Introduction to Computer Networks

Agenda

- **Data Communications**
- **Networks, Internet**
- **Protocols and Standards, Layered Tasks**
- **The OSI Model**
- **The Internet Model (TCP/IP Model)**
- **Addressing**
- **Overview of UDP and TCP, DNS.**

What is Data Communication?

- The term telecommunication means communication at a distance. The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data.
- Data Communication is a process of exchanging data or information.
- In case of computer networks this exchange is done between two devices over a transmission medium.
- This process involves a communication system which is made up of hardware and software.
- The hardware part involves the sender and receiver devices and the intermediate devices through which the data passes.
- The software part involves certain rules which specify what is to be communicated, how it is to be communicated and when. It is also called as a Protocol.

Characteristics of Data Communication

- The effectiveness of any data communications system depends upon the following four fundamental characteristics:
- 1. Delivery: The data should be delivered to the correct destination and correct user.
- 2. Accuracy: The communication system should deliver the data accurately, without introducing any errors. The data may get corrupted during transmission affecting the accuracy of the delivered data.
- 3. Timeliness: Audio and Video data has to be delivered in a timely manner without any delay; such a data delivery is called real time transmission of data.
- 4. Jitter: It is the variation in the packet arrival time. Uneven Jitter may affect the timeliness of data being transmitted.

Components of Data Communication

- A Data Communication system has five components as shown in the diagram below:
- 1. Message: Message is the information to be communicated by the sender to the receiver.
- 2. Sender: The sender is any device that is capable of sending the data (message).
- 3. Receiver: The receiver is a device that the sender wants to communicate the data (message).
- 4. Transmission Medium: It is the path by which the message travels from sender to receiver. It can be wired or wireless and many subtypes in both.

Components of Data Communication

- 5. Protocol: It is an agreed upon set or rules used by the sender and receiver to communicate data.
- A protocol is a set of rules that governs data communication.
- A Protocol is a necessity in data communications without which the communicating entities are like two persons trying to talk to each other in a different language without knowing the other language.

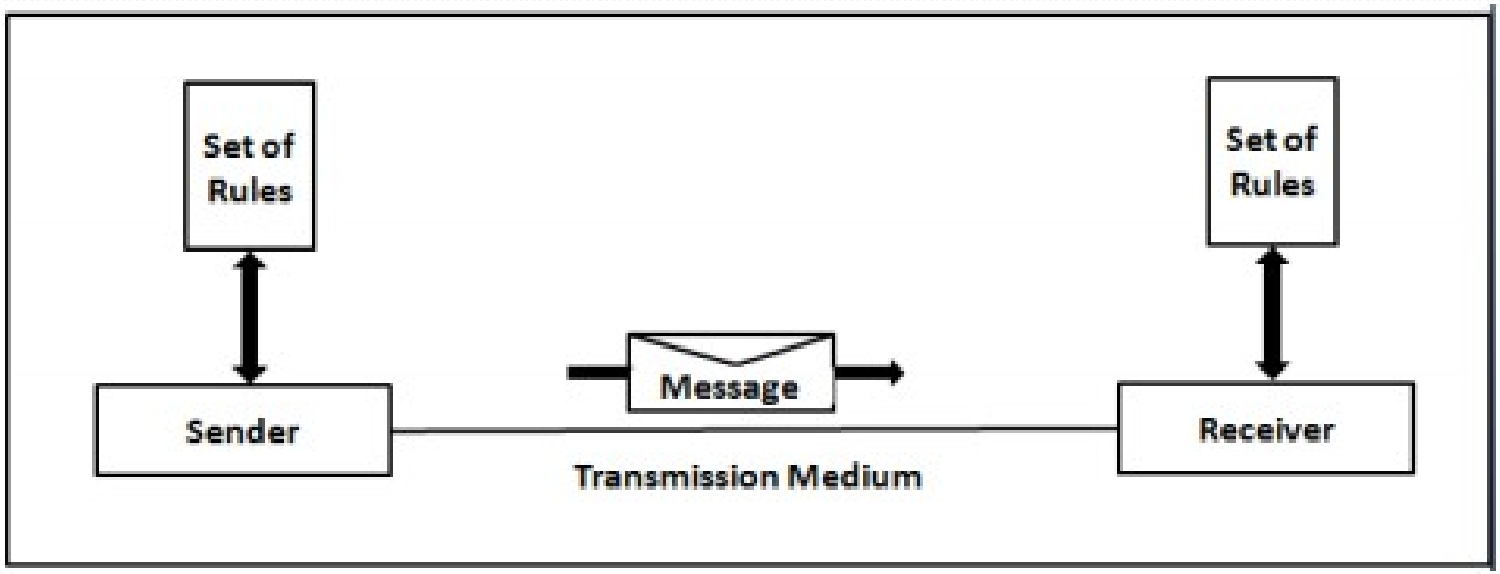


Fig. Components of a Data Communication System

Introduction to Computer Networks

- A network is a set of devices (often referred to as nodes) connected by communication links.
- A network is a group of two or more computer systems sharing services and interacting in some manner.
- A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.
- A link can be a cable, air, optical fibre, or any medium which can transport a signal carrying information.
- A computer network consists of a collection of computers, printers and other equipment that is connected together so that they can communicate with each other.
- A Computer network should ensure reliability of the data communication process, security of the data, and performance by achieving higher throughput and smaller delay times.

Introduction to Computer Networks

- A network is an interconnected collection of autonomous computers. Two computers are said to be interconnected if they are capable of exchanging information.
- Fig 1 gives an example of a network in a school comprising of a local area network or LAN connecting computers with each other, the internet, and various servers.

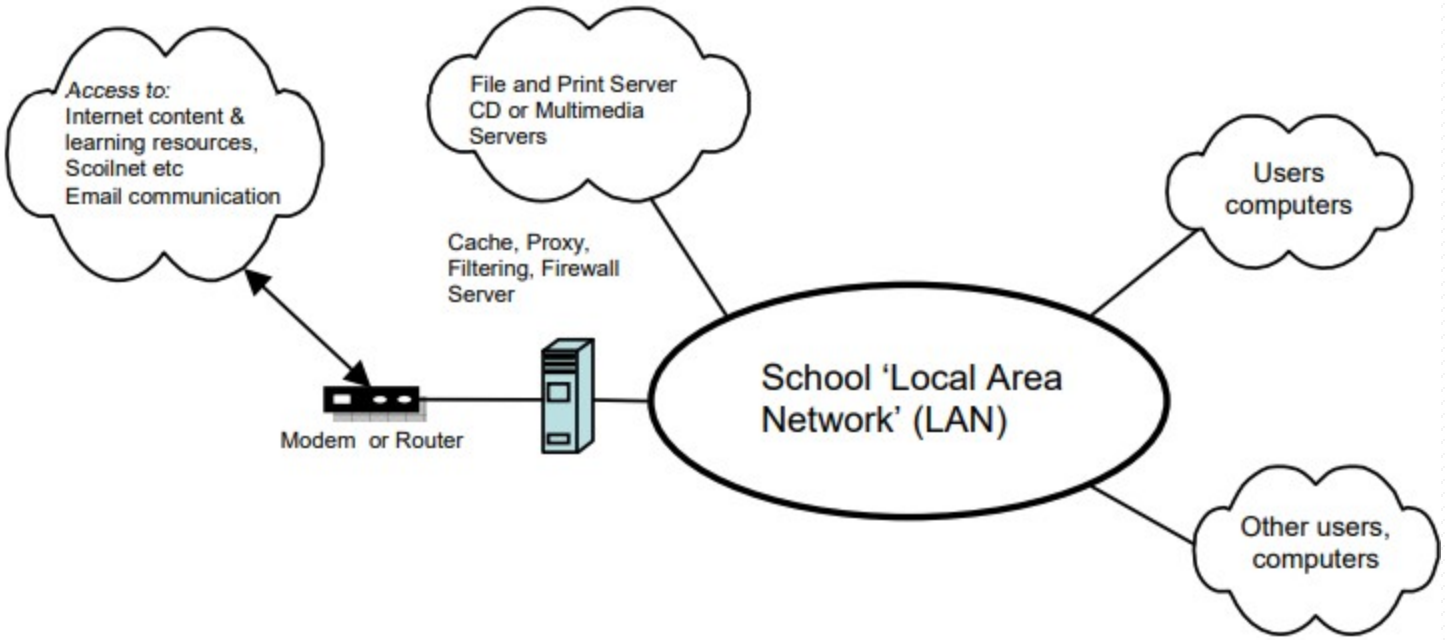


Fig 1: Representation of Network in a school.

Advantages

- (I) RESOURCE SHARING. The aim is to make all programs, data and peripherals available to anyone on the network irrespective of the physical location of the resources and the user.
- (ii) RELIABILITY. A file can have copies on two or three different machines, so if one of them is unavailable (hardware crash), the other copies could be used.
- For military, Banking, Air reservation and many other applications it is of great importance.
- (iii) COST FACTOR. Personal computers have better price/performance ratio than micro computers. So it is better to have PC's, one per user, with data stored on one shared file server machine.
- (iv) COMMUNICATION MEDIUM. Using a network, it is possible for managers, working far apart, to prepare financial report of the company.
- The changes at one end can be immediately noticed at another and hence it speeds up co-operation among them.

Categories of Network

- Networks are categorized on the basis of their size. The three basic categories of computer networks are:
- Local Area Networks (LAN) is usually limited to a few kilometres of area. It may be privately owned and could be a network inside an office on one of the floor of a building or a LAN could be a network consisting of the computers in a entire building.
- Wide Area Network (WAN) is made of all the networks in a (geographically) large area. The network in the entire state of Gujarat could be a WAN.
- Metropolitan Area Network (MAN) is of size between LAN & WAN. It is larger than LAN but smaller than WAN. It may comprise the entire network in a city like Mumbai.

Categories of Network

- Wireless Networks: Mobile computers such as notebook computers laptops are fastest growing segment of computer industry.
- Users want to connect this machine to their office LANs to see the data when they are out from the office, since the wired connection is not possible we have to use wireless networks.

- Internet: People connected to one network may require to communicate with, people connected to a different network.
- Such collection of interconnected networks is called as Internet works or Internet.
- A common form of Internet is collections of LANs connected by WA are formed when distinct networks are connected with each other through routers and hosts.

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.
- Examples of Standard Creation Committees :
- 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:

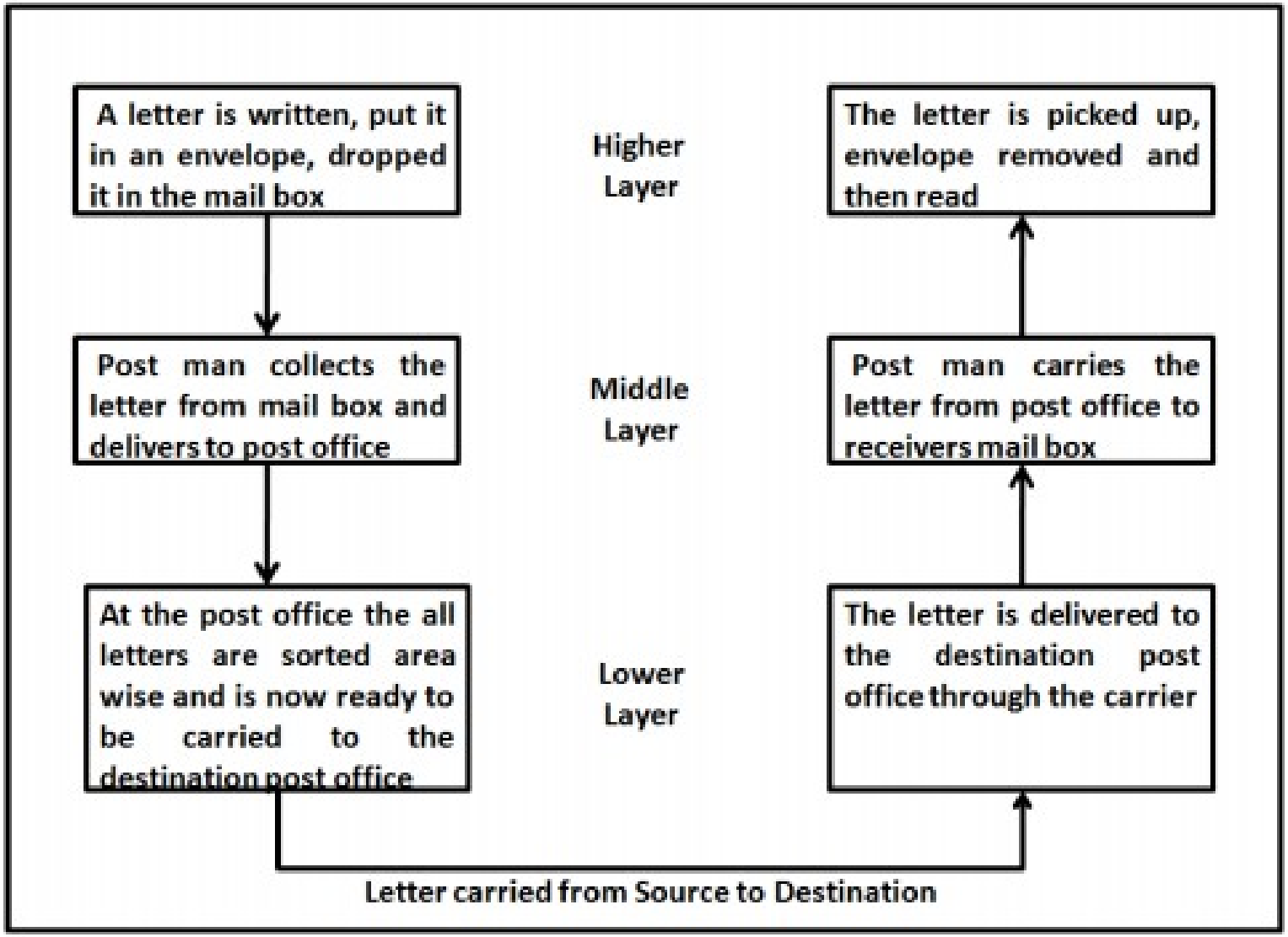


Fig: Concept of layer task: sending a letter

LAYERED TASK

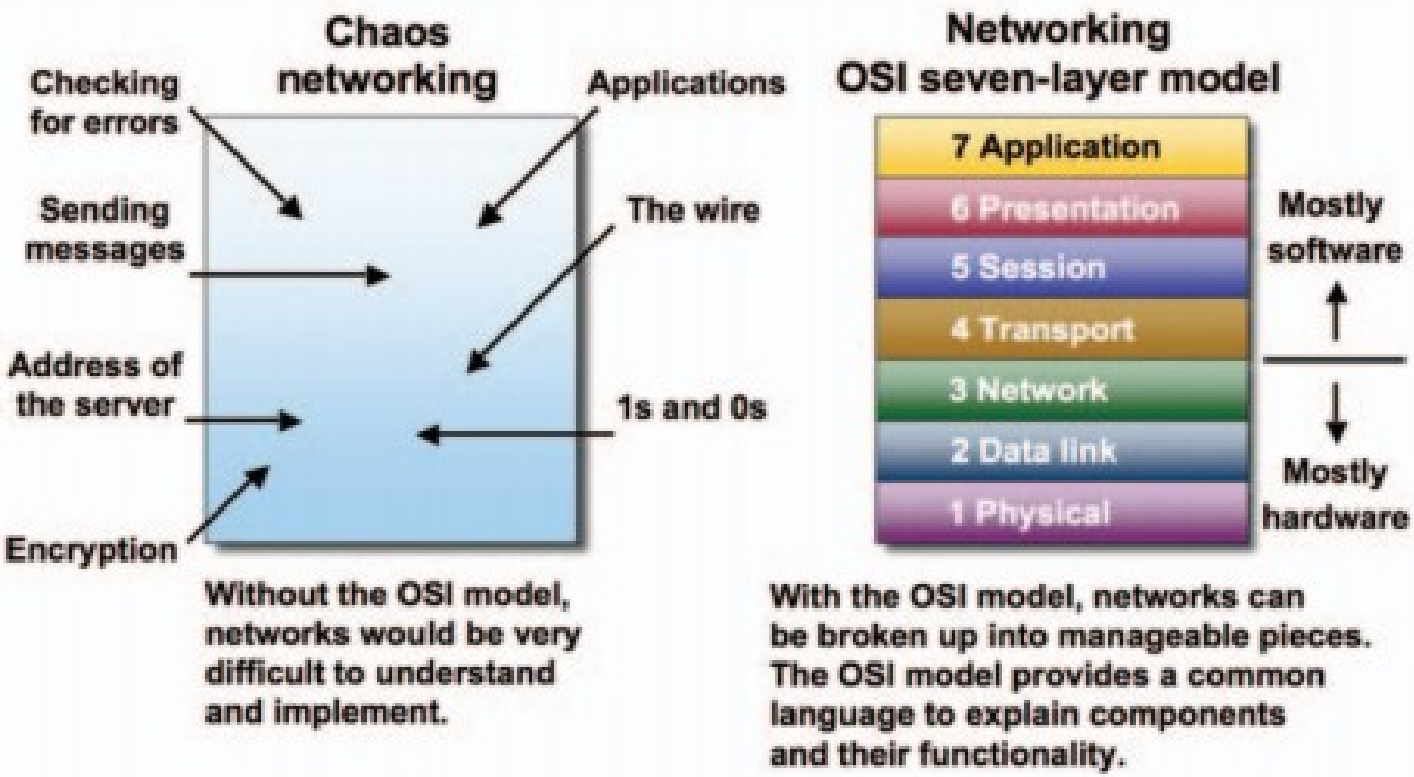
- v. The above figure shows
  - a. Sender, Receiver & Carrier
  - b. Hierarchy of layers
- vi. At the sender site, the activities take place in the following descending order:
  - a. Higher Layer: The sender writes the letter along with the sender and receivers address and put it in an envelope and drop 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.



Introduction to OSI Model & its layers

- The Open Systems Interconnection (OSI) Model was developed by International Organization for Standardization (ISO).
- OSI model was developed to allow systems with different platforms to communicate with each other. Platform could mean hardware, software or operating system.
- It is a network model that defines the protocols for network communications.
- It is a hierarchical model that groups its processes into layers. It has 7 layers as follows: (Top to Bottom)
- 1. Application Layer
- 2. Presentation Layer
- 3. Session Layer
- 4. Transport Layer
- 5. Network Layer
- 6. Data Link Layer
- 7. Physical Layer
- Each layer has specific duties to perform and has to cooperate with the layers above and below it.

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.

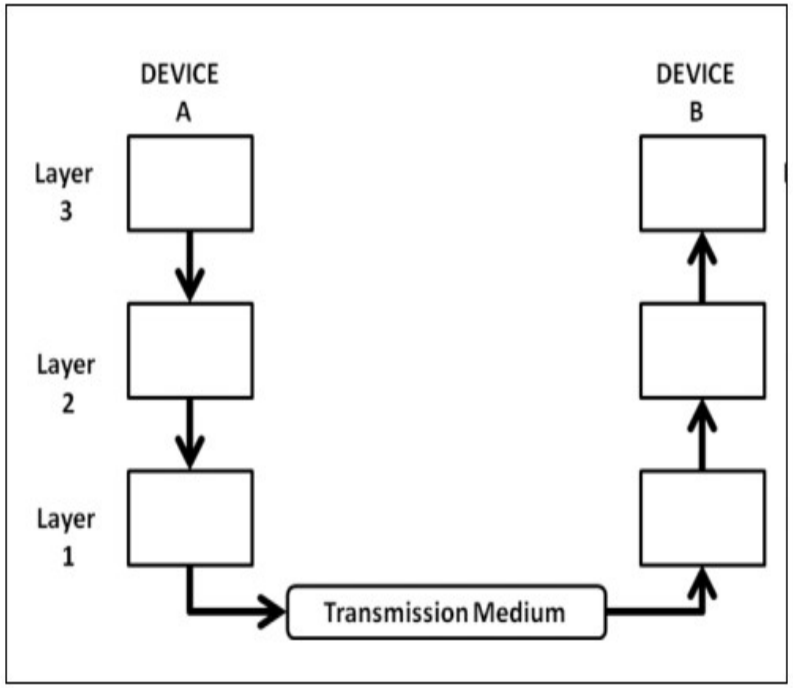


Fig: Flow of Data from Device A to Device B through various layers

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 below.

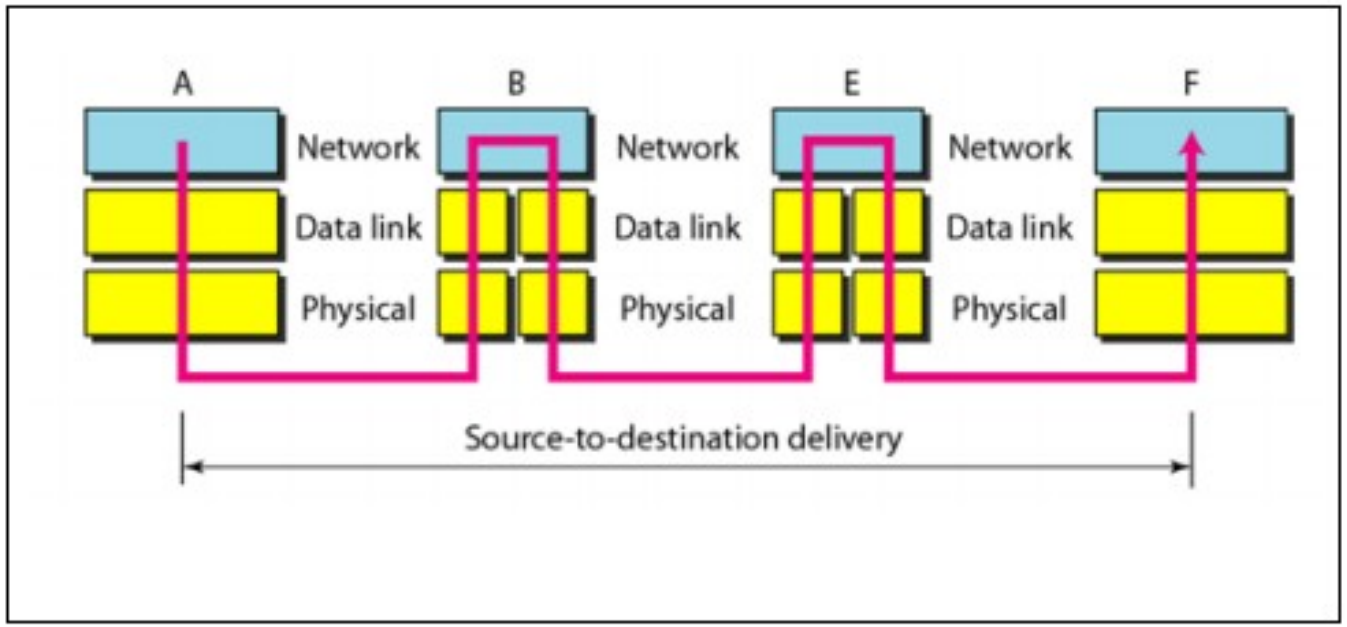


Fig: Data Transfer through Intermediate nodes

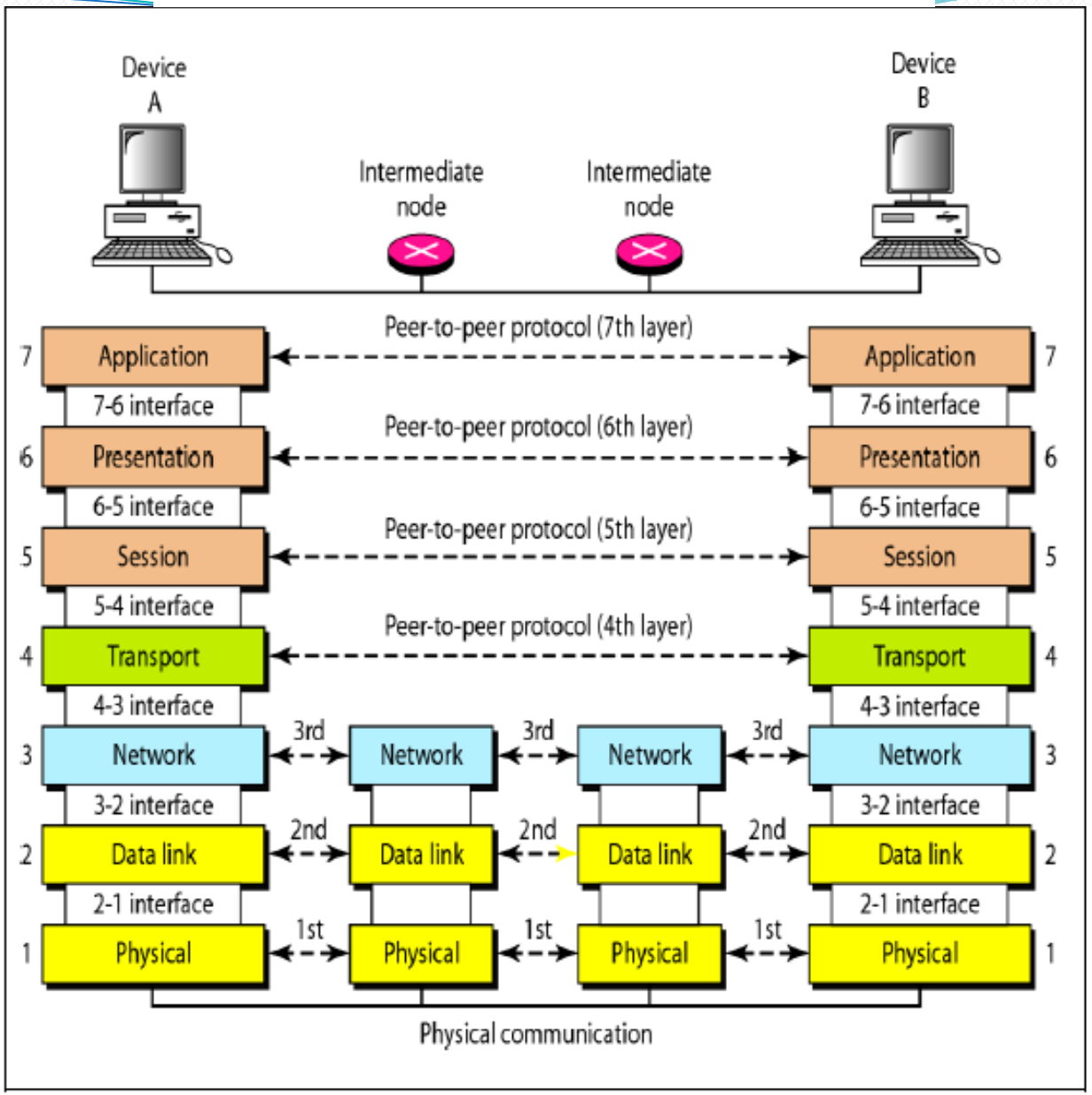
- The Data Link layer determines the next node where the message is supposed to be forwarded and the network layer determines the final recipient.

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.

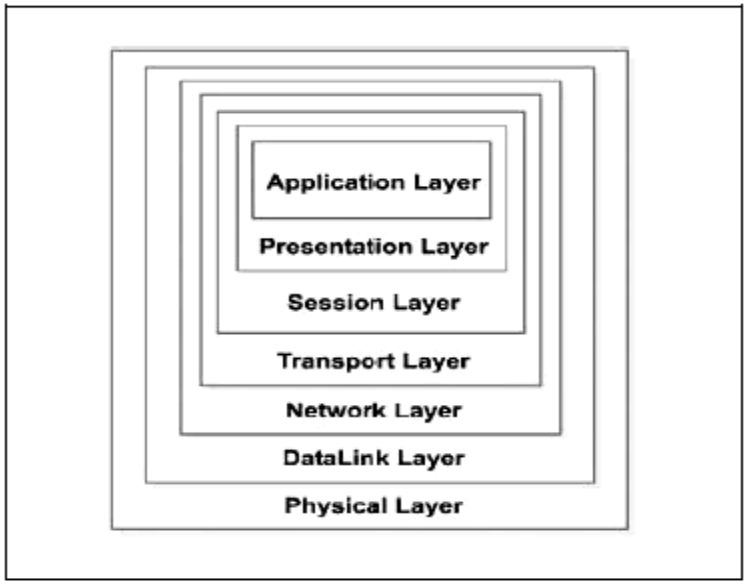


Fig: Encapsulation

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.
- **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.

Physical Layer

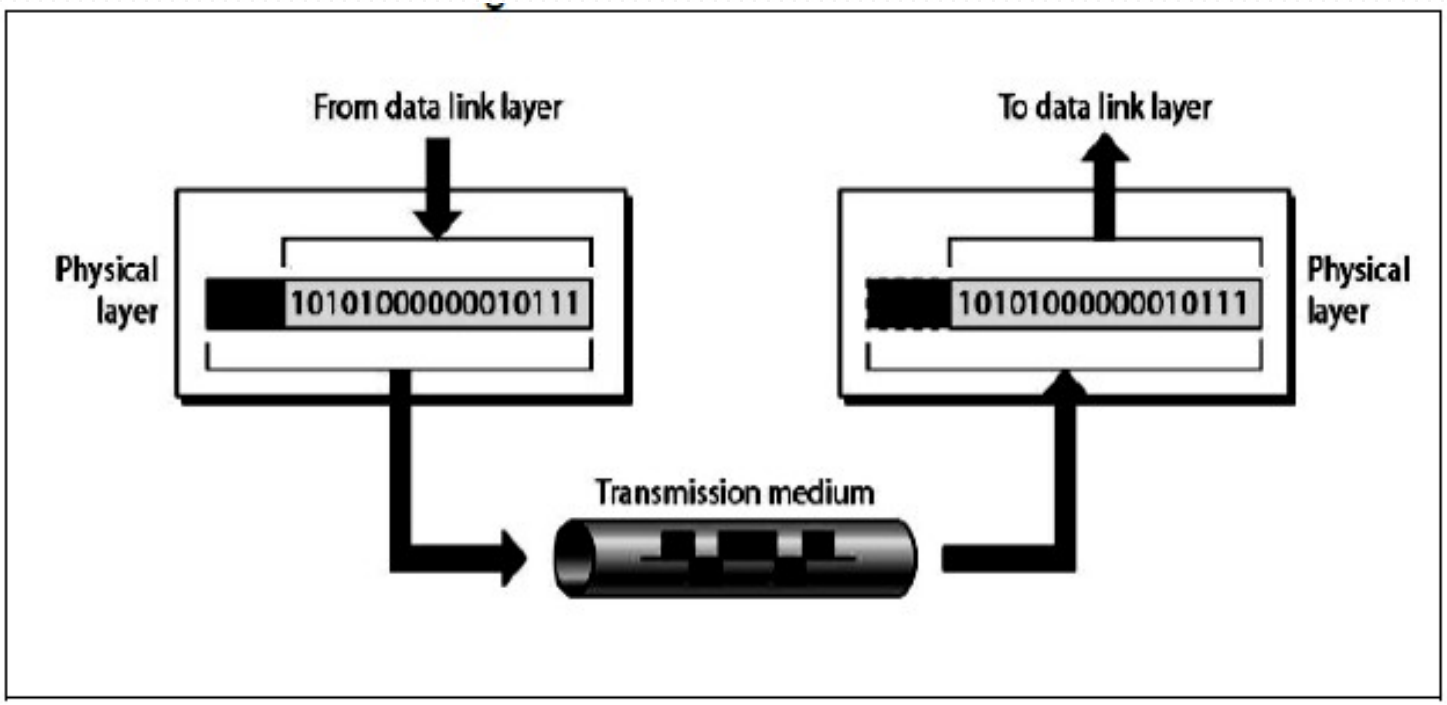


Fig: Transmission of data to and from Physical Layer

Physical Layer

- 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.
- 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.

Data Link Layer

- **I**. The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms.
- **II.** 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:

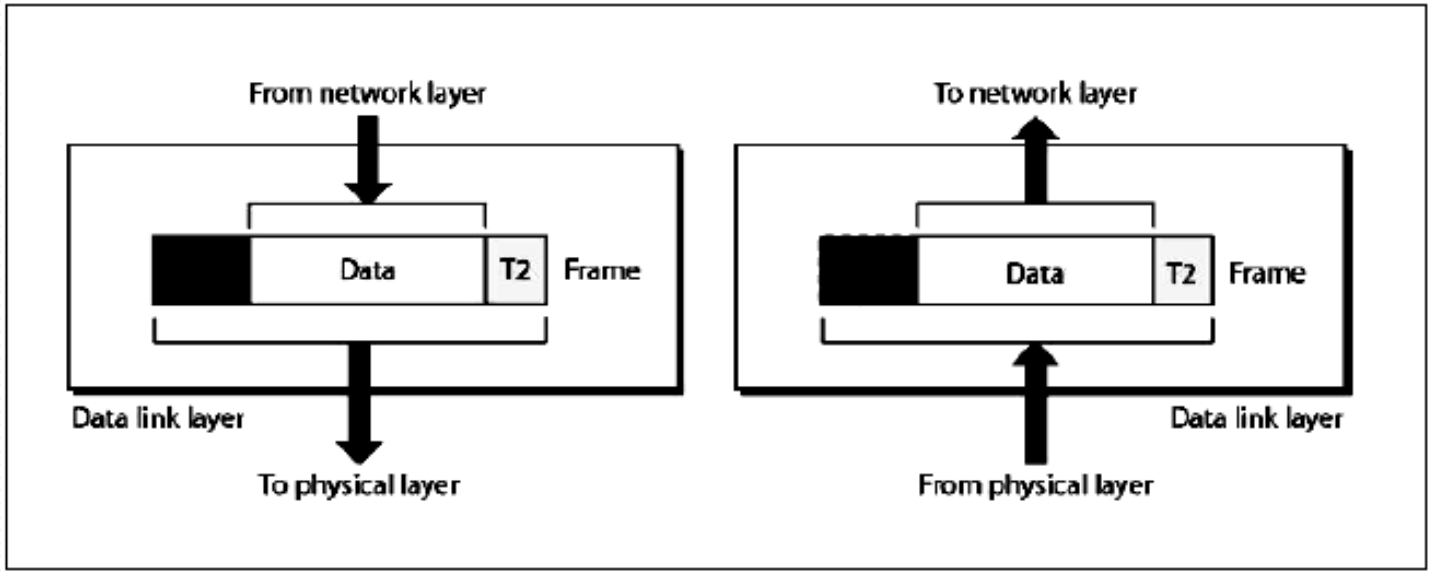


Fig: Data Link Layer: The process of Framing

Data Link Layer

- **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.
  - c. In case the receiver happens to be on the same physical network as the sender; the receiver is at only one hop from the sender and 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.

Data Link Layer

- **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.
- **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.

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.

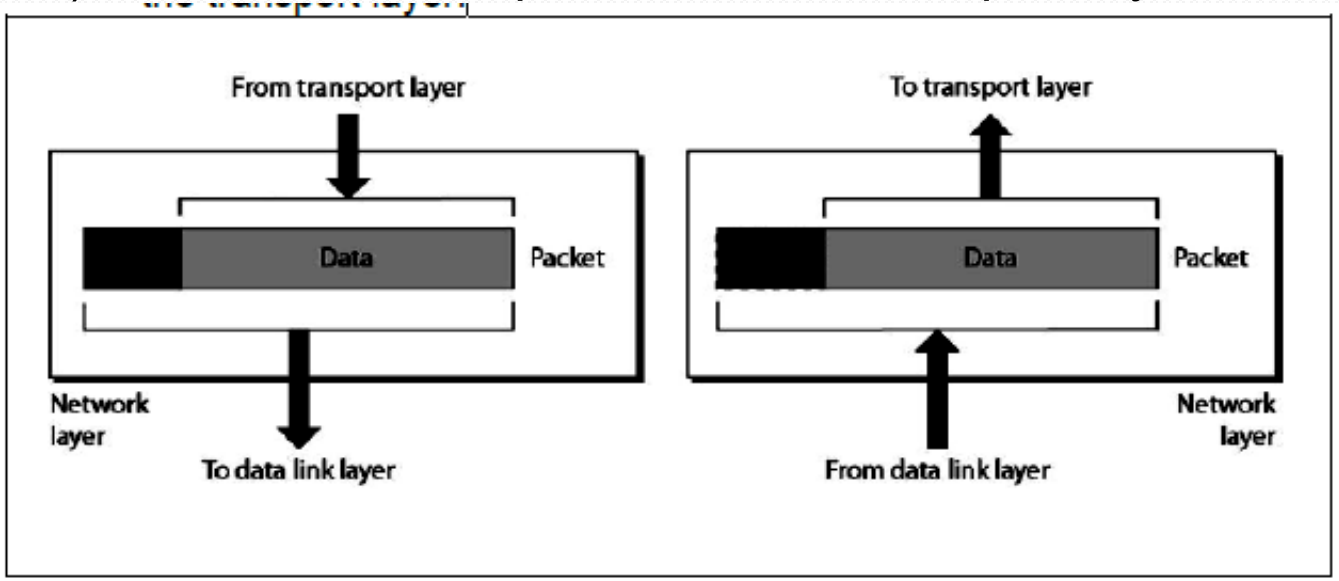


Fig: Network Layer

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.

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

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

- **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.

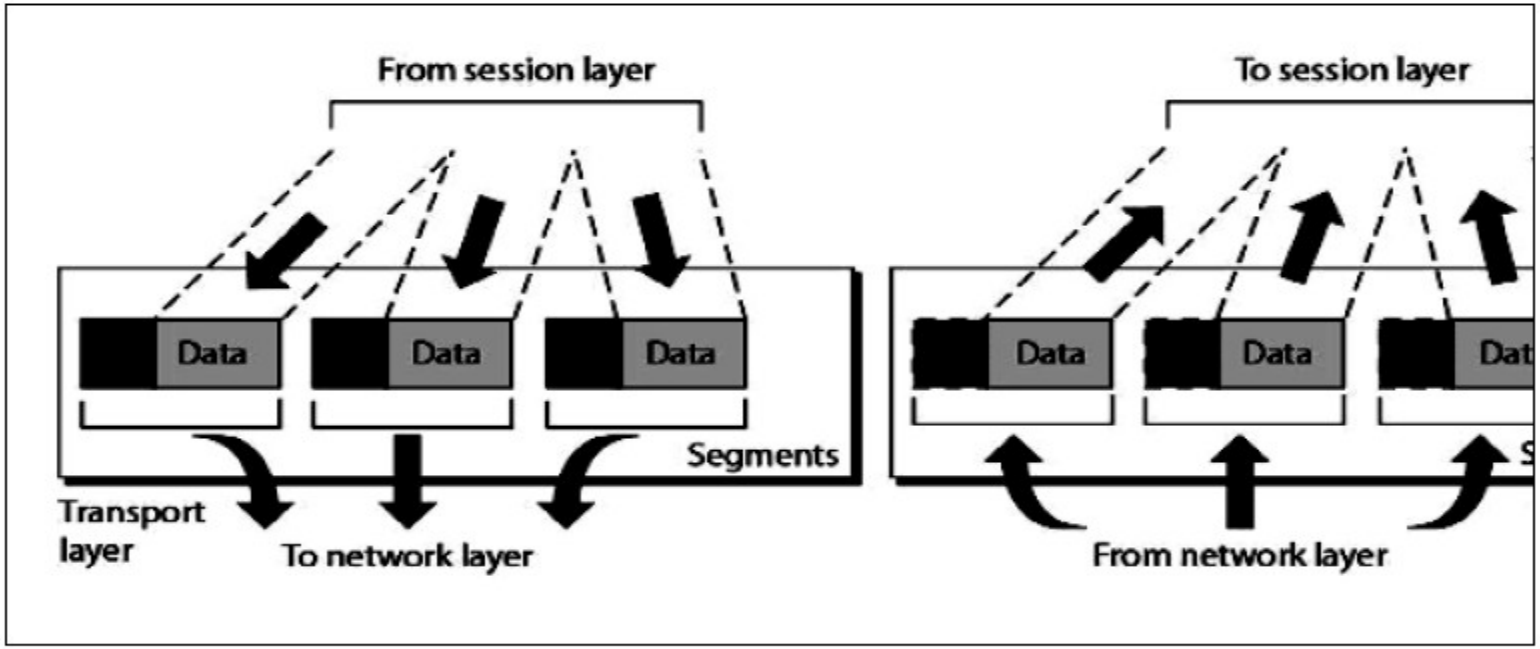
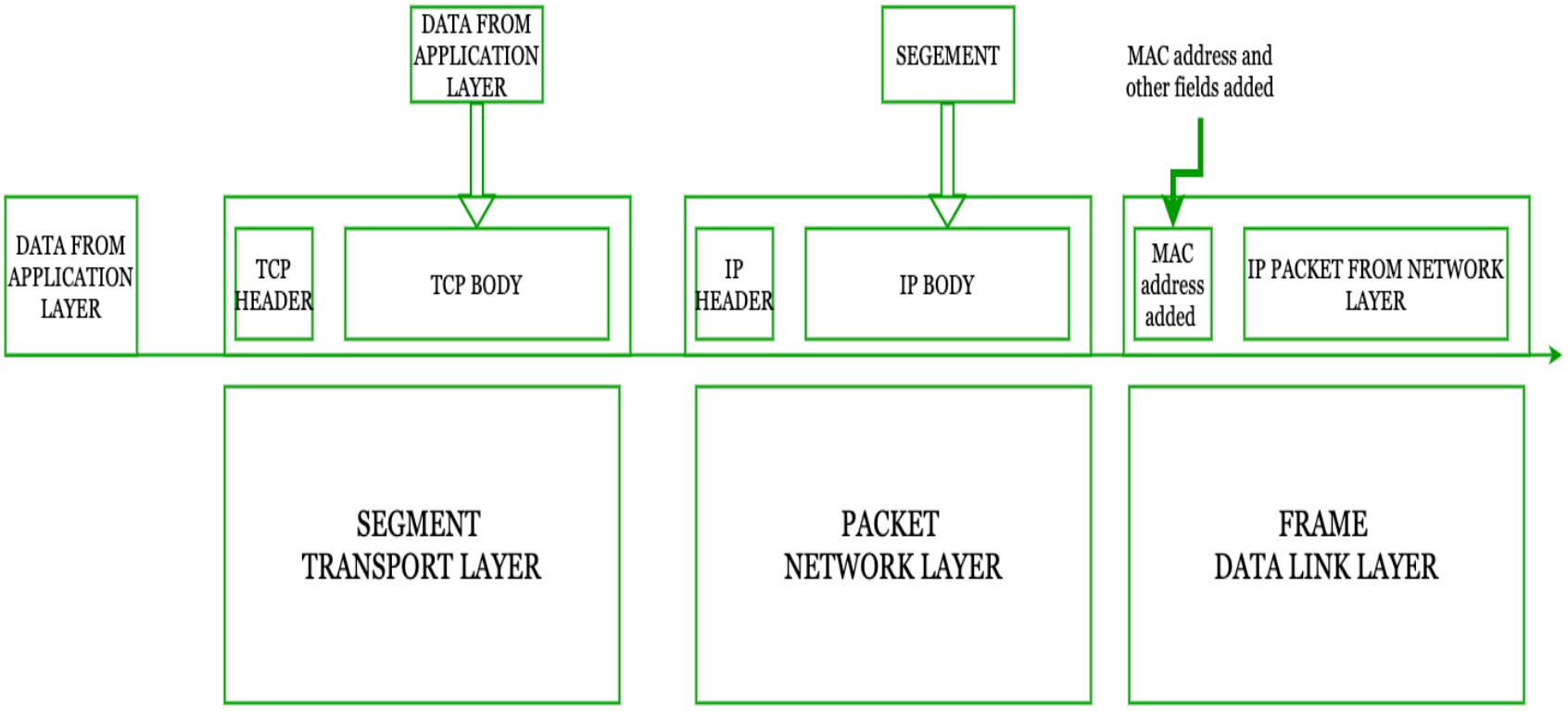


Fig: Transport Layer

Transport Layer

- **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.

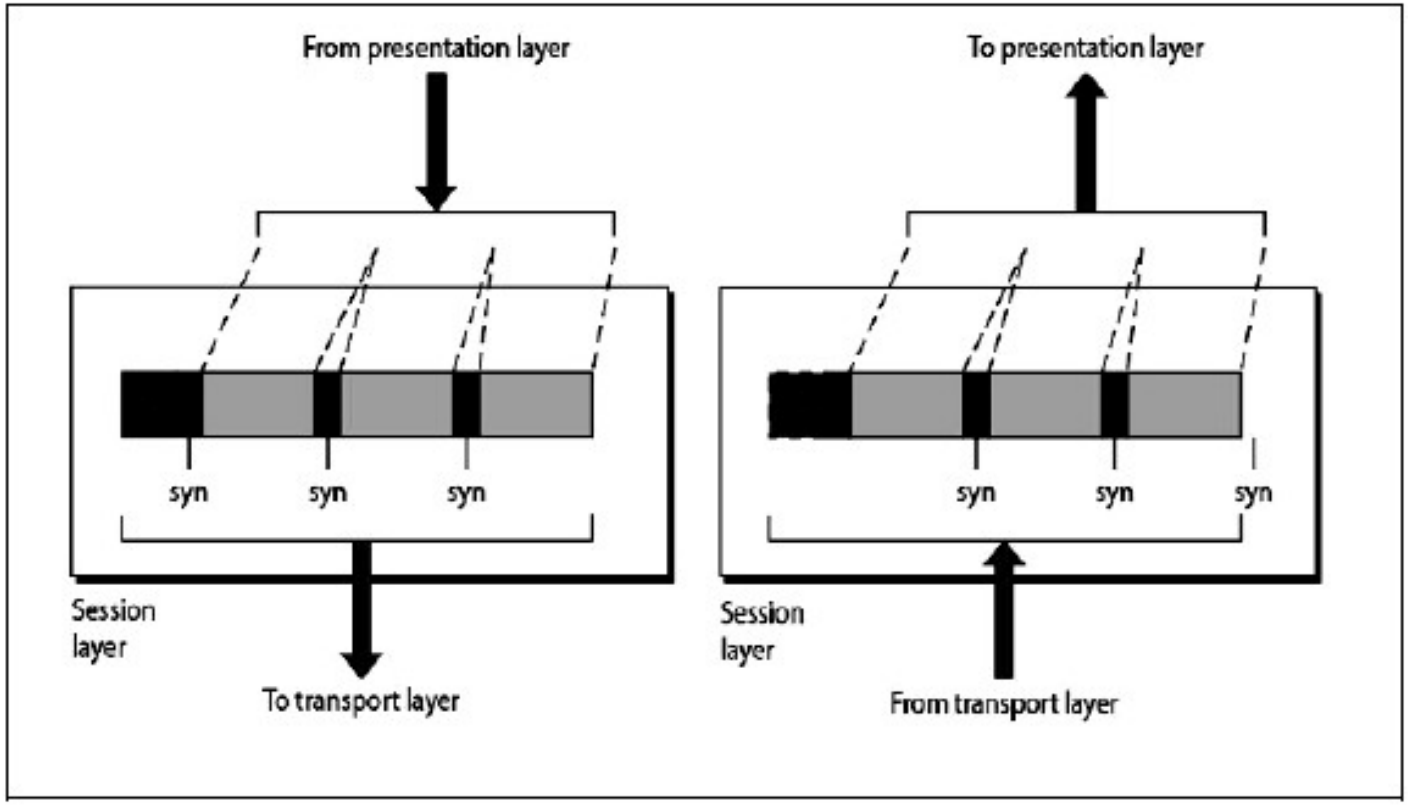
Fragment-Packet-Frame



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



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. Hence a translation service may be required which is provided by the Presentation layers.

Presentation Layer

- **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.

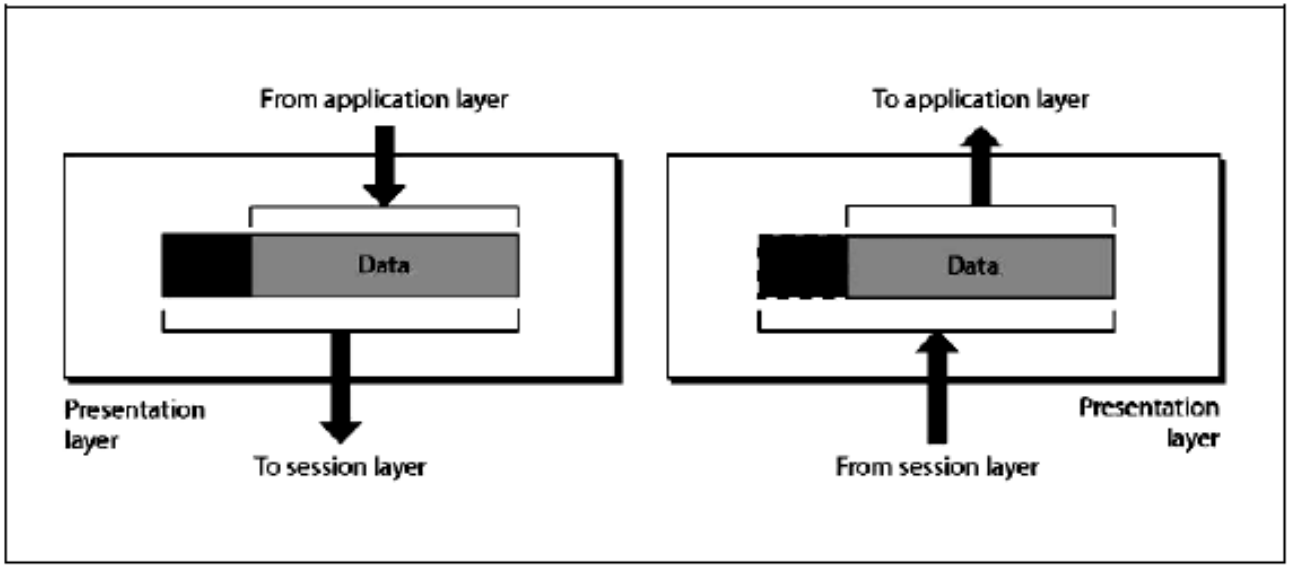


Fig : Presentation Layer

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

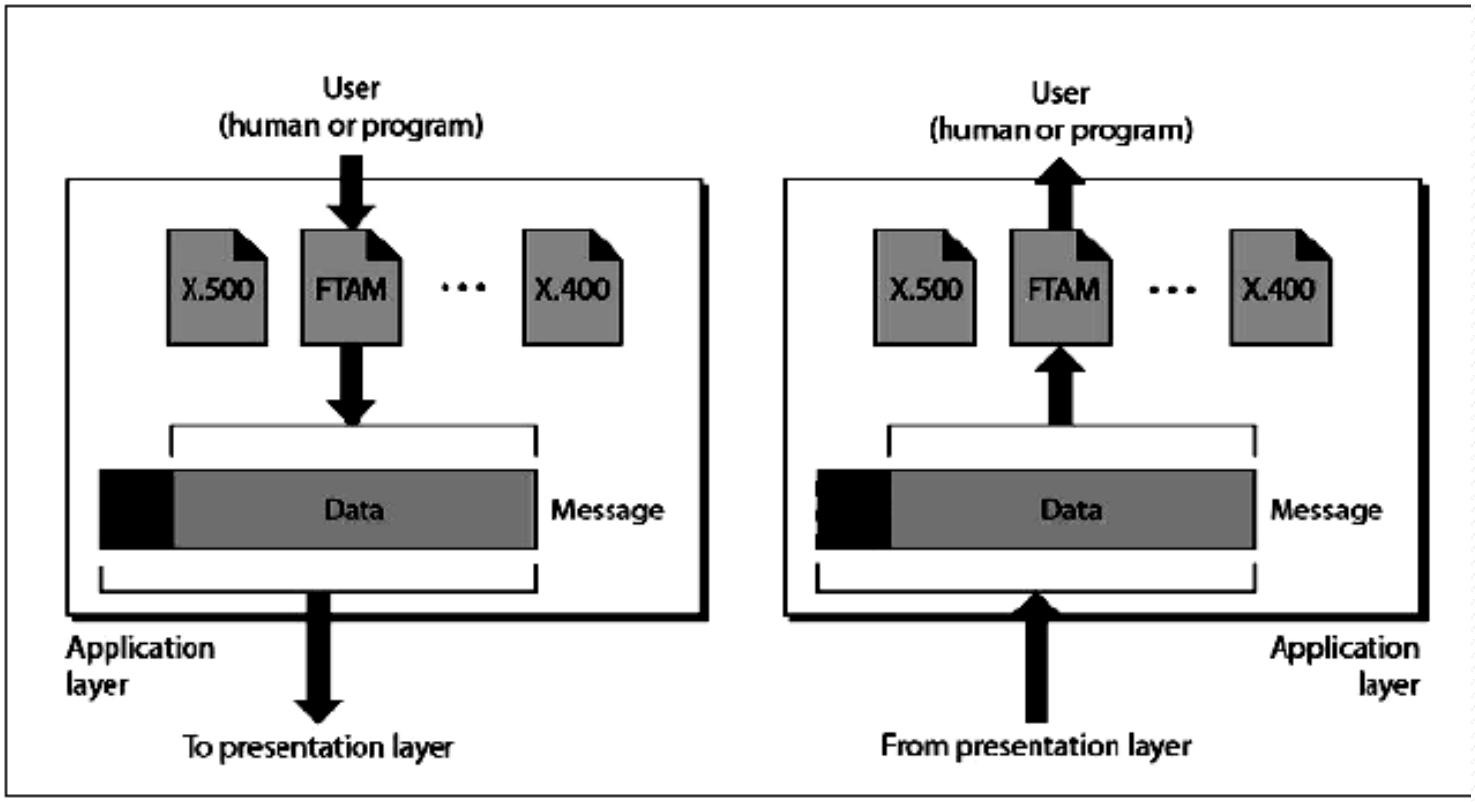
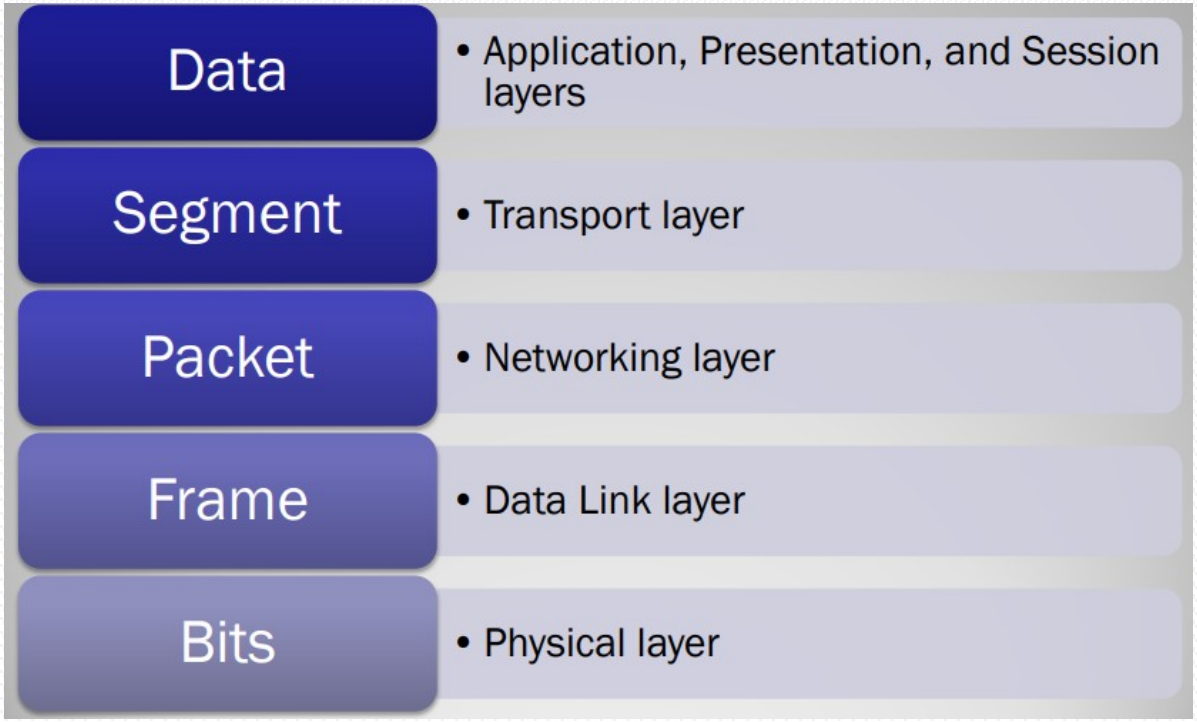


Fig : Application Layer

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.



The TCP/IP Model

- 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.
- Originally had four layers (bottom to top):
  - 1. Host to Network Layer
  - 2. Internet Layer
  - 3. Transport Layer
  - 4. Application Layer
- The figure for TCP/IP model is as follows:

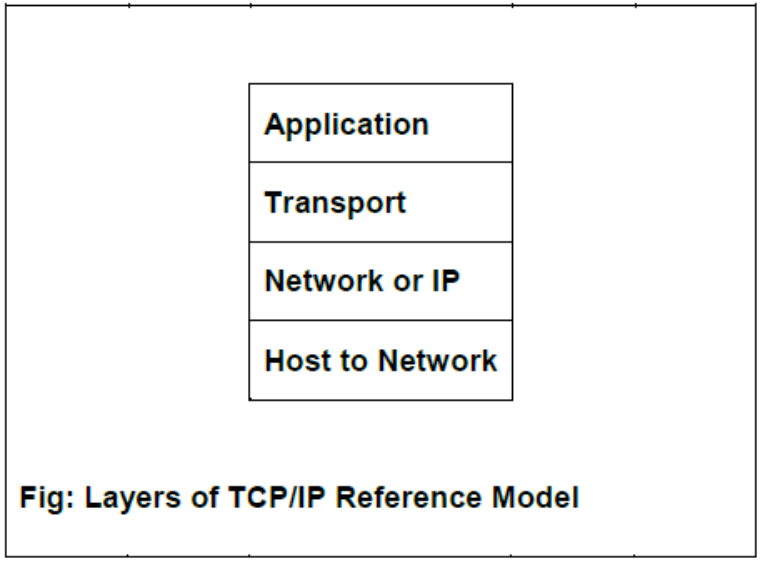
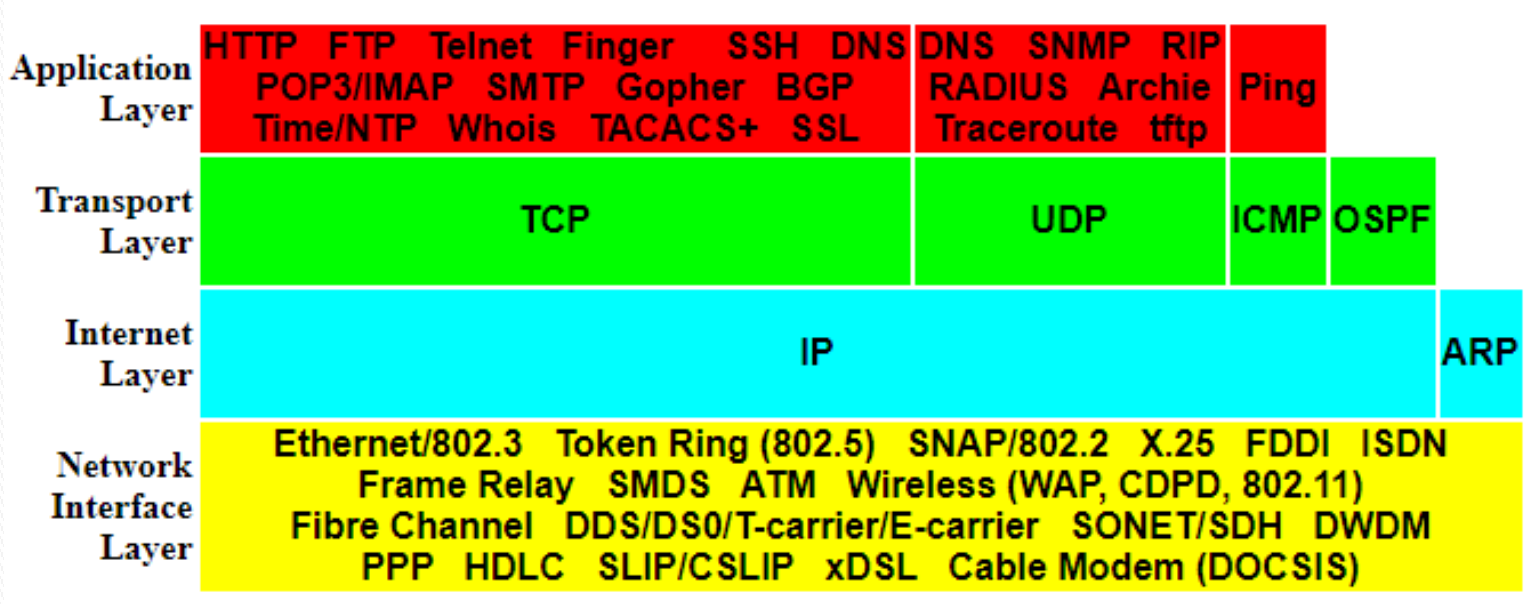


Fig: Layers of TCP/IP Reference Model

The TCP/IP Model

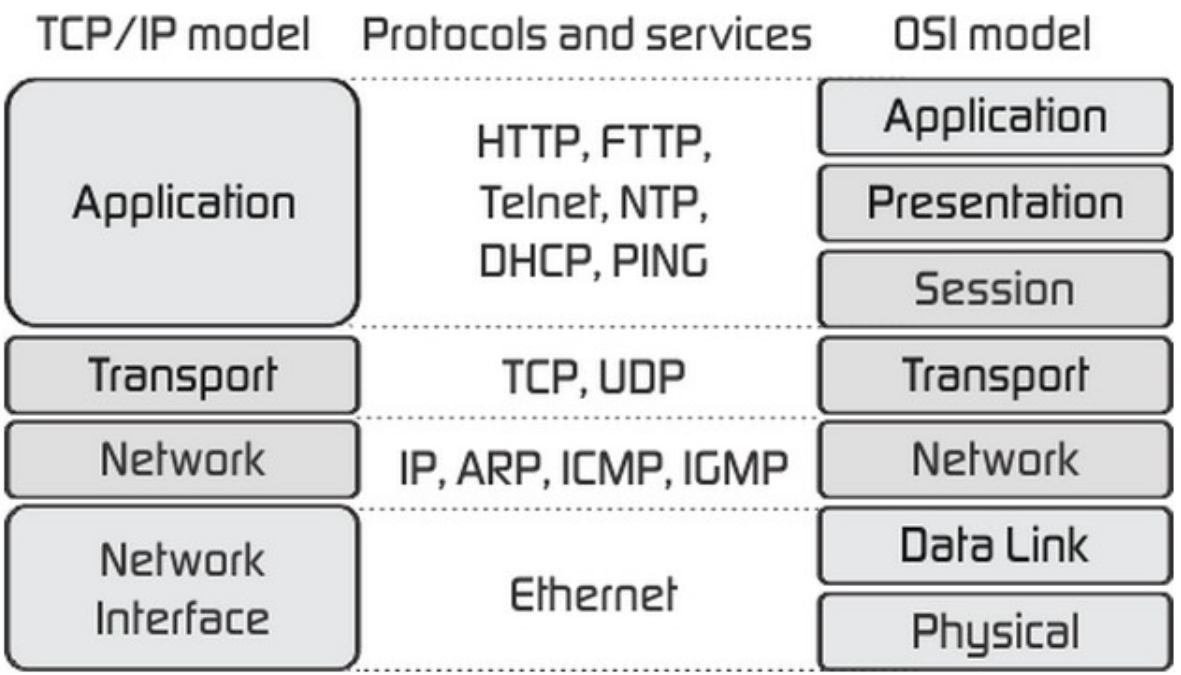
- The most common protocol used; in data networks today is the TCP / IP protocol stack. TCP/IP is used to interconnect devices in corporate networks as well the protocol of the Internet.
- The TCP/IP suite of protocols was developed as part of the research done by the Defence Advance Research Projects 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 team about how the TCP/IP protocol suite maps to a four -layer model.

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

The TCP/IP Model

- The Network Interface layer is responsible for communicating directly with the network. The Internet layer is primarily concerned with the routing and delivery of packets through the Internet protocol (IP).
- All protocols in transport layer must use IP to send data.
- The transport layer maps to the Transport Layer of OSI model and is responsible for providing communication between machines for applications.
- The Application layer of the Internet Protocol Suite is responsible for all the activities that occur in the session, presentation an application layer of the OSI model.
- Numerous protocols have been written for use in this layer, including HTTP, Simple Network Management Protocol SNMP File Transfer Protocol (FTP) etc.

Functions of the Layers of TCP/IP model

- **A. 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.
- **B. Network Layer or IP**
- 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 a connection-less & unreliable protocol.
- It is a best effort delivery service. i.e. there is no error checking in IP, it simply sends the data and relies on its underlying layers to get the data transmitted to the destination.
- IP transports data by dividing it into packets or 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.
- In other words, since there is no connection set up between the sender and the receiver the packets find the best possible path and reach the destination. Hence, the word connection-less.

Functions of the Layers of TCP/IP model

- The packets may get dropped during transmission along various routes. Since IP does not make any guarantee about the delivery of the data its call an unreliable protocol.
- Even if it is unreliable IP cannot be considered weak and useless; since it provides only the functionality that is required for transmitting data thereby giving maximum efficiency. Since there is no mechanism of error detection or correction in IP, there will be no delay introduced on a medium where there is no error at all.
- IP is a combination of four protocols:
- 1. ARP
- 2. RARP
- 3. ICMP
- 4. IGMP
- 1. ARP – Address Resolution Protocol
- I. It is used to resolve the physical address of a device on a network, where its logical address is known.
- II. Physical address is the 48 bit address that is imprinted on the NIC or LAN card, Logical address is the Internet Address or commonly known as IP address that is used to uniquely & universally identify a device.

Functions of the Layers of TCP/IP model

- 2. RARP– Reverse Address Resolution Protocol
- I. It is used by a device on the network to find its Internet address when it knows its physical address.
- 3. ICMP- Internet Control Message Protocol
- I. It is a signalling mechanism used to inform the sender about datagram problems that occur during transit
- II. It is used by intermediate devices.
- III. In case and intermediate device like a gateway encounters any problem like a corrupt datagram it may use ICMP to send a message to the sender of the datagram.
- 4. IGMP- Internet Group Message Protocol
- I. It is a mechanism that allows to send the same message to a group of recipients. .

Functions of the Layers of TCP/IP model

- **C. 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
- 1. TCP – Transmission Control Protocol
- I. TCP is a connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted.
- II. 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.

Functions of the Layers of TCP/IP model

- 2. UDP – User Datagram Protocol
- I. UDP is a simple protocol used for process to process transmission.
- II. It is an unreliable, connectionless protocol for applications that do not require flow control or error control.
- III. It simply adds port address, checksum and length information to the data it receives from the upper layer.
- 3. SCTP – Stream Control Transmission Protocol
- I. SCTP is a relatively new protocol added to the transport layer of TCP/IP protocol suite.
- II. It combines the features of TCP and UDP.
- III. It is used in applications like voice over Internet and has a much broader range of applications
- **D. Application Layer**
- I. The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and define high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

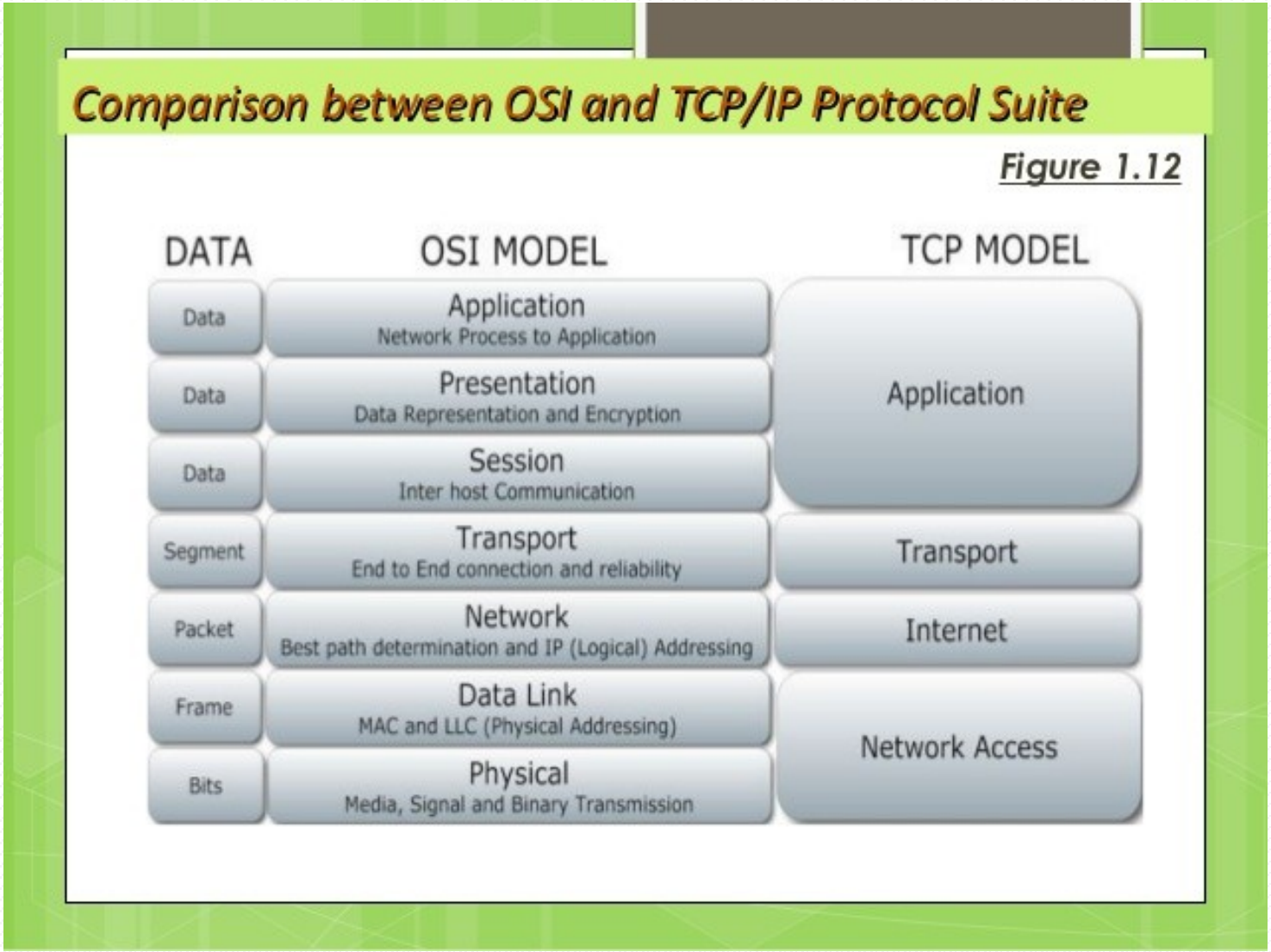
The TCP/IP Model

- The structure TCP/IP model is very similar to the structure of the OSI reference model. The OSI model has seven layers where the TCP/IP model has four layers.
- The Application layer of TCP/IP model corresponds to the Application Layer of Session, Presentation & Application Layer of OSI model.
- The Transport layer of TCP/IP model corresponds to the Transport Layer of OSI model.
- The Network layer of TCP/IP model corresponds to the Network Layer of OSI model.
- The Host to network layer of TCP/IP model corresponds to the Physical and Datalink Layer of OSI model.
- The diagram showing the comparison of OSI model and TCP/IP model along with the protocols is as shown below:

Differences between OSI and TCP/IP Model

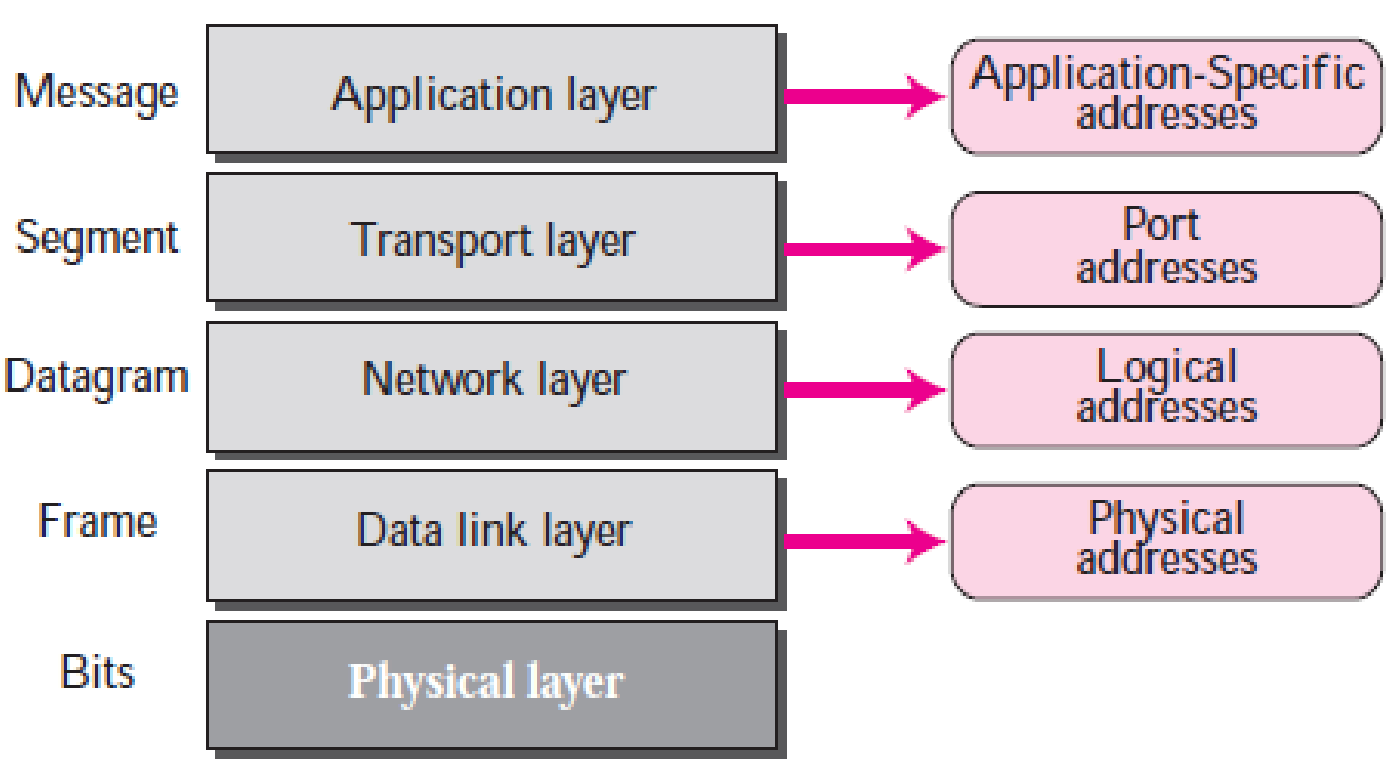
TCP/IP	OSI
Implementation of OSI model	Reference model
Model around which Internet is developed	This is a theoretical model
Has only 4 layers	Has 7 layers
Considered more reliable	Considered a reference tool
Protocols are not strictly defined	Stricter boundaries for the protocols
Horizontal approach	Vertical approach
Combines the session and presentation layer in the application layer	Has separate session and presentation layer
Protocols were developed first and then the model was developed	Model was developed before the development of protocols
Supports only connectionless communication in the network layer	Supports connectionless and connection-oriented communication in the network layer
Protocol dependent standard	Protocol independent standard

Comparison: OSI and TCP/IP Model



ADDRESSING IN TCP/IP

- The TCP/IP protocol suited involves 4 different types of addressing:
- 1. Physical Address
- 2. Logical Address
- 3. Port Address
- 4. Specific Address



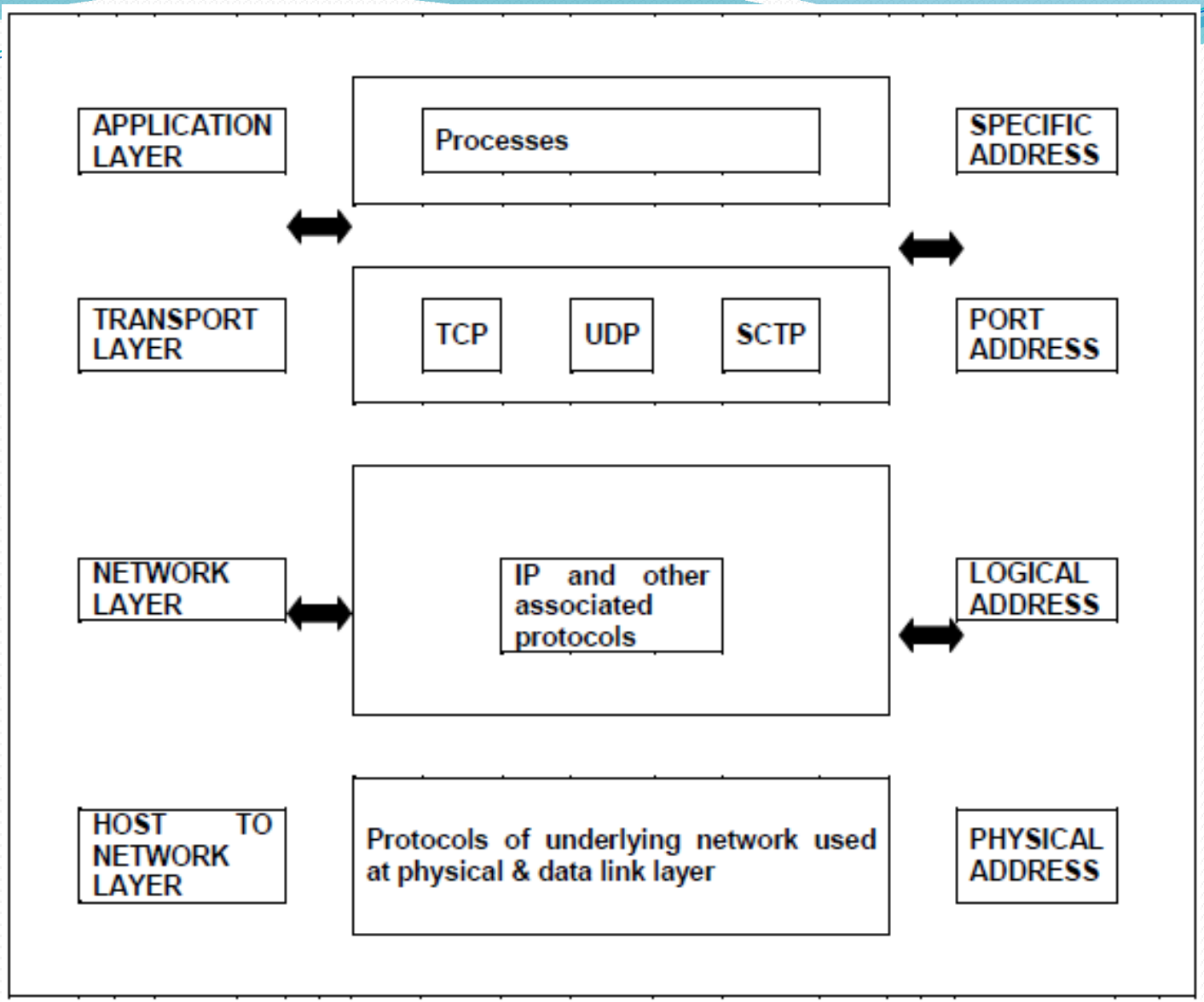


Fig: Addressing in TCP/IP model

ADDRESSING IN TCP/IP

- **1. Physical Address**
- **i.** Physical Address is the lowest level of addressing, also known as link address.
- **ii.** It is local to the network to which the device is connected and unique inside it.
- **iii.** The physical address is usually included in the frame and is used at the data link layer.
- **iv.** 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.
- **v.** The size of physical address may change depending on the type of network. Ex. An Ethernet network uses a 6 byte MAC address.

ADDRESSING IN TCP/IP

- **2. Logical Address**
- i. Logical Addresses are used for universal communication.
- ii. Most of the times the data has to pass through different networks; since physical addresses are local to the network there is a possibility that they may be duplicated across multiples networks also the type of physical address being used may change with the type of network encountered.
- For ex: Ethernet to wireless to fibre optic. Hence physical addresses are inadequate for source to destination delivery of data in an internetwork environment.
- iii. Logical Address is also called as IP Address (Internet Protocol address).
- iv. At the network layer, device i.e. computers and routers are identified universally by their IP Address.
- v. IP addresses are universally unique.
- vi. Currently there are two versions of IP addresses being used:
- a. IPv4: 32 bit address, capable of supporting 232 nodes
- b. IPv6: 128 bit address, capable of supporting 2128 nodes

ADDRESSING IN TCP/IP

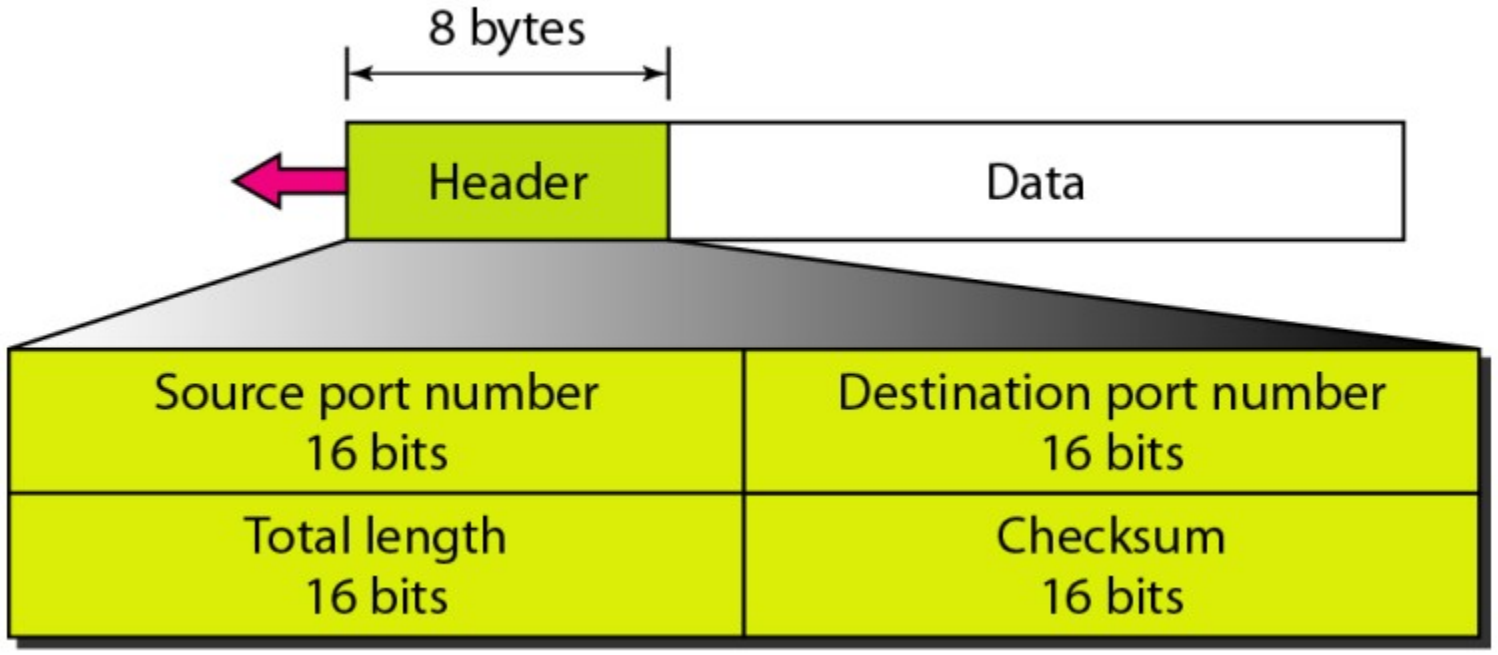
- **3. Port Address**
- **VIII.** A logical address facilitates the transmission of data from source to destination device. But the source and the destination both may be having multiple processes communicating with each other.
- Ex. Users A & B are chatting with each other using Google Talk, Users B & C are exchanging emails using Hotmail.
- The IP address will enable transmitting data from A to B, but still the data needs to be delivered to the correct process. The data from A cannot be given to B on yahoo messenger since A & B are communicating using Google Talk.
- **IX.** Since the responsibility of the IP address is over here there is a need of addressing that helps identify the source and destination processes.
- In other words, data needs to be delivered not only on the correct device but also on the correct process on the correct device.
- **X.** A Port Address is the name or label given to a process. It is a 16 bit address.
- **XI.** Ex. TELNET uses port address 23, HTTP uses port address 80

ADDRESSING IN TCP/IP

- **4. Specific Address**
- **i.** Port address facilitates the transmission of data from process to process but still there may be a problem with data delivery.
- For Ex: Consider users A, B & C chatting with each other using Google Talk. Every user has two windows open, user A has two chat windows for B & C, user B has two chat windows for A & C and so on for user C. Now a port address will enable delivery of data from user A to the correct process (in this case Google Talk) on user B but now there are two windows of Google Talk for user A & C available on B where the data can be delivered.
- **ii.** Again the responsibility of the port address is over here and there is a need of addressing that helps identify the different instances of the same process.
- **iii.** Such address are user friendly addresses and are called specific addresses.
- **iv.** Other Examples: Multiple Tabs or windows of a web browser work under the same process that is HTTP but are identified using **Uniform Resource Locators (URL**), Email addresses.

User Datagram Protocol (UDP)

- The User Datagram Protocol (UDP) is called a connectionless, unreliable transport protocol. It does not add anything to the services of IP except to provide process-to-process communication instead of host-to-host communication.
- User Datagram Format:



UDP Operations

- **Connectionless Services**
- UDP provides a connectionless service. There is no relationship between the different user datagrams even if they are coming from the same source process and going to the same destination program.
- The user datagrams are not numbered. Also, there is no connection establishment and no connection termination, as is the case for TCP. This means that each user datagram can travel on a different path.
- **Encapsulation and Decapsulation**
- To send a message from one process to another, the UDP protocol encapsulates and decapsulates messages in an IP datagram.

UDP Operations

- **Flow and Error Control**
- UDP is a very simple, unreliable transport protocol. There is no flow control, hence the receiver may overflow with incoming messages.
- There is no error control mechanism in UDP except for the checksum. This means that the sender does not know if a message has been lost or duplicated.
- When the receiver detects an error through the checksum, the user datagram is silently discarded.

Well-known ports used with UDP

Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
53	Nameserver	Domain Name Service
67	BOOTPs	Server port to download bootstrap information
68	BOOTPc	Client port to download bootstrap information
69	TFTP	Trivial File Transfer Protocol
111	RPC	Remote Procedure Call
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol
162	SNMP	Simple Network Management Protocol (trap)

Transmission Control Protocol (TCP)

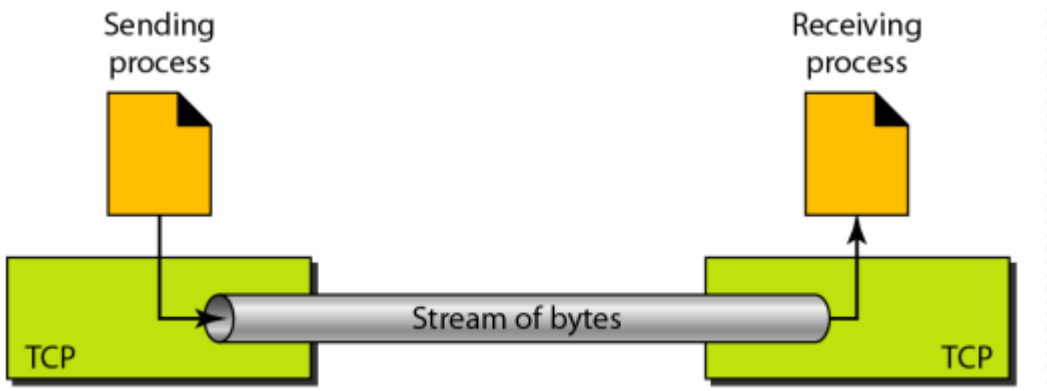
- TCP is a connection oriented protocol; it creates a virtual connection
- between two TCPs to send data. In addition, TCP uses flow and error control mechanisms at the transport level.
- In brief, TCP is called a connection-oriented, reliable transport protocol. It adds connection-oriented and reliability features to the services of IP.
- **TCP Services**
- Process-to-Process Communication
- TCP provides process-to-process communication using port numbers. Below Table lists some well-known port numbers used by TCP.

Transmission Control Protocol (TCP)

Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FTP, Data	File Transfer Protocol (data connection)
21	FTP, Control	File Transfer Protocol (control connection)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

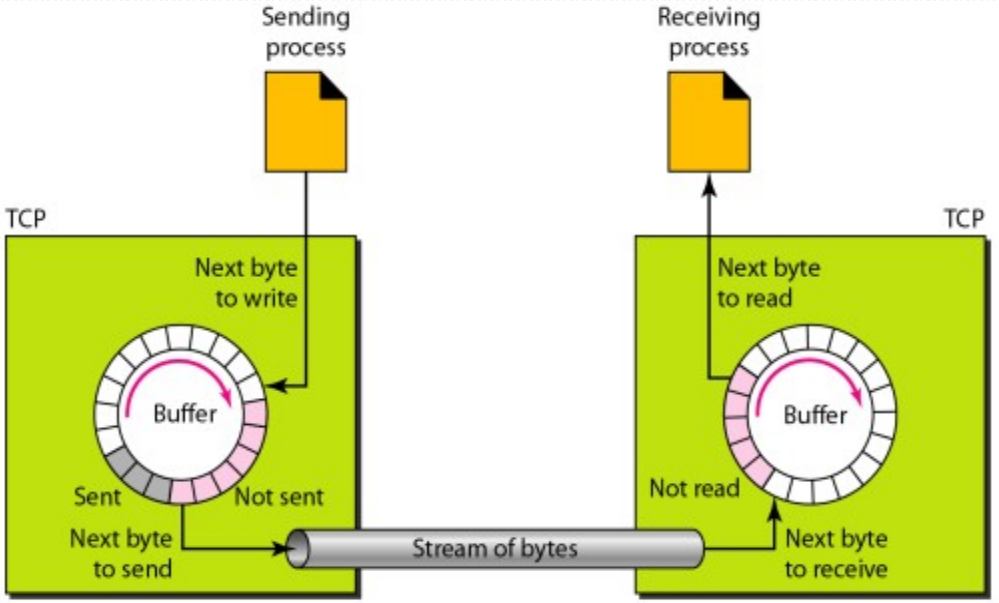
Transmission Control Protocol (TCP)

- Stream Delivery Service
- TCP, on the other hand, allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes.
- TCP creates an environment in which the two processes seem to be connected by an imaginary "tube“ that carries their data across the Internet.
- The sending process produces (writes to) the stream of bytes, and the receiving process consumes (reads from) them.



Transmission Control Protocol (TCP)

- Sending and Receiving Buffers
- Because the sending and the receiving processes may not write or read data at the same speed, TCP needs buffers for storage. There are two buffers, the sending buffer and the receiving buffer, one for each direction.
- One way to implement a buffer is to use a circular array of l-byte locations as shown in Figure.
- Normally the buffers are hundreds or thousands of bytes, depending on the implementation. We also show the buffers as the same size (20 bytes), which is not always the case.



Transmission Control Protocol (TCP)

- TCP segments
- At the transport layer, TCP groups a number of bytes together into a packet called a segment.
- TCP adds a header to each segment (for control purposes) and delivers the segment to the IP layer for transmission.
- The segments are encapsulated in IP datagrams and transmitted.
- This entire operation is transparent to the receiving process. Segments may be received out of order, lost, or corrupted and resent. All these are handled by TCP with the receiving process unaware of any activities.
- Full-Duplex Communication
- TCP offers full-duplex service, in which data can flow in both directions at the same time. Each TCP then has a sending and receiving buffer, and segments move in both directions

Transmission Control Protocol (TCP)

- Connection-Oriented Service
- TCP is a connection-oriented protocol. When a process at site A wants to send and receive data from another process at site B, the following occurs:
- 1. The two TCPs establish a connection between them.
- 2. Data are exchanged in both directions.
- 3. The connection is terminated.
- Reliable Service
- TCP is a reliable transport protocol. It uses an acknowledgement mechanism to check the safe and sound arrival of data.

Transmission Control Protocol (TCP)

- **TCP Features**
- Number System: There are two fields called the sequence number and the acknowledgement number refer to the byte number and not the segment number respectively.
- Flow Control: The receiver of the data controls the amount of data that are to be sent by the sender to prevent the receiver from being overwhelmed with data. The numbering system allows TCP to use a byte-oriented flow control.
- Error Control: To provide reliable service, TCP implements an error control mechanism. Although error control considers a segment as the unit of data for error detection (loss or corrupted segments), error control is byte-oriented.
- Congestion Control: TCP takes into account congestion in the network. The amount of data sent by a sender is not only controlled by the receiver (flow control), but is also determined by the level of congestion in the network.

Transmission Control Protocol (TCP)

- **A TCP Connection**
- TCP is connection-oriented. A connection-oriented transport protocol establishes a virtual path between the source and destination. All the segments belonging to a message are then sent over this virtual path.
- Using a single virtual pathway for the entire message facilitates the acknowledgement process as well as retransmission of damaged or lost frames.
- In TCP, connection-oriented transmission requires three phases:
- 1. connection establishment,
- 2. data transfer,
- 3. connection termination.

DNS (Domain Name System)

- DNS stands for Domain Name System. DNS is required for the functioning of the internet.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

DNS (Domain Name System)

- **Working of DNS**
- DNS is a client/server network communication protocol. DNS clients send requests to the server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as DNS resolver sends a request to the DNS server to obtain the IP address of a hostname.
- If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

DNS (Domain Name System)

- DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections:
- Generic Domains
- It defines the registered hosts according to their generic behaviour
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.
- Country Domain
- The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.
- Inverse Domain
- The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients.
- To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.