1

Introduction to Network Models

Unit structure :

1.0 OBJECTIVES

This chapter will introduce you to the world of computer networking. We will discuss data communication and the role of protocol. The networks of network, Internet is also explained. We will see some standardization committee who standardised the protocols.

Further, we give a general idea of the layers of an OSI and TCP/IP network models and discuss the functions of each.

1.1 COMPUTER NETWORK

1.1.1 Communication Model

- It is an interconnection of autonomous computer systems communicating with each other.
- The necessity of exchanging information between computer systems aroused with the computing era evolution.
- Data communication is the exchange of data between two devices (computers, telephones, satellites) via some transmission medium.

- The data communication model takes the following form:

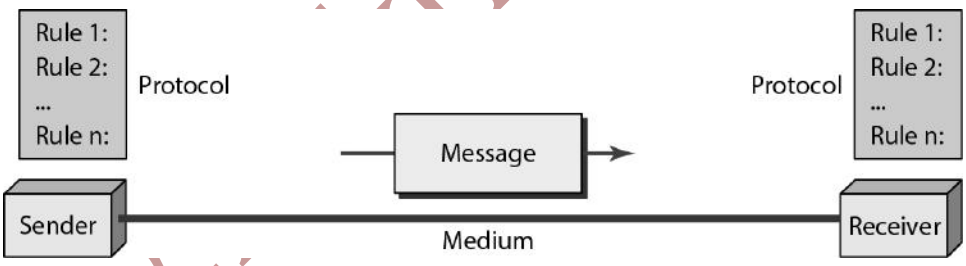


Figure: Five components of data communication

1. **Message.** The message is the information (data) to be communicated.
2. **Sender.** The sender is the device that sends the data message. It can be any electronic device capable to generate and/or send digital data e.g. Computer.
3. **Receiver**. The receiver is the device that receives the message.
   It can be any electronic device capable to generate and/or send digital data e.g. Computer.
4. **Transmission medium.** The physical wired or wireless link that

   destination.
   It include twisted-pair wire, coaxial cable, fibre-optic cable, and radio waves.
5. **Protocol.** A protocol is a set of rules that governs the communications between computers on a network.

These rules include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer.

1.1.2 Transmission Modes / Data Flow.

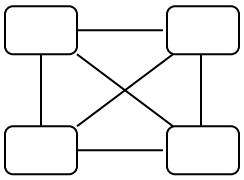
- **Simplex :** One can only send and the other can only receive e.g. T.V Remote.
- **Half Duplex :** Both can send and receive, but not at the same time e.g. Walkie Talkie.
- **Full Duplex :** Both can send and receive at the same time e.g. Telephone.

1.1.3 Types of Connection.

- **Broadcast Link or Multi-link:** When a communication channel is shared among multiple computer systems, it is referred to as a broadcast link. On a broadcast link, messages could be wither broadcasted or multicasted.
- **Broadcasting:** The message is intended to reach all the devices on the multilink or broadcast link.
- **Multicasting:** The message is intended to reach a particular subset of the devices on the multilink or broadcast link.
- **Point-to-Point Link:** The communication channel between two devices is dedicated for the communications between them. This means the two devices exclusively own the communication link.
- **Unicasting:** A message intended for a single receiver is referred to as a unicasted message.

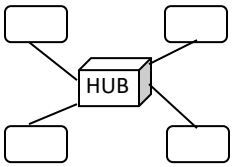
1.1.4 Topology

- The physical or logical way in which the network is laid out is called topology. A peer to peer or primary-secondary relationship is possible among the nodes.
- **Mesh Topology:**
  - Every node connected to every other node
  - Dedicated link between each node
  - n nodes would have n(n-1)/2 links



- Advantages:
  - No traffic problems as dedicated link exists between two nodes
  - Privacy or security
  - Easy fault isolation and correction
- Disadvantages:
  - Heavy amount of cabling
  - Large number of input – output ports

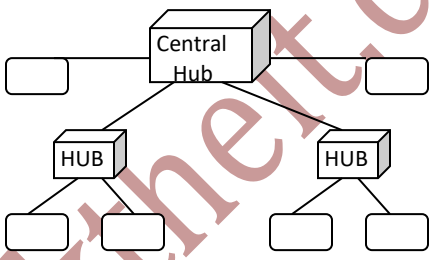
- **Star Topology**:



- Every device has a dedicated link to a central controller called Hub
- No direct communication exists between two devices
- All the communications are via the Hub
- It is less expensive as compared to the Mesh topology
- It is also more robust as the failure of one link would not affect other links
- But the failure of the Hub would lead to a total collapse of the network

➢ **Tree Topology:**

- A variation of the star topology
- All the nodes are either connected to the Central Hub or connected to a Secondary Hub which is in turn connected to the Central Hub



- Secondary hubs are all passive hubs (just meant for the purpose of forwarding)
- The central hub is an active hub (meant for regenerating the signals transmitted through it)
- Advantages and disadvantages are similar to the star topology
- The signals can travel to greater distances due to the presence of the active hub in between
- The network can be prioritized and hence isolated into smaller sub networks

➢ **Bus Topology:**

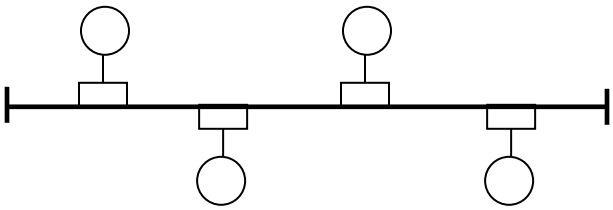
- It is classified as a multipoint topology
- It contains a long cable called the backbone connected to different nodes via taps
- The number of nodes in a bus topology are limited
- The signal becomes weaker as it travels farther away from the originator

➢ Advantages:

- Easy for installation

➢ Disadvantages:

- Difficult to reconfigure
- Prone to traffic problems
- A break in the backbone would lead to the corruption of the entire network
- Difficult for fault isolation



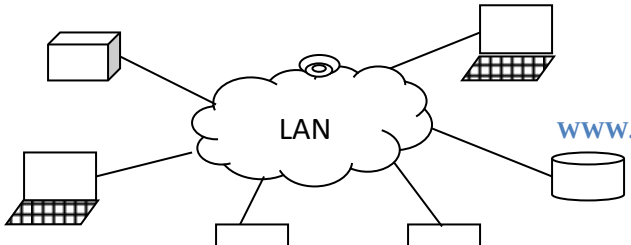
- **Ring Topology:**
  - Every node connected point to point to two other nodes
  - The signals in a ring topology are usually unidirectional
  - Every device contains a repeater that forwards the message to the next device in the ring
  - It is easy to install and configure
  - Fault isolation is also easy

- **Note:** Ring & Mesh topologies follow peer-to-peer architecture, whereas Star & Tree topology follow secondary-primary architecture. Bus topology follows both the architectures.

1.2 NETWORK CATEGORIES

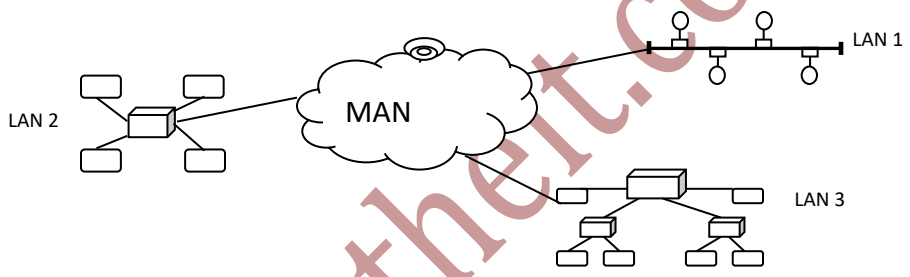
1.2.1 LAN (Local Area Network)

- A privately own network which is restricted to a single building or campus within a few kilometer range.
- The main purpose of LAN is to share resources.
- These resources may include data, printers, database etc. Since the bonds of LAN are known in advance, it is easier to set it up.
- The transmission technology used in LAN is made up of cable connecting devices Traditional LAN offers speed 10Mbps to 100Mbps connections. Recent LAN may operate up to 100Gbps. The topology for LAN is usually Bus or Ring.
- The following are some uses of LAN:
  1] Sharing data
  2] Sharing peripherals
  3] Sharing application
  4] Electronic messaging
  5] Client Server application



1.2.2 MAN (Metropolitan Area Network)

- It usually spans an entire city.
- The best example of MAN is cable T.V. network.
- A MAN can also be considered to be a collection of a number of LAN's to form a large network. E.g. A Company may connect all its LAN offices in a city using MAN.
- It may be wholly owned and operated by a private company or it may be a service provided by a public company (like telephone service).



1.2.3 WAN (Wide Area Network)

- It spans over a large geographical region.
- Area may be country or continent.
- It provides transmission of data, voice, images, video and other form of information.
- WAN may be comprising of public, private or leased devices. Logically speaking the WAN may be looked as a host connected by subnet.
- A subnet is a sub network comprising of various interconnecting devices like router, gateways etc.

1.3 THE INTERNET

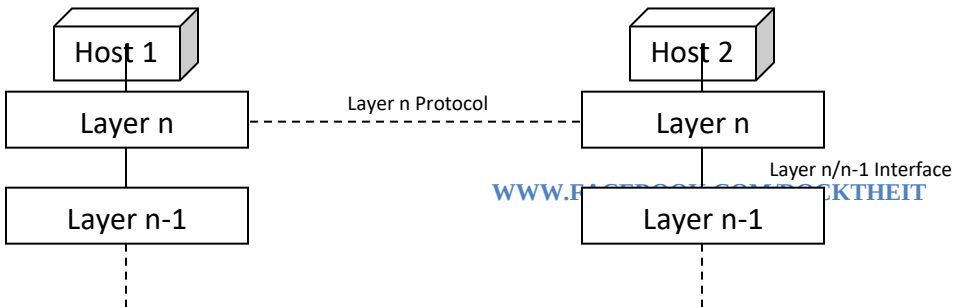
- The Internet is a global system of interconnected computer networks .
- It uses the standard Internet protocol suite ,often called TCP/IP to serve billions of users worldwide.
- It is a *network of networks* .
- End users who want Internet connection use the services of Internet service providers (ISPs).
- There are international service providers, national service providers, regional service providers, and local service providers.

1.4 INTRANET

- **Intranet** is the general term for a collection of private computer networks within an organization.
- An intranet uses network technologies to connect the computational devices within the organization.
- Intranets utilize standard network hardware and software technologies like Ethernet, WiFi,TCP/IP, Web browsers and Web servers.

1.5 PROTOCOL

- Computer network hardware came into existence first and then corresponding software were designed to fit the hardware.
- In order to simplify the network design network software is organized into levels or layers.
- Interrelated and similar functions are grouped and added to a particular layer.
- Protocol is a set of rules that govern the way two parties communicate with each other.
- When a particular layer 'n' communicates with another layer 'n' of another machine, the communication follows a set of rules or conventions collectively called as layer 'n' protocol.
- Entities at corresponding layers of different machines are referred to as peers.
- It is the peers that communicate using a protocol.



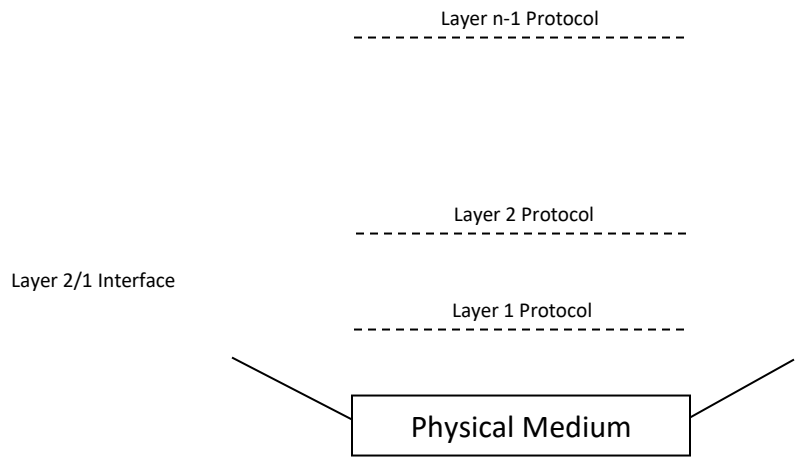
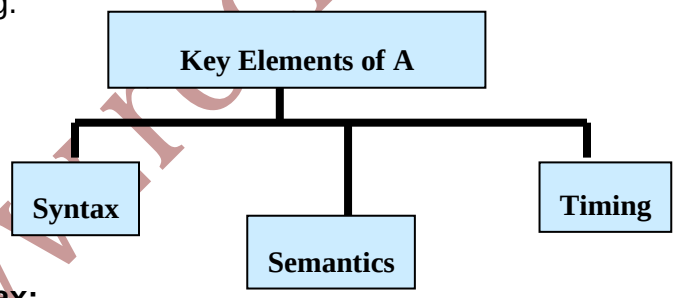


Figure 1.2 Layered Architecture

- Between every layer there is an interface that defines the operations and services the lower layer makes available to the upper one.
- Each layer passes data to the layer below it until the lowest layer is reached.
- Transmission actually occurs at the physical medium.
- This set of layers and protocols make up the network architecture.
- The set of protocols in the network architecture make up the protocol stack.
- The key elements of a protocol are syntax, semantics and timing.



- **Syntax:**
  - The Structure or format of data
  - What is communicated!
- **Semantics:**
  - The Meaning of each section of bits
  - How it is communicated !!
- **Timing:**
  - When should the data be send
  - When it is communicated !!!

1.6 REFERENCE MODELS

1.6.1 OSI MODEL

- OSI (Open System Interconnection)

- It was developed by ISO.
- It is a model that allows any two different systems to communicate regardless of their underlining architecture.
- OSI aims to allow unrelated systems to communicate without changing the underlying hardware or software.
- The OSI model is not a protocol.
- It is just a reference model for developing new protocols.
- It is a layered architecture for designing network system.
- It is made up of 7 layers.
- The reason for layering this model where as follows:
  - For every different abstraction a layer is needed.
  - Each layer performs a well defined function.
  - International standard protocols should be kept in mind while defining function of each layer.
  - Layer boundaries to be chosen to minimize the information flow across the interface.
  - Number of layers should be large enough so that distinct function are not thrown together.
- Communications happening between a layer x at the source and destination are referred to as peer communications and are governed by protocols.
- These processes are referred to as peer to peer processes. Actually speaking direct communication exits only at the physical layer.
- At machine A, message flows down from the top layer to the bottom. A header and trailer gets added at layer 6, 5, 4, 3, 2.
- A trailer is added at layer 2. Between each layer an interface allows the information to be sent to & fro among the two layers.
- This interface defines the information and services a layer must provide the layer above it.

Application	layer 7
Presentation	layer 6
Session	layer 5
Transport	layer 4
Network	layer 3
Data link	layer 2
Physical	layer 1

Figure 1.3 The OSI Model

- ***Organization***:
  - Layer 1, 2, 3 are the network support layers that deal with the physical aspects of moving data from one level to another.
  - Layer 1, 6, 7 are the user support layers that allow interoperability among unrelated software systems.
  - Layer 4 ensures end to end reliable data transmission.

- Upper layers (5, 6, and 7) are implemented in software.
- Lower layers (1, 2, 3) are implemented in hardware and software.
- Except layer 1 which is total hardware.

➢ ***Functions of layers:***

➢ ***Physical layer:*** Deals with the mechanical and electrical specifications of the interface and medium.
  ➢ Performs functions required to transmit a bit stream over a physical medium.
  ➢ **Functions**:
    - **Physical characteristics of interface and medium**: It defines the physical and mechanical characteristics of the medium
    - **Representation of bits:** Physical layer contains a bit stream that needs to be transmitted after encoding them to signals.
    - **Data Rate:** (Transmission rate)
    - **Synchronization of bits**
    - **Line configuration of bits:** (Point to point, Multipoint)
    - **Physical topology:** (LAN, MAN, WAN)
    - **Transmission mode:** (simplex, half duplex, duplex)

➢ ***Data link layer:*** Responsible for reliable link & node to node delivery
➢ **Functions:**
    - **Framing:** Divides stream of bits into manageable frames.
    - **Physical addressing:** A header containing the physical address of the sender (SA) and the receiver (DA) is added to the frame
    - **Flow control:** The rate at which the data is send and received may not match
    - **Error control:** Detect and rectify the error
    - **Access control:** Two or more devices connected to some link. So managing access to the link

➢ ***Network layer:*** Responsible for source to destination delivery of packets possibly across multiple network links.
 If two machines are on the same network then there is no need for the network layer.
 But if machines are across different networks then there is a requirement for network layer.
➢ **Functions:**
    - **Logical addressing:** If a packet is transmitted across networks then a header containing the network addition or logical addressing of Source and destination is added

- **Routing:** Internetworking device that routes a packet across networks

- ***Transport layer:*** Responsible for source to destination delivery of the entire message.
- The network layer treats each packet of the message independently, but the transport layer sees that the whole message gets transmitted reliably.
- It is responsible for setting up a connection between two ports.
- **Functions:**
  - **Service Point Addressing:** Delivery not from one machine to another, but also from specific process to another. Service point addressing or port addressing contains the information or address of which process is sending and receiving the packet
  - **Segmentation and Reassembly:** Message divided into segments with each segment containing the sequence number. Hence at destination proper reassembly of the segments take place.
  - **Flow Control :** Transport layer controls the application sending rate
    • To match the rate at which network layer can deliver data – *congestion control*
    • To match the rate at which receiving application can process the data – *flow control*
    • Must be performed end-to-end, since only end points know characteristics of entire path
  - **Error Control:** It is at this layer that, should a packet fail to arrive (perhaps due to misrouting, or because it was dropped by a busy router), it will be retransmitted, when the sending party fails to receive an acknowledgement from the device with which it is communicating.
  -

- ***Session Layer:*** Also called the network dialog controller
- **Functions:**
  - **Dialog control** : There are three forms of dialog.
    - Simplex Dialogs - One way transfers, similar to an old computer/printer. Data could be sent to the printer but the printer could not communicate back.
    - Half-Duplex Dialogs - Two-way transfers. Each device must take their turn. Both cannot transfer at the same time.
    - Full-Duplex Dialogs - Two-way simultaneous data transfers. Each device has it's own channel. Telephones are full duplex, as are most modems. Full duplex is the most expensive to implement.

- **Synchronization:** Adding check point, synchronizing points for acknowledgement.
  - Consider the problems that might occur when trying to do a two-hour file transfer between two machines on a network with a 1 hour mean time between crashes. After each transfer was aborted, the whole transfer would have to start over again, and would probably fail again with the next network crash. To eliminate this problem, the session layer provides a way to insert checkpoints into the data stream, so that after a crash, only the data after the last checkpoint has to be repeated.

➢ ***Presentation layer:*** Concerned with syntax and semantics of info between two systems translation, encryption and compression.

- **Translation**: There are four forms of data translation.
- They are:
- **Bit Order** - Bit Order refers to a binary number (1110011). The two conversing devices must agree on the order of the bits being transferred.
- **Byte Order Translation** - Similar to Bit Order, and number larger than 1 byte (8 bits) must be represented by several bytes.

- **Character Code Translation** - Most computers use one of three binary numbering systems to represent
- character sets. They are:

  ASCII - American Standard Code for Information Interchange, representing.

  EBCDIC - Extended Binary Coded Decimal Interchange Code, represents English on IBM mainframes.
- **File Syntax Translation** - Converting file formats to another, when transferring to a different system.

- **Encryption**: Encryption is basically scrambling the data before transmission, and then unscrambling it upon receiving it. This is done with a *key* that describes how the message was scrambled. This is done to prevent messages from being intercepted and read by unwanted parties.
- **Compression**: The presentation layer is also concerned with other aspects of information representation. For example, data compression can be used here to reduce the number of bits that have to be transmitted and cryptography is frequently required for privacy and authentication.

- ***Application layer:*** Enables users, (humans or s/w) to access the network.
- Provides interface for services like e-mails, remote file access, shared data base management etc.
    - **Network virtual Terminal:** (remote logins)
    - **FTAM:** (File, transfer and management)
    - **Mail:** directory services

1.6.2 TCP/IP Reference Model

- The TCP/IP protocol suite is used in internet was developed prior to OSI.
- The layers in Transmission Control Protocol/Internet Protocol (TCP/IP) do not exactly match the OSI layers.
- OSI contains the description of the function and is not tied to any particular set of protocols.
- TCP/IP on the other hand is made up of a fixed set of protocols.
- The ARPANET sponsored by DoD led to the beginning of internet which led to the development of TCP/IP.

Application	layer 7	Application
Presentation	layer 6	
Session	layer 5	
Transport	layer 4	Transport
Network	layer 3	Internet
Data link	layer 2	Data link
Physical	layer 1	Physical

OSI MODEL TCP/IP MODEL

- The five layers in TCP/IP suite are:
- **Internet layer:**
    - The requirement for a flexible architecture gave rise to a connectionless internet layer. IP is the main protocol.
    - Packets here travel independently towards the destination.
    - They arrive in different order.
    - They may not reach at all.
    - Hence it is an unreliable and best effort protocol.

- **Transport layer:**
    - At transport layer TCP and UDP are the two major protocols for end-to-end delivery of message.
    - TCP is a reliable connection oriented protocol.
    - It fragments one incoming message into segments, adds sequence number and reassembles them at the destination.

- UDP is an unreliable, connectionless protocol for applications that do not require TCP sequencing or flow control.

SMTP, TELNET, FTP, DNS, HTTP etc.	Application layer
TCP, UDP	Transport layer
ICMP, IGMP, IP, ARP, RARP	Internet layer
Protocols defined by underlying network	Data Link layer

Figure 1.4 The TCP/IP Suite

- **Application layer:**
- TCP/IP suite has no session or presentation layers.
- Application layer contains all higher level protocols.
- **ARP (Address Resolution Protocol):**
  The ARP protocol is used to get the physical address from the IP/logical address.

- **RARP (Reverse Address Resolution Protocol):**
  The RARP protocol is used to get the IP/logical address from the physical address.

- **ICMP (Internet Control Message Protocol):**
  It is used by hosts and routers to send notifications of datagram problems back to sender. As IP is unreliable, this is required.
  Its sole function is to report problems and not correct them.

- **IGMP (Internet Group Message Protocol):**
  It is used to help a multicast router to identify the hosts in a LAN that are members of a multicast group.

- **DNS (Domain Name System):**
  A system that maps English like domain names to the IP addresses and vice versa

- **TELNET:**
  It is used for remote logins

- **FTP (File Transfer Protocol):**
  It is used for transferring files from one node to another

- **SMTP (Simple Mail Transfer Protocol):**
  It is used for sending and receiving electronic messages across a network.
  It is made up of a User Agent (UA) and a Mail Transfer Agent (MTA).

Comparision

OSI Model	*TCP/IP Protocol Suite*
OSI model has 3 imp concept: - Service: Tells what the layer does. - Interface: Tells a process how to access a service - Protocol: how the layer does the service	This model does not distinguish between service, interface and protocol.
OSI model is a very general and hence is adaptable to any protocol as technology changes.	The TCP/IP model is not flexible in that case.
Since it was very general, designers did not have knowledge about which service to put together.	Designer knows which service is fitted where.
The model came first and protocols were fitted into it later.	The protocol came first and then TCP/IP model was introduced

1.7 ADDRESSING

- Four levels of addresses are used in an internet employing the *TCP/IP* protocols:
  - Physical (link) addresses
  - Logical (IP) addresses
  - Port addresses
  - Specific addresses

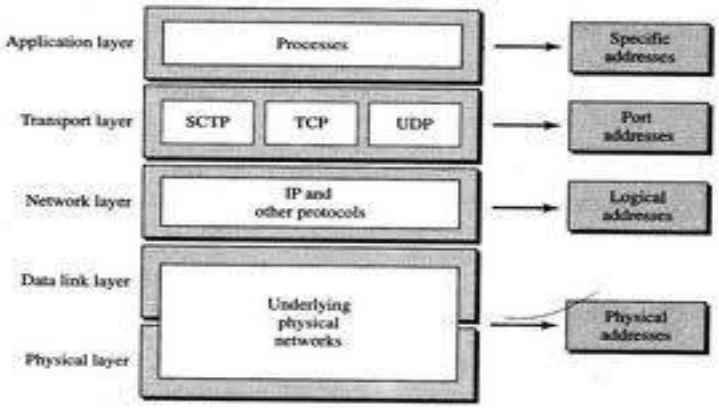


Figure 1.5 Layers and addresses relationship

1.7.1 Physical Addresses

- The physical address is the address of the machine defined by its LAN or WAN.
- This is unique for each system and cannot be changed.
- Physical address is a synonym of MAC address.
- The address is included in the data link layer frames.
- It is the lowest-level address.
- The underlying network decides the size and the format of these addresses.
- For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC).

1.7.2 Logical Addresses

- Logical addresses are created and used by Network layer protocols such as IP or IPX.
- The Network layer protocol translates logical addresses to MAC addresses.
- Logical addresses have a true global significance.
- They uniquely identify hosts within all interconnected network segments.
- TCP/IP uses IP addresses as the logical addressing method.
- A IP address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet.
- No hosts on the Internet can have the same IP address.

1.7.3 Port Addresses

- Computers run multiple processes at a given time.
- To each message in TCP/IP identify its process; every process is given a unique address.
- This address is port number
- The TCP layer requires what is called a port number to be assigned to each message.
- This way it can determine the type of service being provided.
- Ports are reference numbers used to define a service.
- For instance, port 23 is used for telnet services, and HTTP uses port 80 for providing web browsing service.
- There is a group called the IANA (Internet Assigned Numbers Authority) that controls the assigning of ports for specific services.
- There are some ports that are assigned, some reserved and many unassigned which may be utilized by application programs.
- Port numbers can be range up to a value of 65535.
- A port address in TCP/IP is 16 bits in length.

1.7.4 Specific Addresses

- Some applications have user-friendly addresses that are designed for that specific address.

- It's difficult to remember n numbers of alpha-numeric addresses.
- Hence user friendly names can be used.
- These specific names are mapped to the real addresses.
- Example: www.mu.ac.in is a specific address to find the document on World Wide Web.

1.8 SUMMARY

- The 5 components of communication models are Message, Sender, Receiver, Transmission medium and Protocol
- The 3 transmission modes are Simplex, Half Duplex and Full Duplex.
- The network links can be Broadcast, Multicast or Unicast.
- All the nodes in Mesh topology are directly connected to each other.
- Star topology has a central hub to which all the nodes are connected.
- Bus topology is a multipoint topology having common bus.
- Ring & Mesh topologies follow peer-to-peer architecture, whereas Star & Tree topology follow secondary-primary architecture. Bus topology follows both the architectures.
- Networks can be categorize on the basis of their sizes, LAN, MAN and WAN,
- Intranet is inter connection of computers of a organization using TCP/IP protocol.
- The Internet is network of networks, also called as World Wide Web.
- The internet is a public network whereas intranet is private network.
- Protocol is a set of instructions defining the procedure of communication.
- Hence we can state that protocol is a program at each layer which describes the function of the layer.
- Physical layer is responsible for transmitting bit stream over the physical medium.
- Datalink layer maintains end to end delivery and reliability.
- Network layer ensures the routing of data through the network.
- Application layer includes all the network based applications.
- Except Physical address rest all the addresses are virtual addresses which changes with the network architecture.

1.8 UNIT END EXERCISE

1. Describe the five components of data communication

model.

2. List the four basic network topology and their advantages.
3. Why are protocol needed?
4. What are the different types of transmission modes?
5. Write short note on network categories.
6. Distinguish between Internet and Intranet.
7. List the functions of physical layer.
8. Write short note on TCP/IP reference model.
9. Which layers in the Internet model are network supports? Layers?
10. List the addresses and their functions at the various Layers of Internet reference model.

1.10 FURTHER READING / Acknowledgement

1. Data Communication & Networking by Behrouz. A Forouzan, IV Edition, Tata McGraw-Hill.

❖❖❖❖