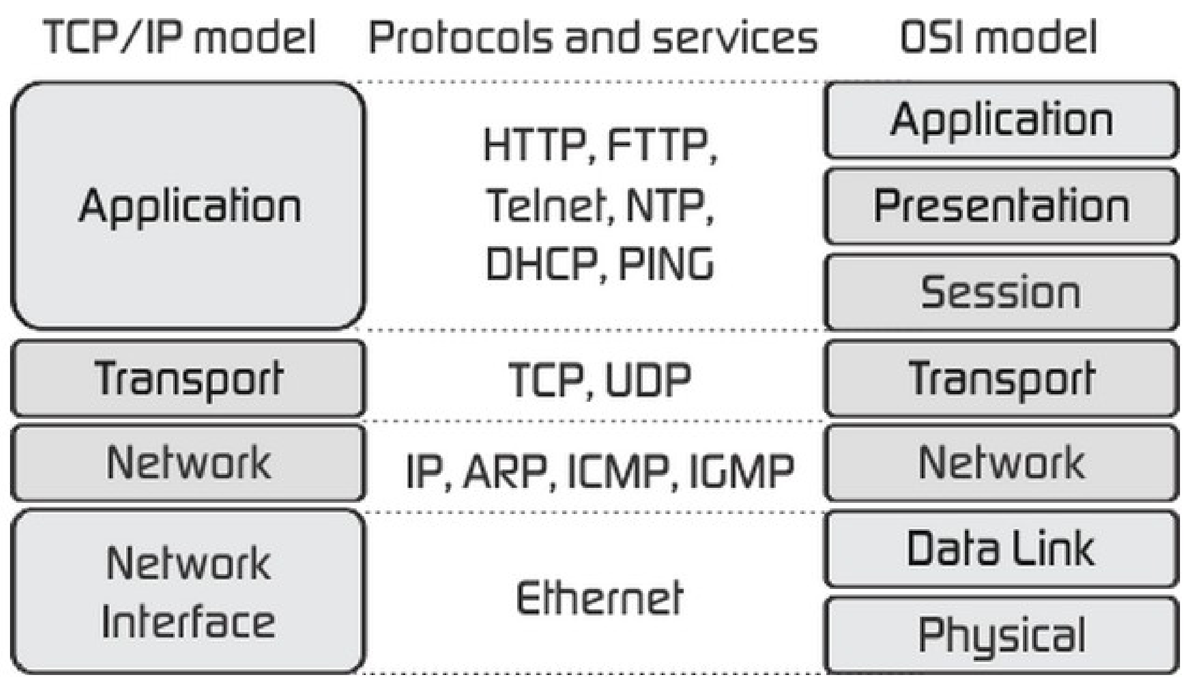
- The most common protocol used; in data networks today is the TCP / IP protocol stack. TCP/IP is used to interconnect devices in corporate networks as well as the protocol of the Internet.
- The TCP/IP suite of protocols was developed as part of the research done by the Defence Advance Research Projects Agency (DARPA).
- Later TCP/IP was included with the Berkeley Software Distribution (BSD) UNIX. TCP/IP is an industry standard suite of protocols designed to be routable, robust, and functionally efficient.



Abbreviated TCP/IP protocol stack.

The TCP/IP Model

- The Internet protocols can be used to communicate across any set of Interconnected networks and are also well suited for both LAN and WAN communication.
- The Internet protocol suite includes not only Layers 3 and 4 specifications, but also specifications for common applications such as e-mail, remote login, terminal emulation, and file transfer.
- The TCP/IP protocol stacks maps closely to the OSI reference model in the lower layer. All standard Physical and data-link protocols are supported.



Advantages of TCP/IP Model

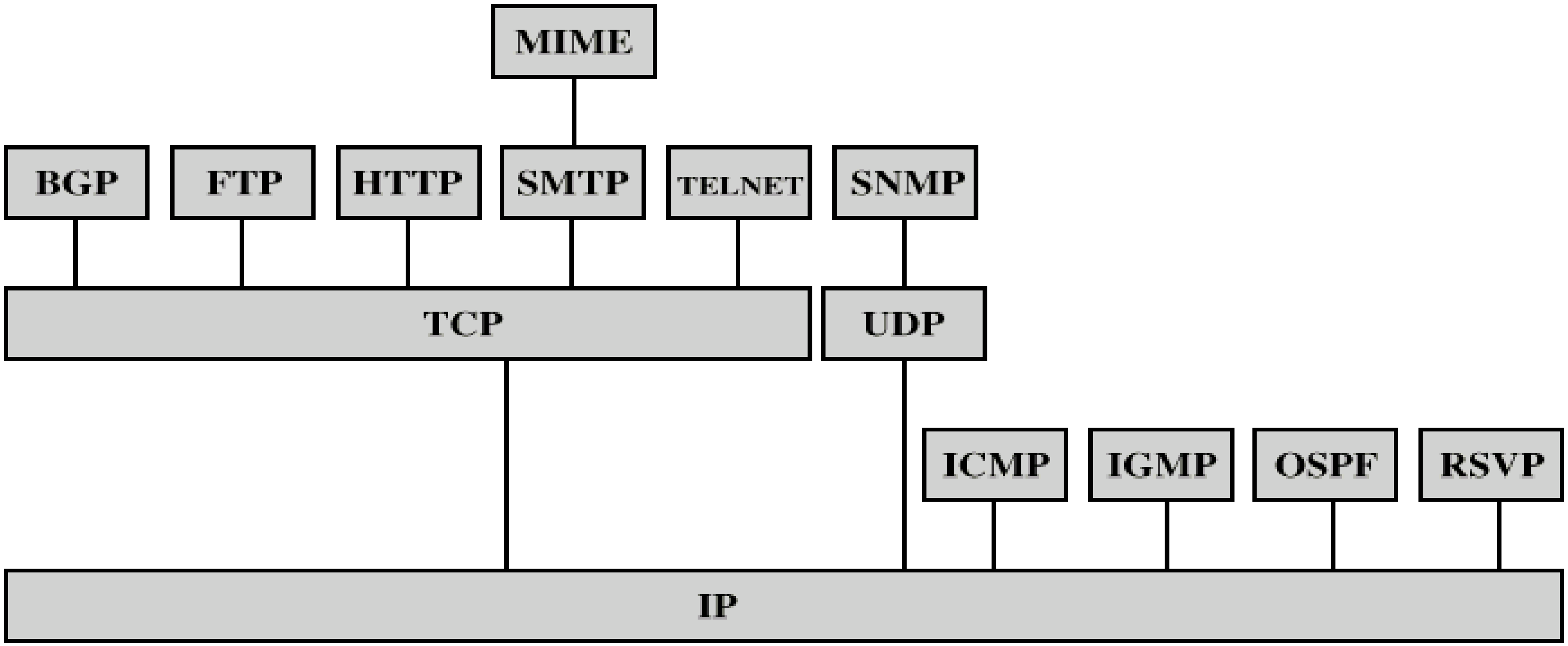
- **1. An industry-standard protocol**
- Because TCP/IP is not maintained or written by one company, it is not subject to as many compatibility issues.
- The Internet community as whole decides whether a particular change or implementation is worthwhile.
- This slows down the implementation of new features and characteristics compared to how quickly one directed company might make changes, but it does guarantee that changes are well thought out, that they provide functionality with most other implementations of TCP/IP.
- **2.** As set of utilities for connecting dissimilar operating systems, many connectivity utilities have been written for the TCP/IP suite, including the File Transfer Protocol (FTP) and Terminal Emulation Protocol (Telnet).
- Because these utilities use the windows Sockets API, connectivity from one machine to another is not dependant on the network operating system used on either machine.

Advantages of TCP/IP Model

- **3.** A scalable Cross-platform client-server architecture
- **4. Access to the Internet**
- TCP/IP is the de facto protocol of the Internet and allows access to a wealth of information that can be found at thousands of locations around the world.
- To connect to the Internet, a valid IP address is required.
- Because IP address have become more and more scarce, and as security issues surrounding access to the Internet have been raised, many creative alternatives have been established to allow connections to the internet.
- Now you understand the benefits of installing TCP/IP, you are ready to about how the TCP/IP protocol suite maps to a four -layer model.

OSI	TCP/IP
Application	
Presentation	
Session	Application
Transport	Transport
Networking	Internet
Data Link	Network interface
Physical	

Some Protocols in TCP/IP Suite

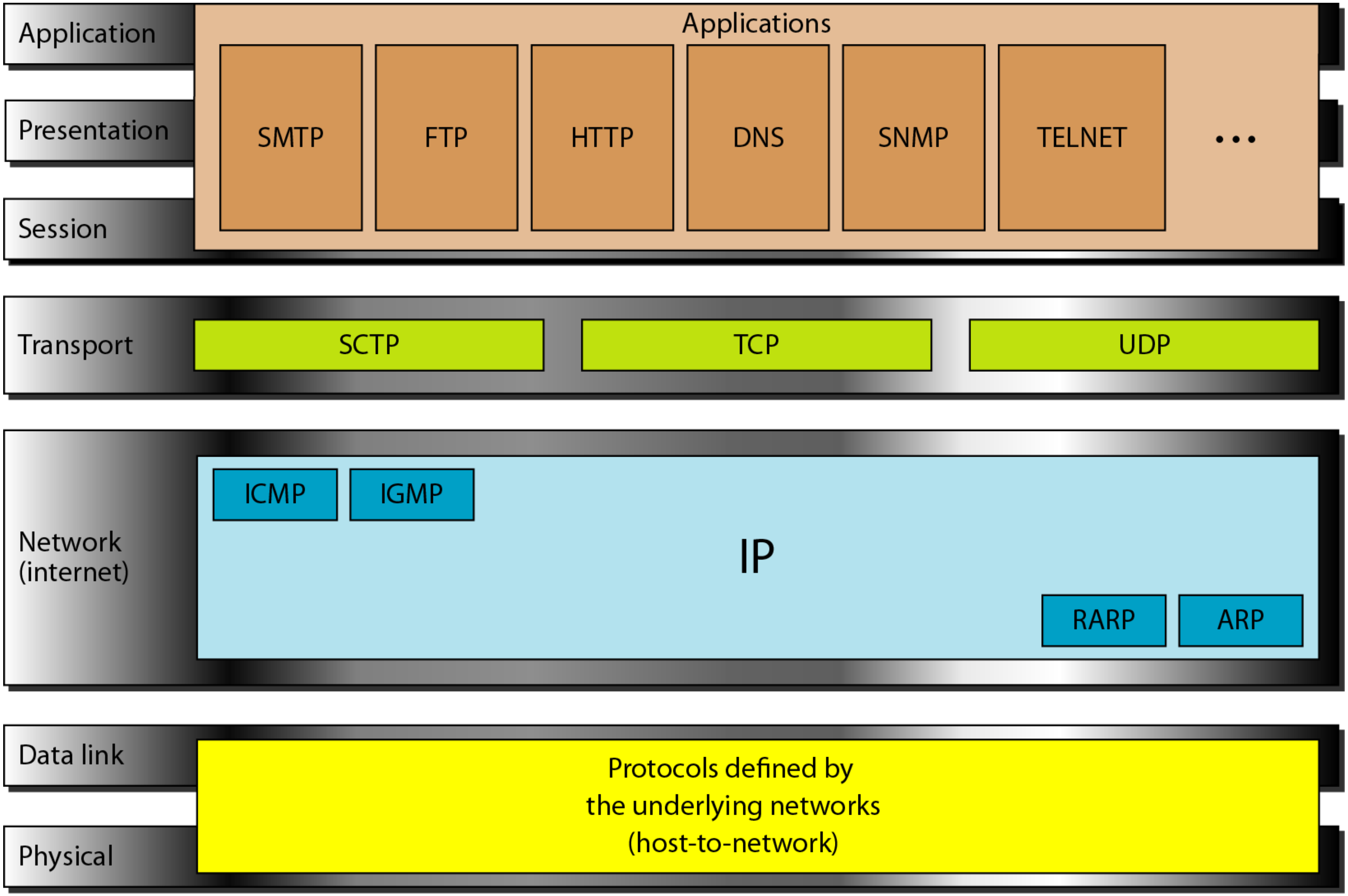


BGP = Border Gateway Protocol
FTP = File Transfer Protocol
HTTP = Hypertext Transfer Protocol
ICMP = Internet Control Message Protocol
IGMP = Internet Group Management Protocol
IP = Internet Protocol
MIME = Multi-Purpose Internet Mail Extension
OSPF = Open Shortest Path First
RSVP = Resource ReSerVation Protocol
SMTP = Simple Mail Transfer Protocol
SNMP = Simple Network Management Protocol
TCP = Transmission Control Protocol
UDP = User Datagram Protocol

TCP/IP Protocol Suite

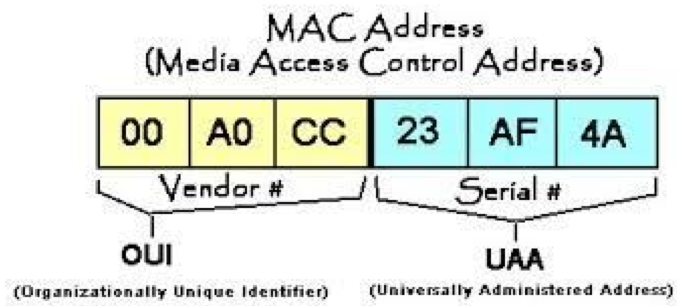
- The layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application.
- However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.

TCP/IP and OSI model

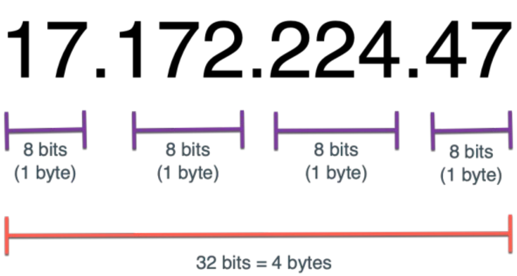


Addressing

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

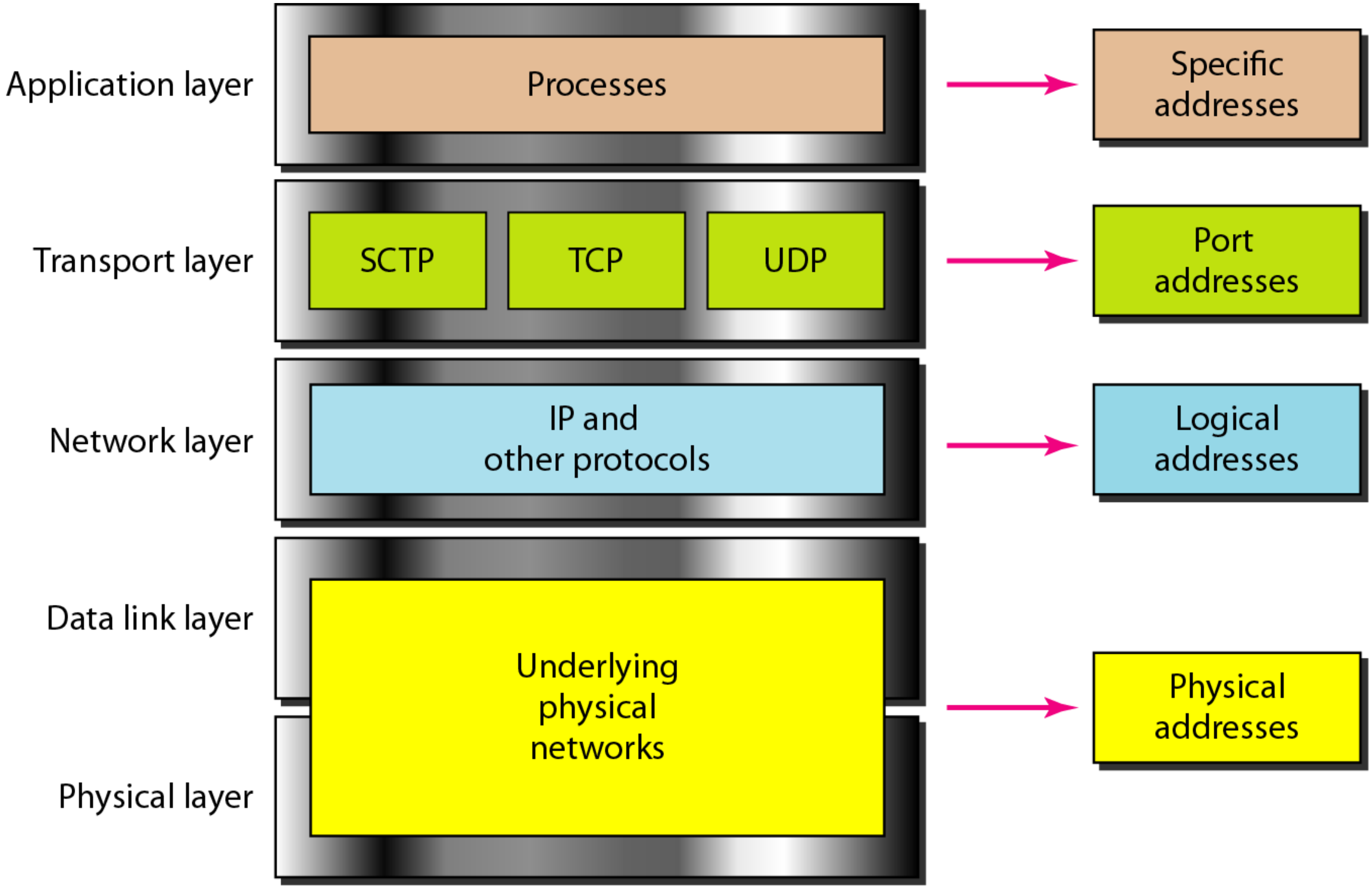


IPv4 Address Example



IPv4	IPv6
Deployed 1981	Deployed 1998
32-bit IP address	128-bit IP address
4.3 billion addresses Addresses must be reused and masked	**7.9x10^{28} addresses** Every device can have a unique address
Numeric dot-decimal notation **192.168.5.18**	Alphanumeric hexadecimal notation **50b2:6400:0000:0000:6c3a:b17d:0000:10a9** (Simplified - 50b2:6400::6c3a:b17d:0:10a9)
DHCP or manual configuration	Supports autoconfiguration

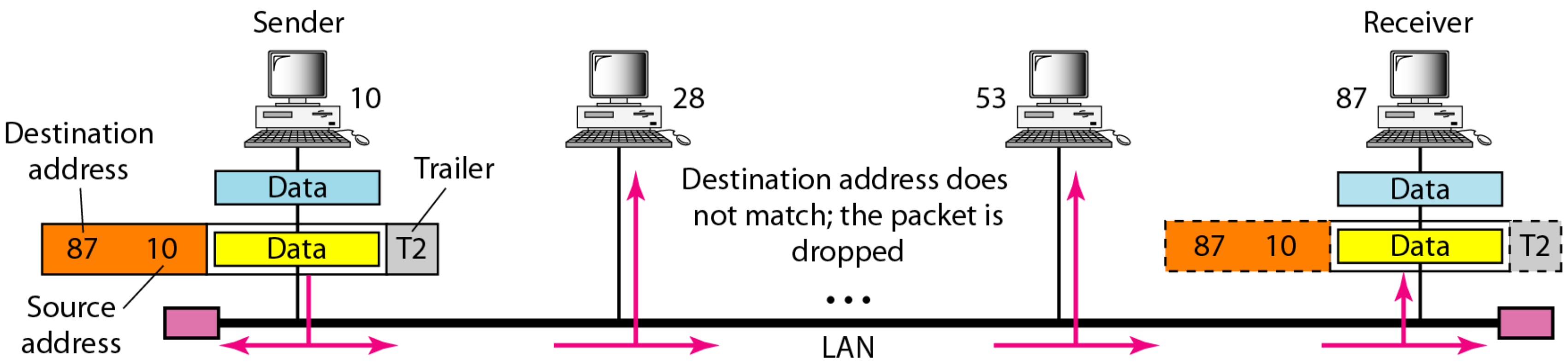
Relationship of layers and addresses in TCP/IP



SCTP: Stream Control Transmission Protocol
TCP: Transmission Control Protocol
UDP: User Datagram Protocol

Example 2.1

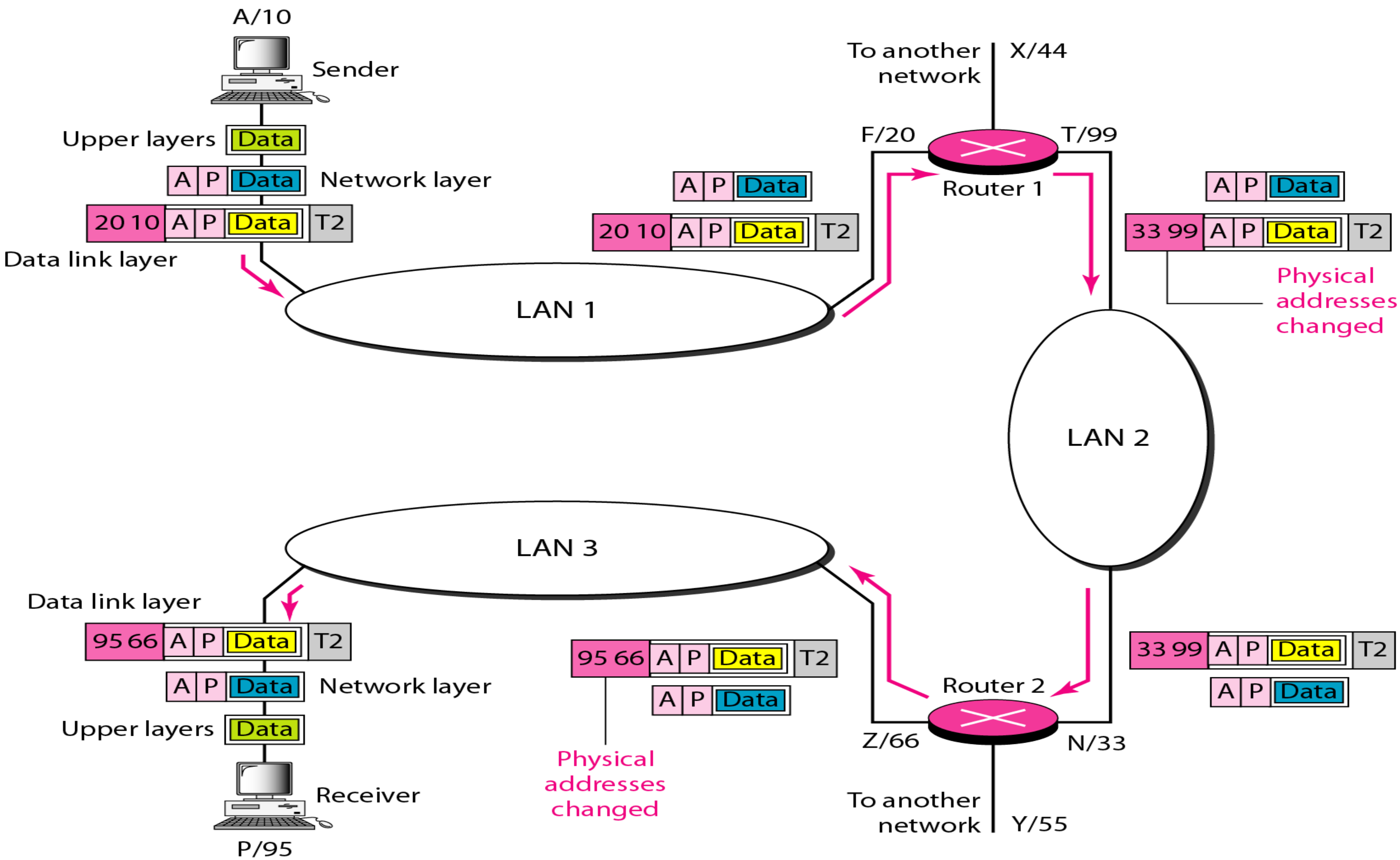
- In Figure 2.19 a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN).
- As the figure shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver.



Example 2.3

- Figure 2.20 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.

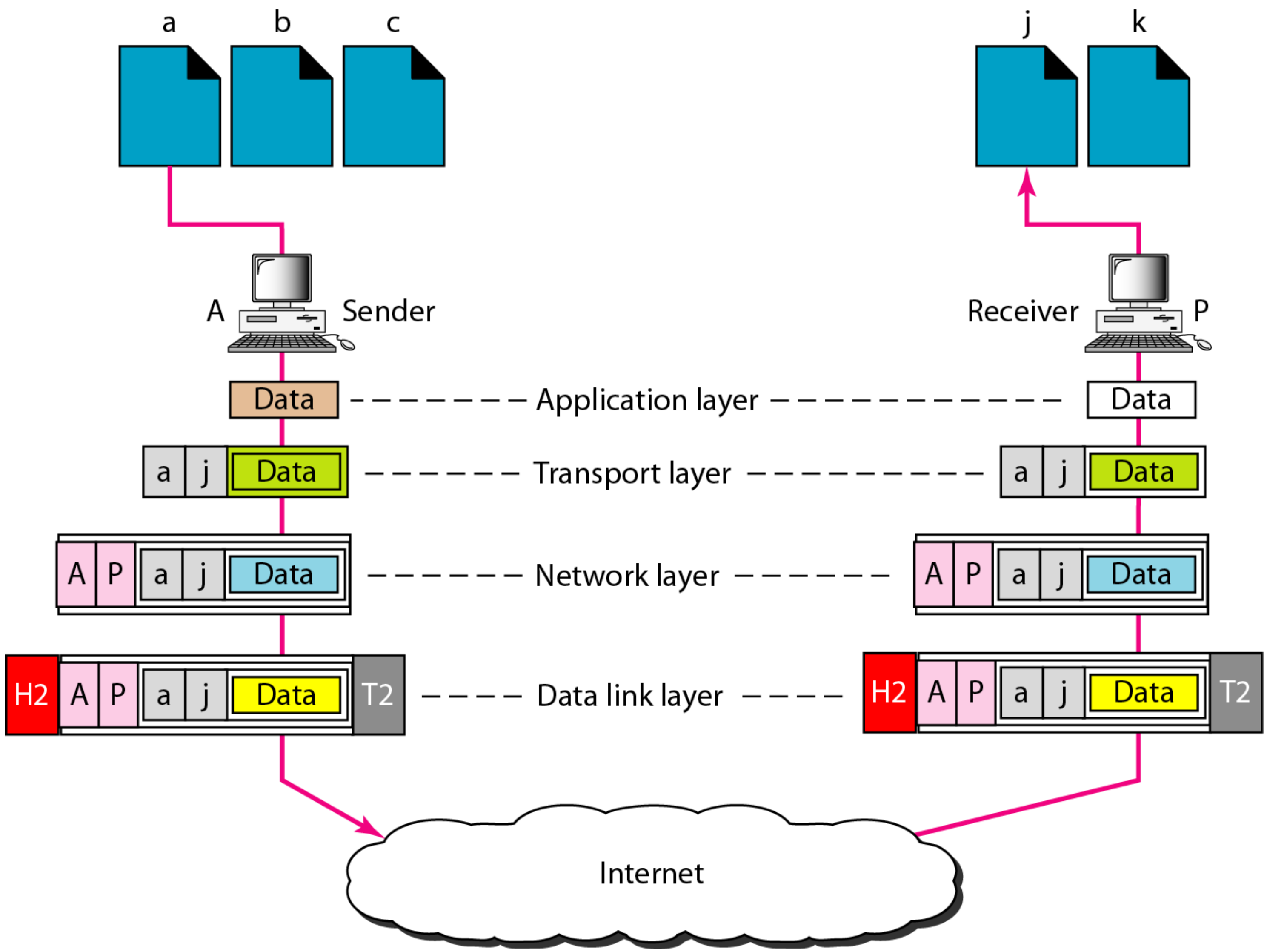
Figure 2.20 *IP addresses*



Example 2.4

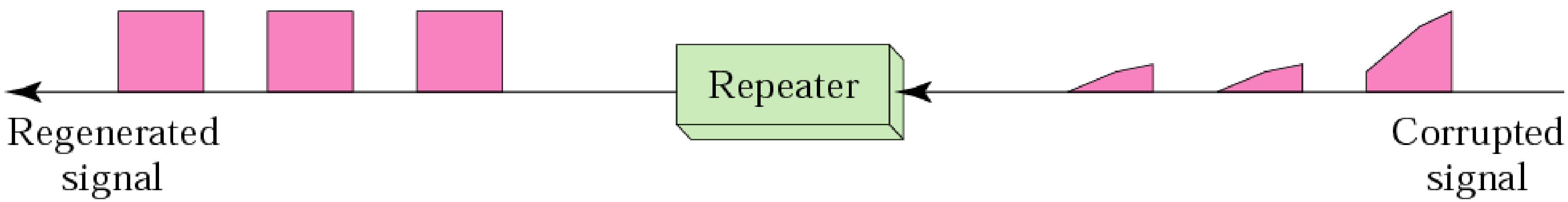
- Figure 2.21 shows two computers communicating via the Internet.
- The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k.
- Process a in the sending computer needs to communicate 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.

Figure 2.21 *Port addresses*

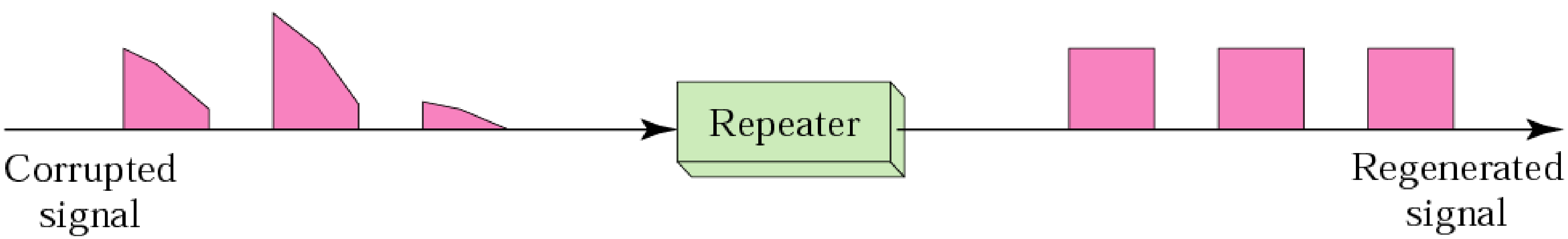


Network Devices

- Modem: a device that modulates a digital signal onto analog signal for transmission over telephone lines.
- Repeater: Re-generates the signal again.



a. Right-to-left transmission.



b. Left-to-right transmission.

DEVICES :

1. Hub

- Hubs connect multiple computer networking devices, working only on the Physical layer of the OSI.
- Hubs do not perform packet filtering or addressing functions. Instead, they send data packets to all connected devices.
- A hub also acts as a repeater, amplifying signals that deteriorate after travelling long distances over connecting cables.
- A hub is the most straightforward network connecting device because it connects LAN components with identical protocols.

DEVICES :

- 2. Switches
- A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance.
- A switch is a data link layer device.
- The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct.
- **3.** Bridge
- A bridge operates at the data link layer.
- A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination.
- It is also used for interconnecting two LANs working on the same protocol.
- It has a single input and single output port, thus making it a 2 port device.

DEVICES

4. Routers,

- A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device.
- Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets.

DEVICES

5. Gateway

- Gateways connect networks operating on different protocols so data can transfer between destinations. These devices normally work at the Transport and Session layers of the OSI model.
- At the Transport layer and above, there are numerous protocols and standards from different vendors, and gateways help deal with them.

5. Repeaters

- A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network.
- It is a 2-port device.

Network devices With Layer

Layers	Network Devices
Application Layer	Application gateway
Transport Layer	Transport gateway
Network Layer	Router and gateway
Data link layer	Bridge and Switch
Physical Layer	Repeater, Hub and Modem.