Department of Collegiate Education

GOVERNMENT FIRST GRADE COLLEGE
RAIBAG-591317

Department of Computer Science

LECTURE NOTES

SUBJECT : **DATA COMMUNICATIONS AND COMPUTER NETWORKS**

SUBJECT CODE : **17BScCST61**

CLASS : **BSC VI Sem Paper-1**

Subject In charge
Smt Bhagirathi Halalli
Assistant Professor

2019-20

UNIT 1: INTRODUCTION

Content:

1.1. Data communications,
1.2. Networks,
1.3. The internet,
1.4. Protocols and standards,
1.5. Network models – OSI model,
1.6. TCP/IP protocol suite,
1.7. Addressing.

1.1.Data Communications,

- **Data** refers to the raw facts that are collected while **information** refers to processed data that enables us to take decisions.
- Ex. When result of a particular test is declared it contains data of all students, when you find the marks you have scored you have the information that lets you know whether you have passed or failed.
- The word ***data*** refers to any information which is presented in a form that is agreed and accepted upon by is creators and users.

Data Communication

- 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.
- The following sections describe the fundamental characteristics that are important for the effective working of data communication process and are followed by the components that make up a data communications system.

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:

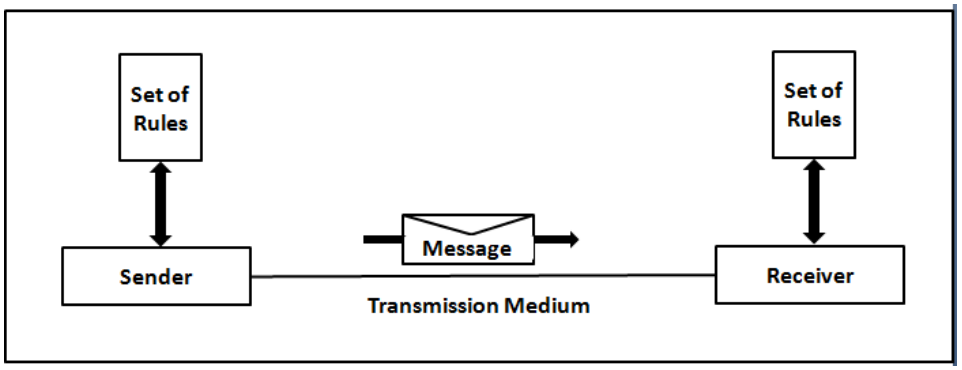


Fig. Components of a Data Communication System

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.

1.2.Networks,

- Computer Networks are used for data communications
- **Definition:**

A computer network can be defined as a collection of nodes. A node can be any device capable of transmitting or receiving data. The communicating nodes have to be connected by communication links.

- A Compute network should ensure
  reliability of the data communication process,

  security of the data

  performance by achieving higher throughput and smaller delay times

Categories of Network

Networks are categorized on the basis of their size. The three basic categories of computer networks are:

A. **Local Area Networks (LAN)** is usually limited to a few kilometers 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.

B. **Wide Area Network (WAN)** is made of all the networks in a (geographically) large area. The network in the entire state of Maharashtra could be a WAN

C. **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.

1.3.Internet

1.4.Protocol and Standards

- 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 know the other language.

PROTOCOL

- A Protocol is one of the components of a data communications system. Without protocol communication cannot occur. 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.

- For successful communication to occur, the sender and receiver must agree upon certain rules called protocol.

- **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.

Concept of Standard

- Standards provide guidelines to product manufacturers and vendors to ensure national and international interconnectivity.

- Data communications standards are classified into two categories:

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 an body that is officially recognized.

Standard Organizations in field of Networking

o Standards are created by standards creation committees, forums, and government regulatory agencies.

o**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)

o **Examples of Forums**

1. ATM Forum
2. MPLS Forum
3. Frame Relay Forum

o **Examples of Regulatory Agencies:**

1. Federal Communications Committee (FCC)

DATA REPRESENTATION

Data is collection of raw facts which is processed to deduce information.

There may be different forms in which data may be represented. Some of the forms of data used in communications are as follows:

1. Text

- Text includes combination of alphabets in small case as well as upper case.
- It is stored as a pattern of bits. Prevalent encoding system : ASCII,

Unicode

2. Numbers

- Numbers include combination of digits from 0 to 9.
- It is stored as a pattern of bits. Prevalent encoding system : ASCII, Unicode

3. Images

- ―An image is worth a thousand words‖ is a very famous saying. In computers images are digitally stored.
- A Pixel is the smallest element of an image. To put it in simple terms, a picture or image is a matrix of pixel elements.
- The pixels are represented in the form of bits. Depending upon the type of image (black n white or color) each pixel would require different number of bits to represent the value of a pixel.
- The size of an image depends upon the number of pixels (also called resolution) and the bit pattern used to indicate the value of each pixel.
- Example: if an image is purely black and white (two color) each pixel can be represented by a value either 0 or 1, so an image made up of 10 x 10 pixel elements would require only 100 bits in memory to be stored.
- On the other hand an image that includes gray may require 2 bits to represent every pixel value (00 - black, 01 – dark gray, 10– light gray, 11 –white). So the same 10 x 10 pixel image would now require 200 bits of memory to be stored.
- Commonly used Image formats : jpg, png, bmp, etc

4. Audio

- Data can also be in the form of sound which can be recorded and broadcasted. Example: What we hear on the radio is a source of data or information.
- Audio data is continuous, not discrete.

5. Video

- Video refers to broadcasting of data in form of picture or movie/

1.5.Network Models : OSI Reference Model

In the study of computer networks it is essential to study the way our networks work. Computer networks are operated by network models; most prominently the OSIRM and the TCP/ IP Model. This chapter gives the understanding of the OSI reference model.

Concept Of 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.

i. 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.

ii. 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:

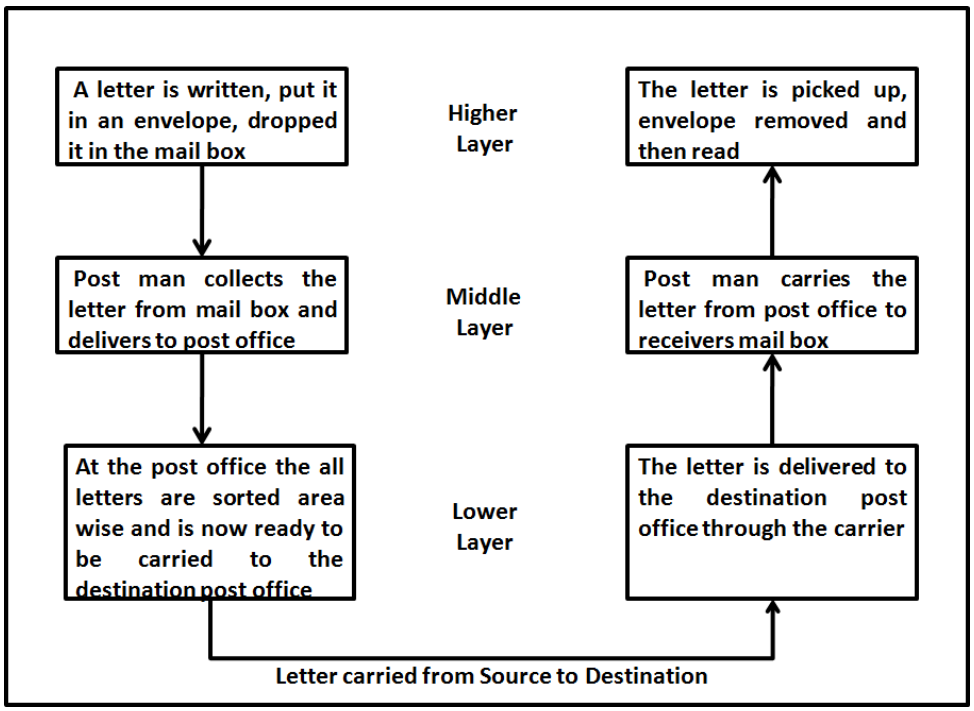


Fig: Concept of layer task: sending a letter

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.

vi. 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.

vii. 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.

OPEN SYSTEMS INTER CONNECTION(OSI) REFERENCE MODEL

Introduction to OSI Model & its layers

- The Open Systems Interconnection (OSI) Model was developed by International Organization for Standardization (ISO).
- ISO is the organization, OSI is the model
- It 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 co- operate 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 has to pass 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.

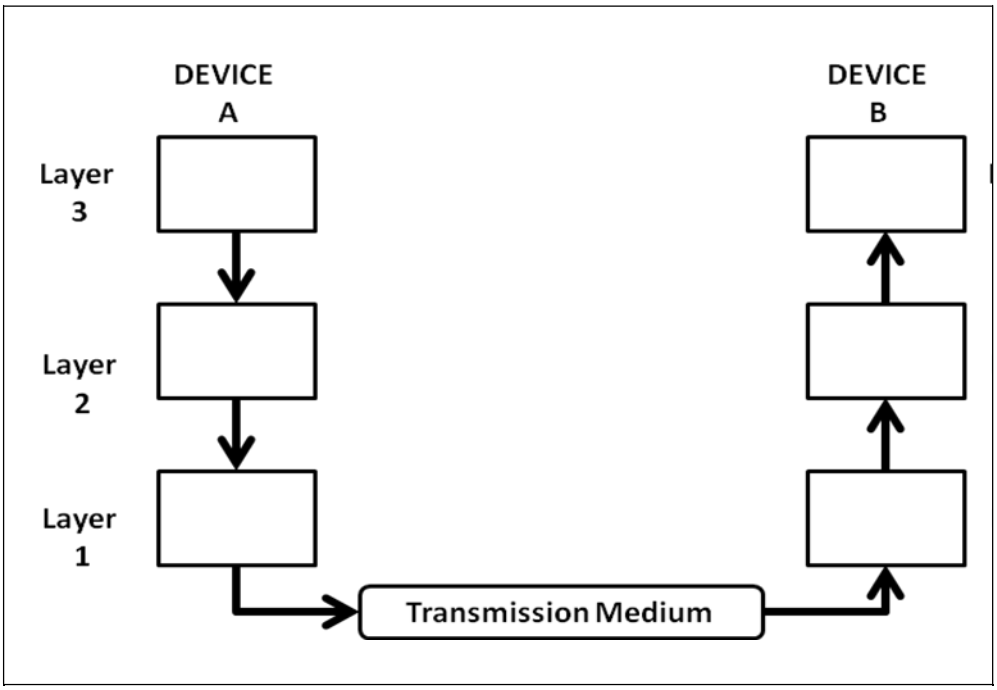


Fig: Flow of Data from Device A to Device B through various layers

- 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.

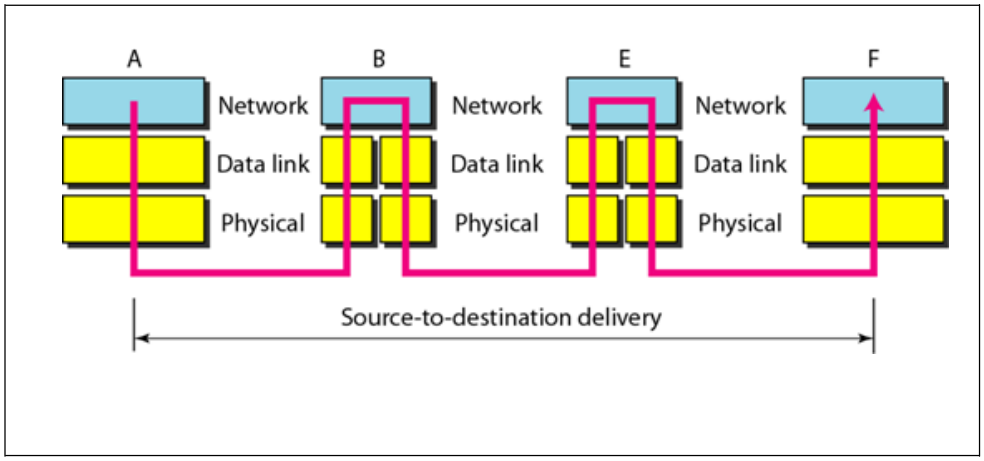


Fig: Data Transfer through Intermediate nodes

- 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 to occur, 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 dedicated function or services and is different from the function of the other layers.

- 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 below

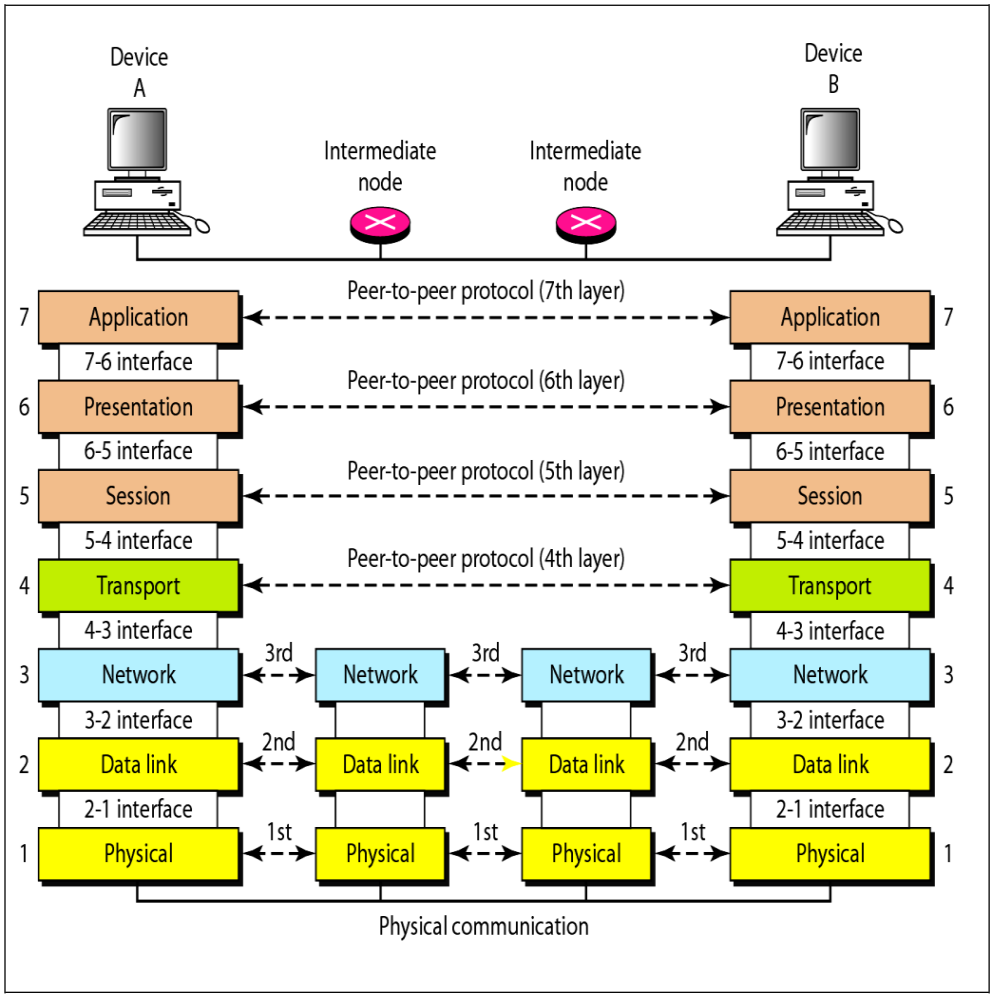


Fig: Communication & Interfaces in the OSI model

Encapsulation of Data

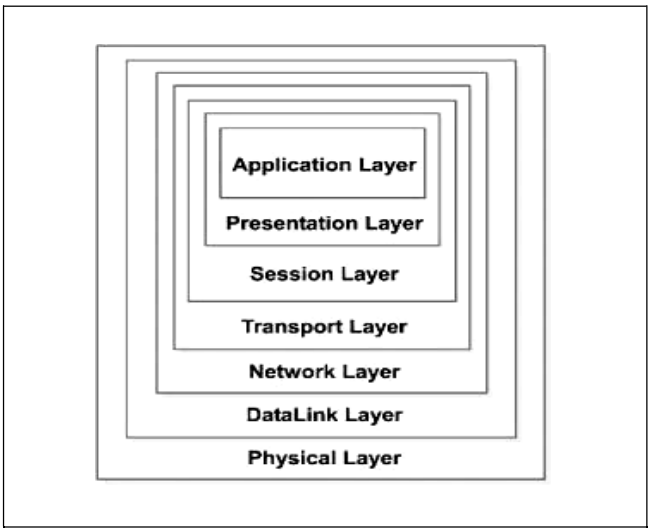


Fig: Encapsulation

- 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

Description of Layers in the OSI Model

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:

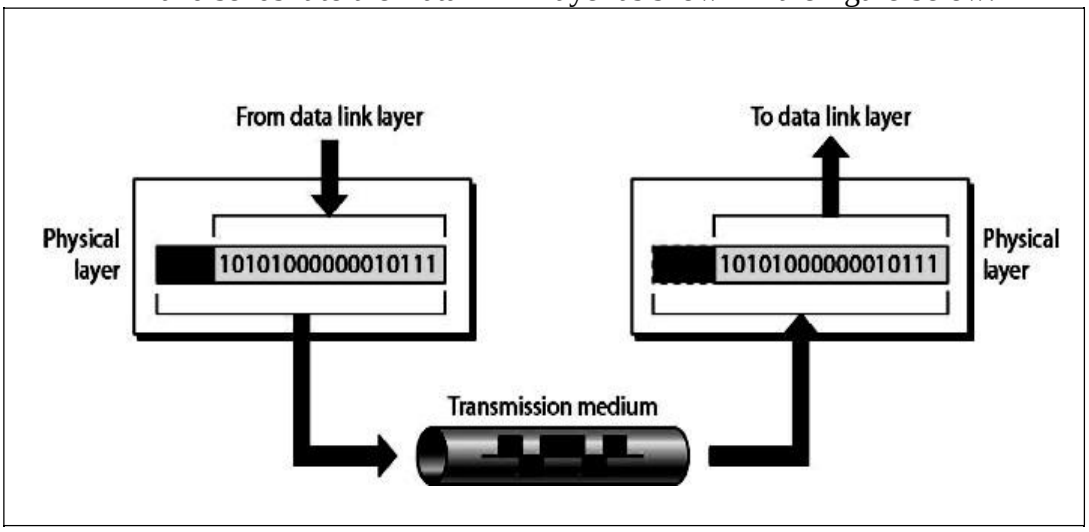


Fig: Transmission of data to and from Physical Layer

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.

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:

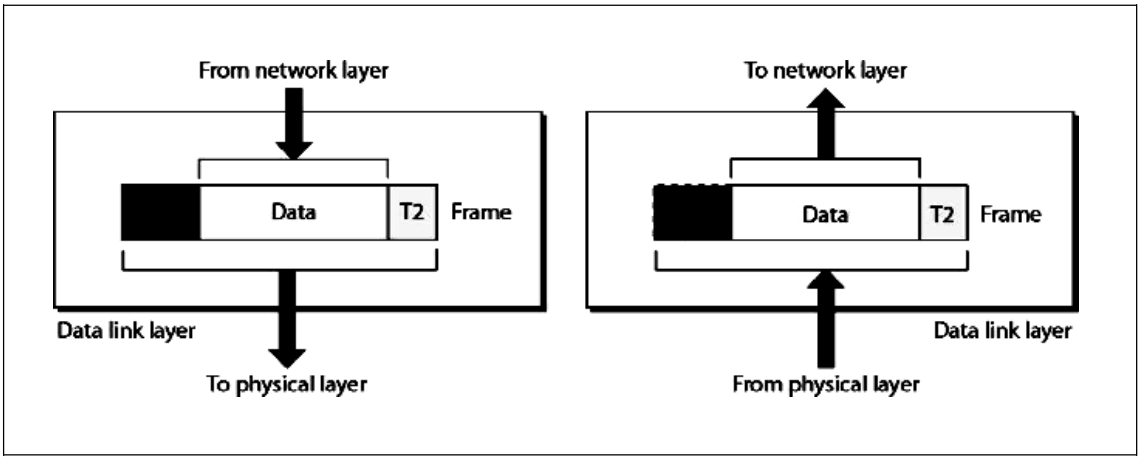


Fig: Data Link Layer: The process of Framing

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.

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.

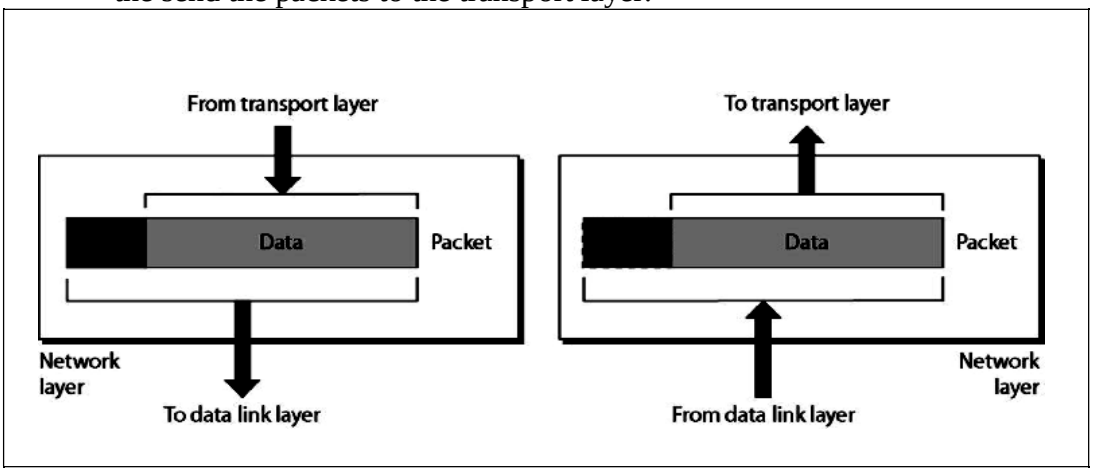


Fig: Network Layer

III. The network layer is responsible for source to destination of delivery of data. Hence it may have to route the data through multiple networks via multiple intermediate devices. In order to achieve this the network layer relies on two things:

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 universally 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 check the IP address in the header, if its own IP address does not match with the IP address of the receiver found in the header, the intermediate node concludes that it is not the final node but an intermediate node and passes the packet to the data link layer where the data is forwarded to the next node.

V. Routing

- **VI.** The network layer divides data into units called packets of equal size and bears 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. The best possible path 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. But the source and the destination both may be having multiple processes communicating with each other. Hence it is important to deliver the data not only from the sender to the receiver but 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.

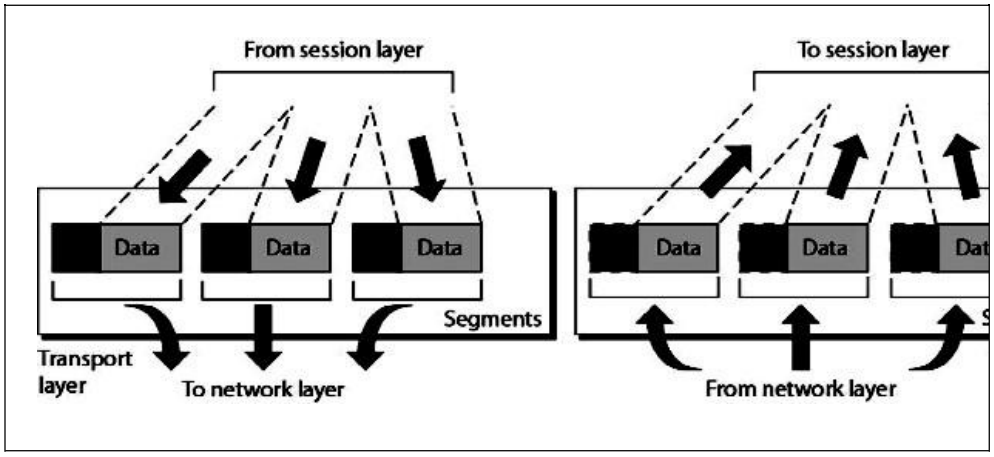


Fig: Transport Layer

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

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

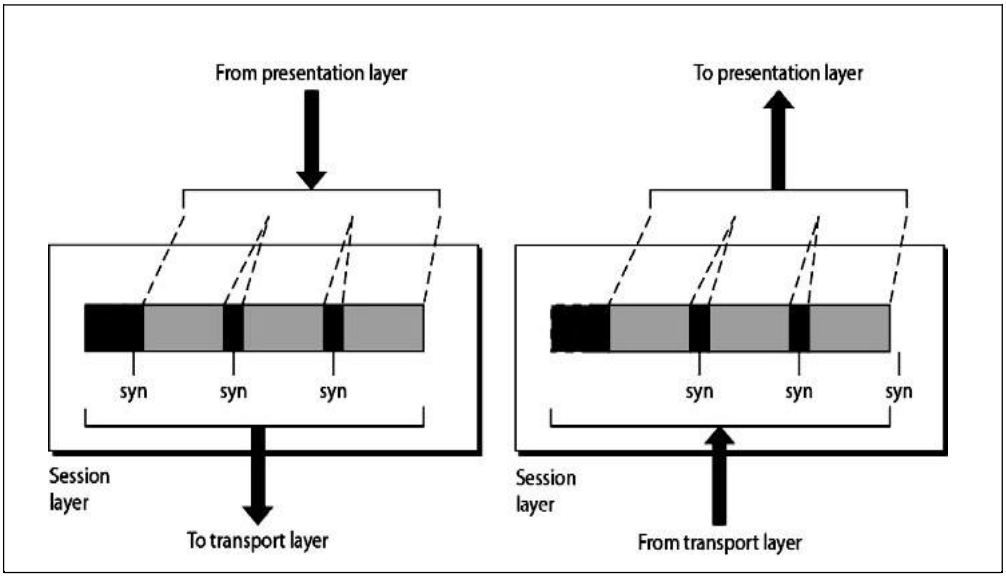
- The main responsibility of the transport layer is process to process delivery of the entire message.

Session Layer

I. The session layer establishes a session between the communicating devices called dialog and synchronizes their interaction. It is the responsibility of the session layer to establish and synchronize the dialogs. It is also called the network dialog 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 synchronizatoin

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.

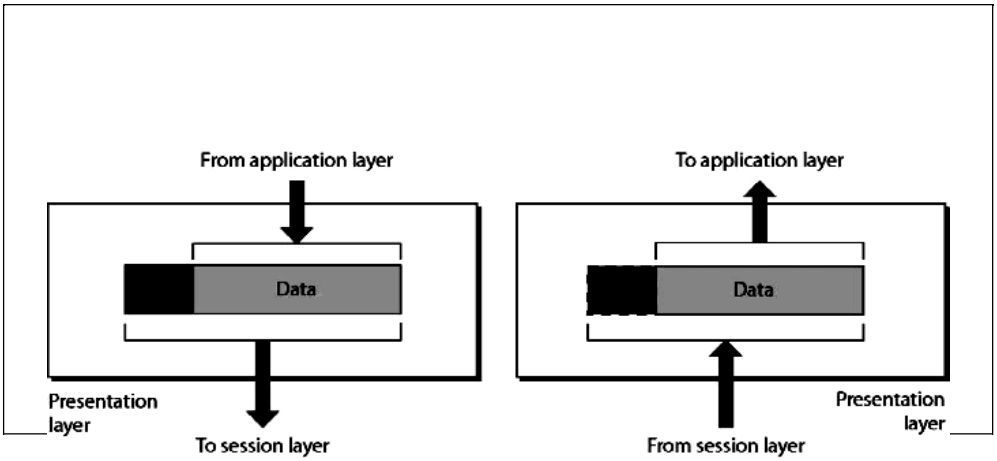


Fig : Presentation Layer

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

IV. Compression

Compression ensures faster data transfer. The data compressed at sender has to be decompressed at the receiving end, both performed by the Presentation layer.

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 original message from the encrypted message.

VI. Main responsibility

The main responsibility of the Presentation layer is translation, compression and encryption.

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.

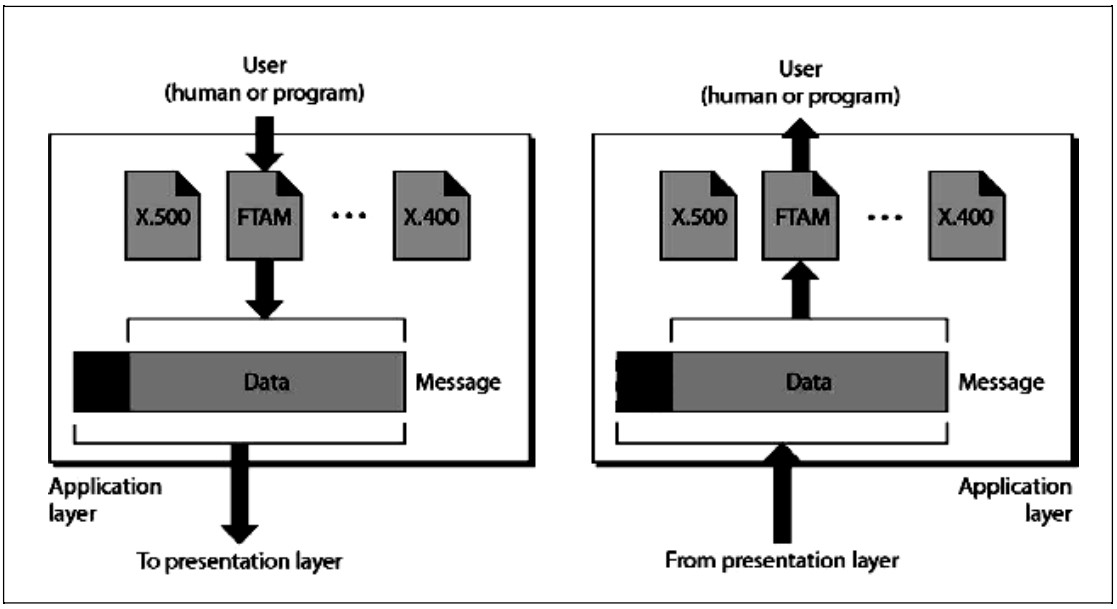


Fig : Application Layer

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.

Point to remember :

1. Application Layer : To provide the users access to network resources
2. Presentation Layer: To provide the functions of translation, encryption and compression.
3. Session Layer: To establish, manage and terminate sessions

4. Transport Layer: To provide process to process delivery of message
5. Network Layer: To provide source to destination delivery of packets.
6. Datalink Layer: To provide hop to hop delivery of frames
7. Physical Layer: To transmit data over a bit stream from one hop to the next and provide electrical and mechanical specification.

1.6.TCP/IP MODEL

After an understand of the concept of layered task and then understanding the OSI model we introduce the TCP/IP model. This model is currently being used on our systems. 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, ie. There are multiple layers and higher layer protocols are supported by lower layer protocols.
  It existed even before the OSI model was developed.
- Originally had four layers (bottom to top):
- 1. Host to Network Layer
  2. Internet Layer
  3. Transport Layer
  4. Application Layer
- The figure for TCP/IP model is as follows:

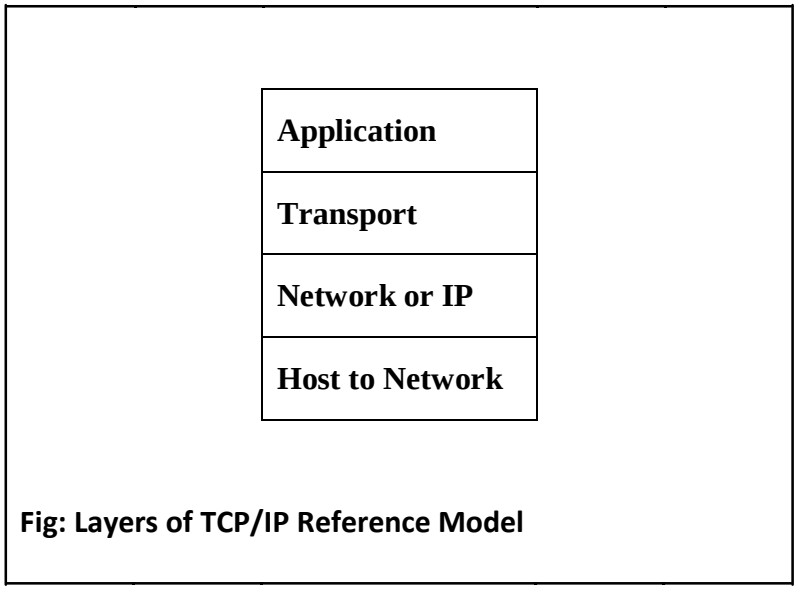


Fig: Layers of TCP/IP Reference Model

- The 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:

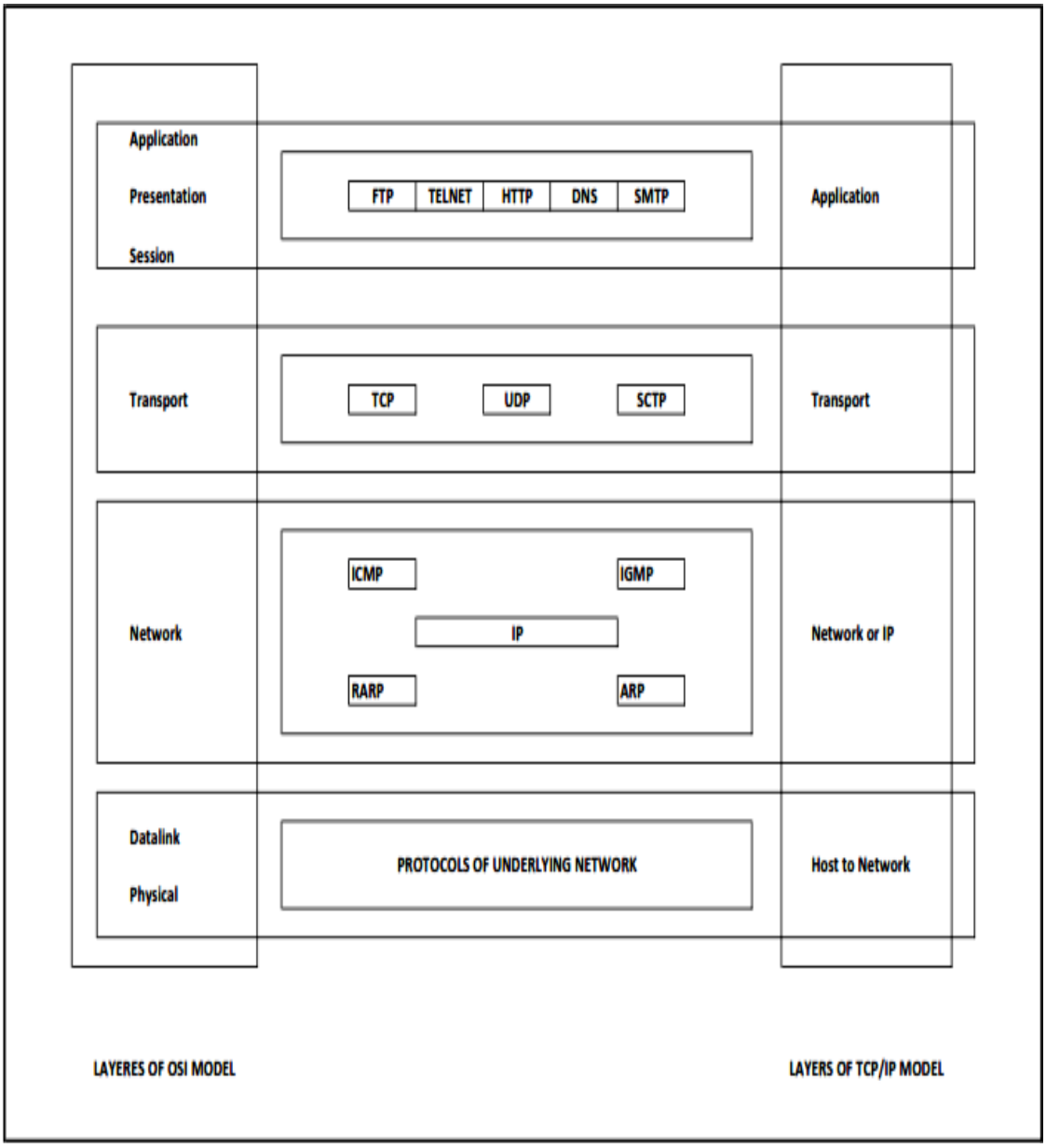


Fig: Comparison of OSI model and TCP/IP model

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 an **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**.

- 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.

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 signaling 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.

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 reliable 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.

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.

1.7.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

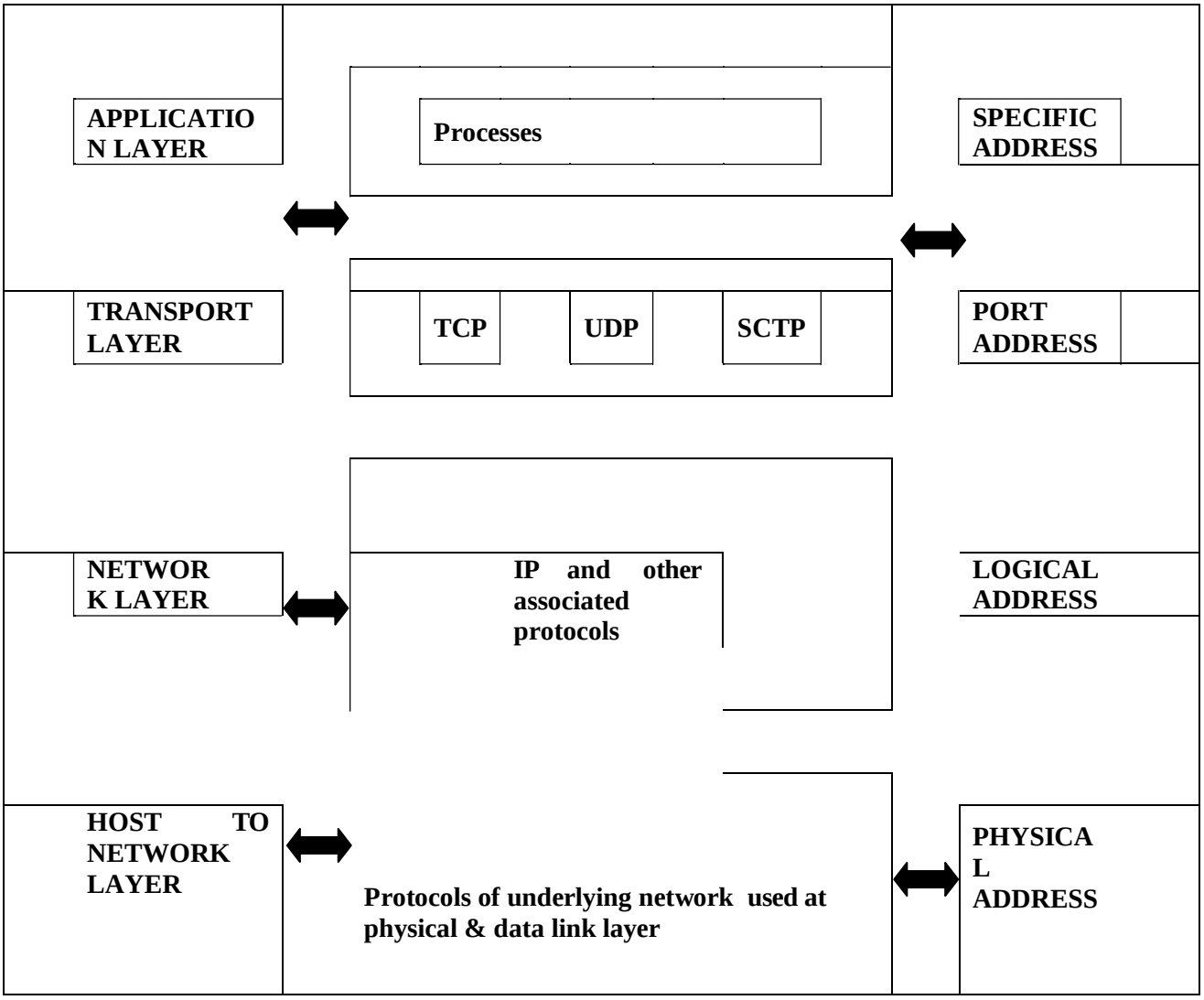


Fig: Addressing in TCP/IP model

Each of these addresses are described below:

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.

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 fiber 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 2^{32} nodes
     b. **IPv6:** 128 bit address, capable of supporting 2^{128} nodes

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

4. Specific Address

i. Port addresses 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.

IP PROTOCOL – IPV4

Packets in the IPv4 format are called datagram. An IP datagram consists of a header part and a text part (payload). The header has a 20-byte fixed part and a variable length optional part. It is transmitted in big-endian order: from left to right, with the high- order bit of the Version field going first.

IPv4 can be explained with the help of following points:

1. IP addresses
2. Address Space
3. Notations used to express IP address
4. Classfull Addressing
5. Subnetting
6. CIDR
7. NAT
8. IPv4 Header Format

IP addresses

- Every host and router on the Internet has an IP address, which encodes its network number and host number.
- The combination is unique: in principle, no two machines on the Internet have the same IP address.
- An IPv4 address is 32 bits long
- They are used in the Source address and Destination address fields of IP packets.
- An IP address does not refer to a host but it refers to a network interface.

Address Space

- An address space is the total number of addresses used by the protocol. If a protocol uses *N* bits to define an address, the address space is 2^N because each bit can have two different values (0 or 1) and *N* bits can have 2^N values.
- IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 (more than 4 billion).

Notations

- There are two notations to show an IPv4 address:
  1. **Binary notation**
     The IPv4 address is displayed as 32 bits.
     ex. 11000001 10000011 00011011 11111111

2. **Dotted decimal notation**
   To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes.

   Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value ranging from 0 to 255.
   Ex. 129.11.11.239

Classful addressing

In classful addressing, the address space is divided into five classes: A, B, C, D, and E.

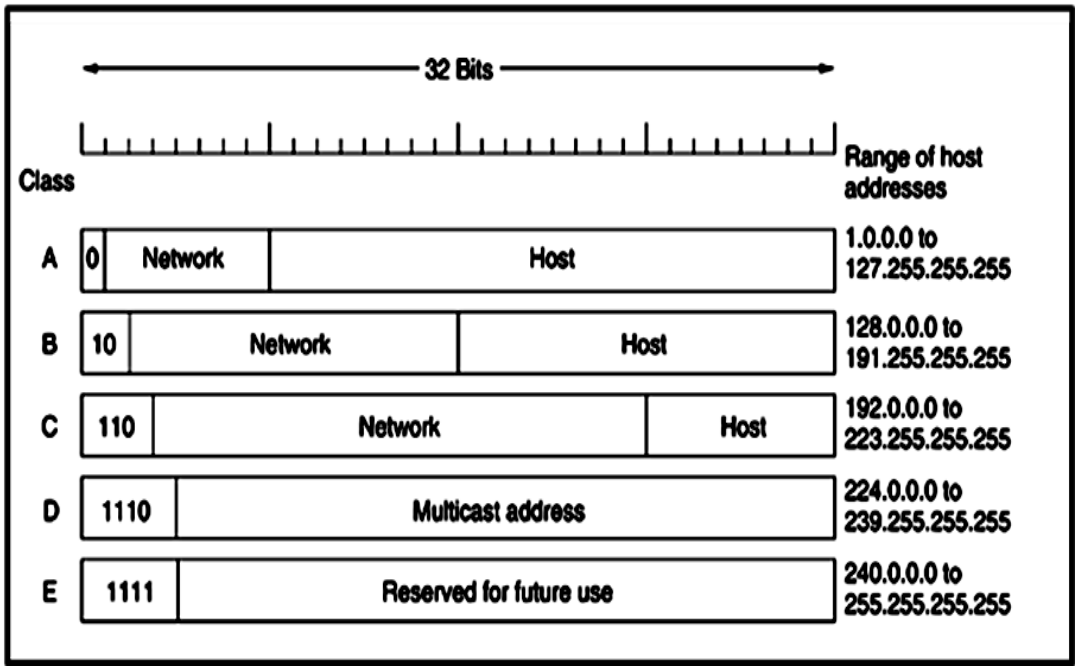


Figure: Classful addressing : IPv4 Netid

and Hostid

- In classful addressing, an IP address in class A, B, or C is divided into netid and hostid.

- These parts are of varying lengths, depending on the class of the address as shown above.

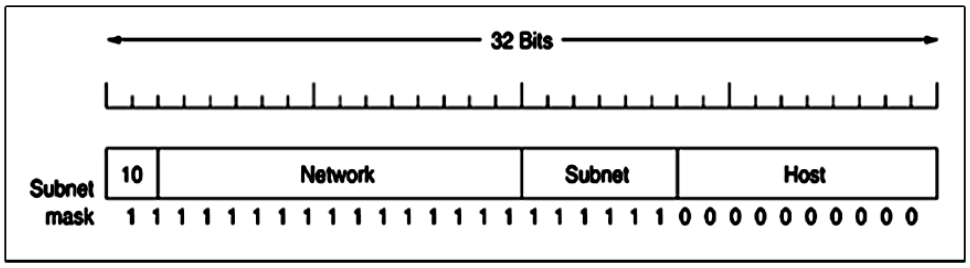
Information on the Number of networks and host in each class is given below:

Class	Number of Networks	Number of Hosts	Application
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

- The IP address 0.0.0.0 is used by hosts when they are being booted.
- All addresses of the form 127.xx.yy.zz are reserved for loopback testing, they are processed locally and treated as incoming packets.

Subnetting

- It allows a network to be split into several parts for internal use but still act like a single network to the outside world.
- To implement subnetting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A‖/22‖ to indicate that the subnet mask is 22 bits long.
- Consider a class B address with 14 bits for the network number and 16 bits for the host number where some bits are taken away from the host number to create a subnet number.



4Fig: A Class B network subnetted into 64 subnets.

- If 6 bits from the host Id are taken for subnet then available bits are :
  14 bits for network + 6 bits for subnet + 10 bits for host
- With 6 bits for subnet the number of possible subnets is 2^6 which is 64.
- With 10 bits for host the number of possible host are 2^{10} which is 1022 (0 & 1 are not available)

CIDR

A class B address is far too large for most organizations and a class C network, with 256 addresses is too small. This leads to granting Class B address to organizations who do not require all the address in the address space wasting most of it.

This is resulting in depletion of Address space.

A solution is CIDR (Classless InterDomain Routing) The basic idea behind CIDR, is to allocate the remaining IP addresses in variable-sized blocks, without regard to the classes.

NAT (Network Address Translation)

- The scarcity of network addresses in IPv4 led to the development of IPv6.

- IPv6 uses a 128 bit address, hence it has 2^{128} addresses in its address space which is larger than 2^{32} addresses provided by IPv4.
- Transition from IPv4 to IPv6 is slowly occurring, but will take years to complete, because of legacy hardware and its incompatibility to process IPv6 address.

- NAT (Network Address Translation) was used to speed up the transition process

- The only rule is that no packets containing these addresses may appear on the Internet itself. The three reserved ranges are:
  10.0.0.0 – 10.255.255.255/8 (16,777,216 hosts)
  172.16.0.0 – 172.31.255.255/12 (1,048,576 hosts)
  192.168.0.0 – 192.168.255.255/16 (65,536 hosts)

- **Operation:**

  Within the Organization, every computer has a unique address of the form 10.x.y.z. However, when a packet leaves the organization, it passes through a NAT box that converts the internal IP source address, 10.x.y.z, to the organizations true IP address, 198.60.42.12 for example.

IP Header

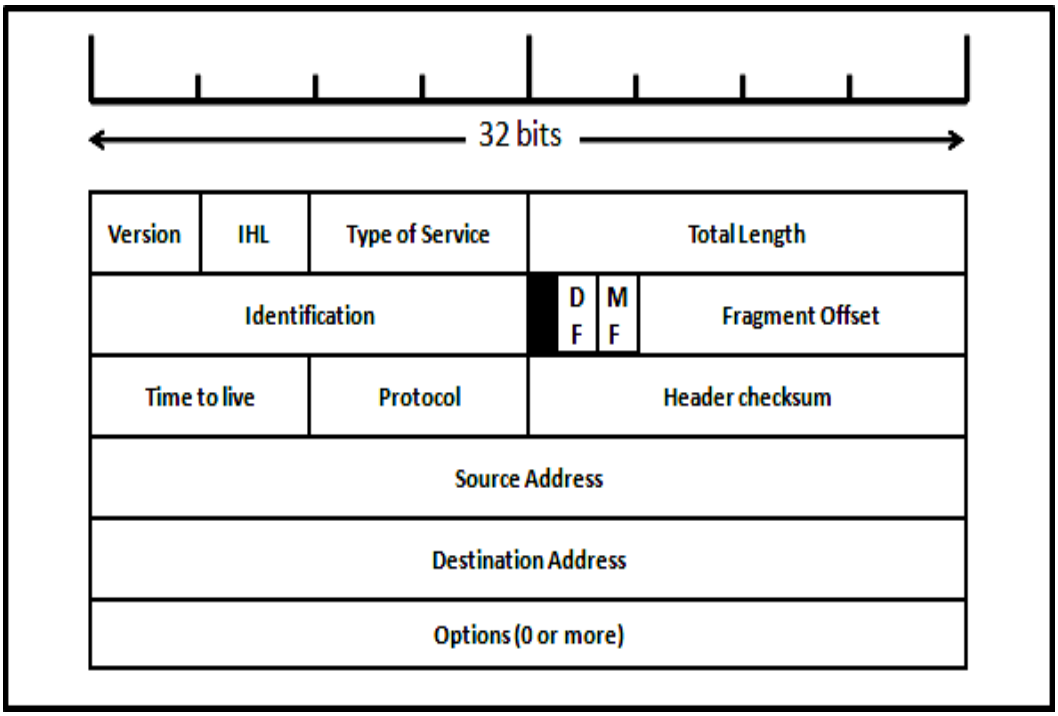


Figure: The IPv4 (Internet Protocol) header

The description of the fields shown in the diagram is as follows:

No	Field Name	Description
1	Version	Keeps track of the version of the protocol the datagram belongs to (IPV4 or IPv6)
2	IHL	Used to indicate the length of the Header. Minimum value is 5 Maximum value 15
3	Type of service	Used to distinguish between different classes of service
4	Total length	It includes everything in the datagram—both header and data. The maximum length is 65,535 bytes
5	Identification	Used to allow the destination host to identify which datagram a newly arrived fragment belongs to. All the fragments of a datagram contain the same Identification value

6	DF	1 bit field. It stands for Don't Fragment. Signals the routers not to fragment the datagram because the destination is incapable of putting the pieces back together again
7	MF	MF stands for More Fragments. All fragments except the last one have this bit set. It is needed to know when all fragments of a datagram have arrived.
8	Fragment offset	Used to determine the position of the fragment in the current datagram.
9	Time to live	It is a counter used to limit packet lifetimes. It must be decremented on each hop. When it hits zero, the packet is discarded and a warning packet is sent back to the source host.
10	Header checksum	It verifies Header for errors.
11	Source address	IP address of the source
12	Destination address	IP address of the destination
13	Options	The options are variable length. Originally, five options were defined: 1. Security : specifies how secret the datagram is 2. Strict source routing : Gives complete path to be followed 3. Loose source routing : Gives a list of routers not to be missed 4. Record route: Makes each router append its IP address 5. Timestamp: Makes each router append its IP address and timestamp

Points remember:

1. TCP/IP has 4 layers: host to network, IP, Transport & Application
2. It uses 4 levels of address: physical, logical, port & specific
3. IP address uniquely identifies a device on the Internet.

REVIEW QUESTIONS

1. Differentiate between data & information. What are the different forms in which data can be represented?
2. What are the characteristics of data communication?
3. What are the components of a data communication system?
4. Define computer network and categorize.
5. Explain protocols in details
6. Explain the concept of layered task.
7. What is the OSI model? List its layers and explain their responsibility in exactly one line.
8. Explain how the communication takes place between layers of OSI model.
9. Write a short note on encapsulation of data in OSI model.
10. Differentiate between the working of Data link layer, Network layer and Transport layer.
11. Explain the structure of TCP/IP protocol
12. Explain in short the functions of every layer of TCP/IP
13. Explain the function of every protocol of the IP layer
14. Explain the concept of IP addresses in detail
15. Why do we use subnetting?
16. What Is NAT? why is it used for?
17. Explain the header of and IPv4 Packet.

REFERENCE & FURTHER READING

Data Communication & Networking – Behrouz Forouzan