

# Computer Networks

## EG 3101 CT

**Year: III**  
**Semester: V**

**Total: 6 hour /week**  
**Lecture: 3 hours/week**  
**Practical: 3 hours/week**

### Course Description:

This course deals with fundamentals of computer network, its architecture, its standards, protocols and security issues used in computer network.

### Course Objectives:

After completing this course the students will be able to:

1. Introduce the architecture of computer network
2. Explain various hardware devices and software used in computer networks
3. Setup small home/office network
4. Make secure computer network

### Course Contents:

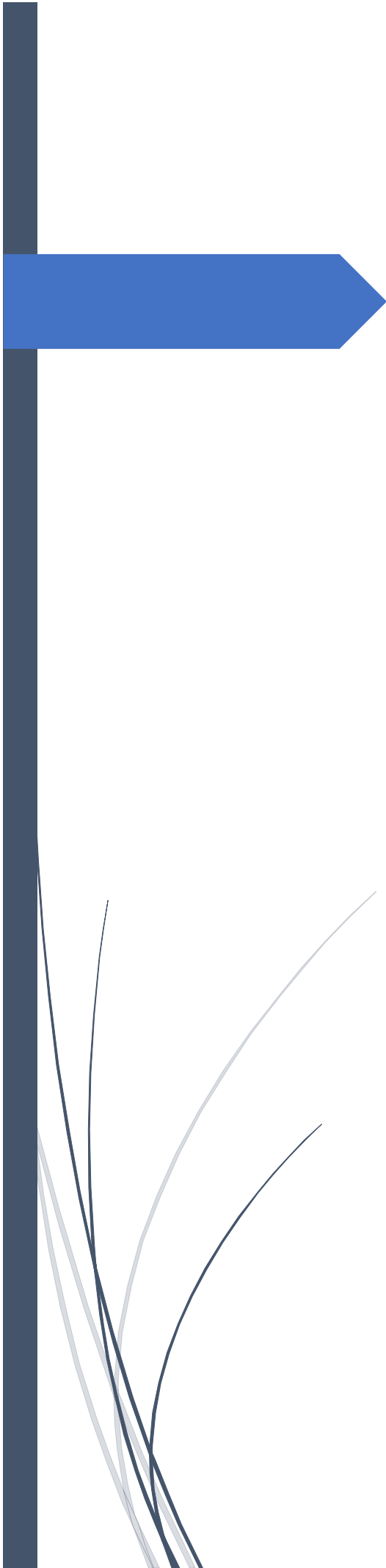
Unit	Topics	Contents	Hours	Methods/ Media	Marks
1	<b>Introduction to computer network:</b>	1.1 Introductory concept of computer network 1.2 Features of computer network 1.3 Classification of computer network 1.4 Introduction of networking 1.5 Concept of internet 1.6 Application and challenging issues of computer network	5hrs		
2	<b>Network architecture:</b>	2.1 Network types:[ LAN, MAN, WAN, CAN, SAN, PAN] 2.2 OSI Reference model 2.3 TCP/IP Reference model 2.4 Network protocols, interfaces, services	5hrs		
3	<b>Hardware and Software for Computer Network:</b>	3.1 Concept of hardware and software for networking 3.2 Network devices:[ Repeater, Hub, NIC, Bridge, Switch, Router, Gateway]	6hrs		

Unit	Topics	Contents	Hours	Methods/ Media	Marks
		3.3 Client- server and peer to peer model 3.4 Connection versus connectionless services			
4	<b>LAN architecture and standards:</b>	4.1 Introduction to LAN standards and architecture 4.2 Media access control 4.3 MAC address 4.4 CSMA/CD 4.5 Token ring, Token bus 4.6 IEEE 802.3, 802.4, 802.5 4.7 Introduction to wireless LAN, Bluetooth, Wi-Fi, Wi-Max	3 hrs		
5	<b>Physical layer and data layer:</b>	5.1 Introduction to physical layer 5.2 line coding formats 5.3 Channel bandwidth 5.4 propagation and transmission time 5.5 Introduction to data link layer and its issues 5.6 Flow and error control issues at data link layer 5.7 Data link layer protocols[ HDLC, PPP]	7hrs		
6	<b>Network Layer:</b>	6.1 Internetworking 6.2 Addressing issues,IP address 6.3 Different classes 6.4 Private and Public address 6.5 Subnet mask and Subnetting 6.6 Classless addressing; 6.7 Routing type and its necessity 6.8 Introduction to IPv4, IPv6 and its necessity	7hrs		
7	<b>Transport and Application layer</b>	7.1 Transport layer issues[ Congestion control, Flow control, Quality of service] 7.2 Transport layer protocols[TCP, UDP] 7.3 Application layer and its function	7hrs		

Unit	Topics	Contents	Hours	Methods/ Media	Marks
		7.4 Electronic mail: SMTP, File transfer: FTP 7.5 protocols [DHCP, DNS, HTTP, WWW]			
8	<b>Computer Network security:</b>	8.1 Security concept [Confidentiality, Integrity and Availability] Digital signature 8.2 Cryptography and key management 8.3 Firewalls 8.4 Virtual private network, 8.5 Wireless security threats and mitigation	5hrs		
9	<b>Case study:</b> Visit related organization visit to study existing network system and prepare a REPORT.				
	<b>Practical:</b>				
	<ol style="list-style-type: none"> <li>1. Installation of network interface card and various network devices like hub, switch, router etc.</li> <li>2. To study different types of Network cables and practically implements cross-wired cable and straight through cable using clamping tool.</li> <li>3. Perform Installation and configuration of workstation PC</li> <li>4. To setup peer-to-peer networking and verify it</li> <li>5. To install and configure server for client server networking; also verify it</li> <li>6. Familiarization with basic network commands: Observing IP address and MAC address, Setting IP address and default gateway in PC, Verifying network layer connectivity</li> <li>7. Dynamic routing (e.g. RIP) and default route</li> <li>8. Configure HTTP, FTP, DHCP server and verify it</li> <li>9. Configuration of DNS and e-mail server</li> <li>10. Design of local area network (LAN, MAN, WAN)</li> </ol>		[45]		

**References books:**

1. "Computer Networks", A. S. Tanenbaum
2. "Data Communications and Networking", Behrouz A. Forouzan
3. "Data communication and computer Network" 'Dr. Sanjay Sharma, S. K. Kataria & sons-latest edition



# Computer Networks

## Unit = 1

**Subash Subedi**

# Introduction to Computer Network

## Unit - 1

### ➤ Introduction

- A network is a set of devices (nodes) connected by communication link.
- A node can be a computer printer or any devices capable of sending &/or receiving data generated by other nodes on the network.
- A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications.
- The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

### ➤ Network Function or Features

Following are some of the importance functions that a network needs to perform.

1. Switching
2. Routing
3. Flow control
4. Security
5. Back-up
6. Accountability
7. Failure Monitoring
8. Internetworking

#### ❖ Switching: -

- Switching is defined as the ability of a network to connect different channel attached to each node to each other. This is essential for moving the traffic from incoming channel desired outgoing channel.

#### ❖ Routing: -

- Routing is defined as the ability of a network to select a path.

#### ❖ Flow Control: -

- Flow control is the control over the rate of traffic. It is necessary in order to reduce the network congestion.

#### ❖ Security: -

- Network security is defined as the ability of a network to disallow any unauthorized access to the network and the data travelling over it. We can make huge of password protection or use of data encryption and other physical security.

#### ❖ Back-up: -

- Back-up is the ability of a network to react to the component failures. Back-up also includes sending to indicate failures or to route the traffic via some other path to avoid failed components.

#### ❖ Accountability: -

- It is the ability of the network to keep track of who is actually using the network.

#### ❖ Failure Monitoring: -

- It is ability of network to keep track of faulting & networking components.

## ❖ Internetworking: -

- When two or more networks are connected, they are called internetwork or internet. Individual network is joined into internetworks by using networking devices like routers, gateways, switches & bridges.

## ➤ Classification of computer network

- The Network allows computers to connect and communicate with different computers via any medium. LAN, MAN and WAN are the three major types of the network designed to operate over the area they cover.
- One of the major differences is the geographical area they cover, i.e., LAN covers the smallest area; MAN covers an area larger than LAN and WAN comprises the largest of all.

## ➤ Introduction of networking

- Networking involves connecting computers and other electronic devices for the purpose of sharing information and resources and for communication. A great deal of technology is required for one device to connect and communicate with another, and many choices for physical connections and related software are possible.
- An elementary network consists of two computers connected by some kind of transmission medium.
- need to share data and to communicate quickly and efficiently.

## ➤ Concept of Internet

- Internet is defined as an Information super Highway, to access information over the web.
- Internet is a world-wide global system of inter connected computer networks.
- Internet uses the standard Internet Protocol (TCP/IP).
- Every computer in internet is identified by a unique IP address.
- IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer location.
- Internet is accessible to every user all over the world.
- It can be considered a global network of physical cables such as copper telephone wires, fiber optic cables, tv cables, etc.
- Internet is different from the World Wide Web as the World Wide Web is a network of computers and servers created by connecting them through the internet. So, the internet is the backbone of the web as it provides the technical infrastructure to establish the WWW and acts as a medium to transmit in form of information from one computer to another computer. It uses web browsers to display the information on the client, which it fetches from web servers.

## ➤ Computer Network Criteria

The criteria that have to be met by a computer network are:

### 1. Performance: - It is measured in terms of transit time and response time.

- Transit time is the time for a message to travel from one device to another

- Response time is the elapsed time between an inquiry and a response.

Performance is dependent on the following factors: -

- The number of users
- Type of transmission medium
- Capability of connected network
- Efficiency of software

2. Reliability: - It is measured in terms of

- i. Frequency of failure
- ii. Recovery from failures
- iii. Robustness during catastrophe

3. Security: - It means protecting data from unauthorized access.

### ➤ Goals of Computer Networks: -

The following are some important goals of computer networks:

1. Resource Sharing: -

- Many organizations have a substantial number of computers in operations, which are located apart. Ex. A group of office workers can share a common printer, fax, modem, scanner, etc.

2. High Reliability: -

If there are alternate sources of supply, all files could be replicated on two or more machines. If one of them is not available, due to hardware failure, the other copies could be used.

3. Inter-process Communication: -

- Network users, located geographically apart, may converse in an interactive session through the network. In order to permit this, the network must provide almost error-free communications.

4. Flexible access: -

- Files can be accessed from any computer in the network. The project can be begun on one computer and finished on another. Other goals include Distribution of processing functions, Centralized management, and allocation of network resources, Compatibility of dissimilar equipment and software, Good network performance, Scalability, Saving money, Access to remote information, Person to person communication, etc.

### ➤ Application of Network

1. Marketing & Sales.
2. Financial Service.
3. Manufacturing.
4. Electronic Message.

5. Tele conferencing (Real Time Multiple Communication).
6. Resource Sharing.
7. Availability of Data.

### ❖ Marketing & Sales

- Used to collect, exchange & analyze data relating to customer needs & product development cycles. Example: - Teleshopping, Online services, e-commerce etc.

### ❖ Financial Service

- Financial Service like electronic fund transfer foreign currency exchange etc.

### ❖ Manufacturing

- Multiple users/workers can work on a project simultaneously which leads faster production of materials.

### ❖ Electronic Messaging

- Email, Messenger, Hangout, etc.

### ❖ Tele conferencing (Real Time Multiple Communication)

- Video call, Audio call etc. This could be helpful in distant learning & telemedicine.

### ❖ Resource Sharing

- It allows all Programs, equipment and data available to anyone on the network irrespective of the physical location of the resource and the user.

### ❖ Availability of Data

- It provides high reliability by having alternative sources of data, so that the data is always replication of data and backup are used.

## ➤ Computer Network Issues

- There are many problems associated with computer network that affect networking. The typical problems can be easily identified & dealt with but there is certain problem that can be tricky to manage. They are: -
  1. Performance Degradation.
  2. Host Identification.
  3. Security Issue.
  4. Net-configuration Conflict.

### ❖ Performance Degradation

- When you experience loss of data integrity and speed in a network, it is generally down to poor transmission and is also known as performance degradation. Due to large size of networks this issue is overloading. This issue can be improved, overcome by using high quality hardware over networking



devices and by using proper software that regularly checks bot-ware, spyware and viruses.

### ❖ Host Identification

- When it comes to host identification, you need to get proper configuration because without an address your computer networking hardware will be unable to send data and messages. Small network generally does not have this issue but in large networks, this is a serious problem use of DHCP server and proper addressing protocols & software could be used when building big computer network, to improve this issue.

### ❖ Security Issues

- This involves protecting computer networking from denial-of-service attack (DOS), Preventing unauthorized users and maintaining network integrity. This issue increases with increase in size of network. This issue can be minimized by proper use of fire-walls, strict password policies, physically securing computer networking assets, installing strong antivirus s/ws and making huge of network analytics s/ms.

### ❖ Net-Configuration conflict

- A small network will generally have a couple of Thousand IP addresses with unique host names available and there is a small chance that a particular device will conflict with another one. That is why you should add multiple routes, so that you can by-pass the problem of busy network. Large networks have to deal with configuration conflicts and busy networks, since they have a lot more traffic going through the network.

To overcome this problem, you need to design a good network structure that could deal with configuration conflicts. You need to acquire professional network setup and design consulting services like Noel Network IT Support.

For internet, IEFT (Internet Engineering task Force) can be implemented for removal of busy network & collision.

## Unit - 2

# Network Architecture

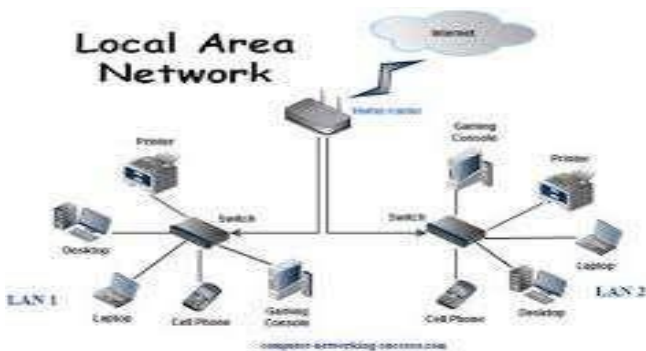
### ➤ Network Types: -

A computer network can be categorized by the size

1. Local Area Network (LAN)
2. Personal Area Network (PAN)
3. Metropolitan Area Network (MAN)
4. Wide Area Network (WAN)
5. Campus Area Network (CAN)
6. Storage Area Network (SAN)

### ❖ Local Area Network: -

- A LAN is a network that is used for communicating among computer devices, usually within an office building or home.
- LAN's enable the sharing of resources such as files or hardware devices that may be needed by multiple users • • Is limited in size, typically spanning a few hundred meters, and no more than a mile.
- Is fast, with speeds from 10 Mbps to 10 Gbps.
- Requires little wiring, typically a single cable connecting to each device.
- Has lower cost compared to MAN's or WAN's.
- LAN's can be either wired or wireless. Twisted pair, coax or fiber optic cable can be used in wired LAN's.



#### ▪ Advantages of LAN: -

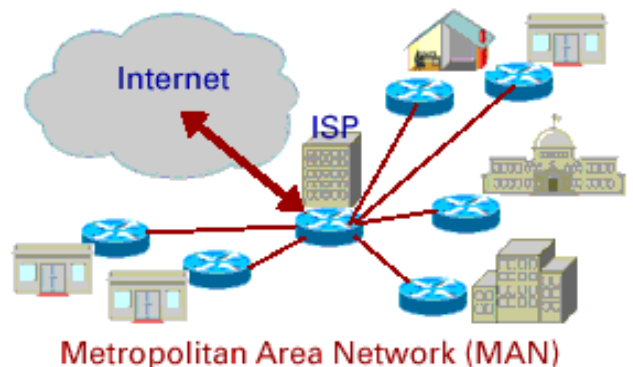
- The data is transferred at an extremely faster rate in local Area Network.
- Local area network (LAN) provides higher security.

#### ▪ Disadvantages of LAN: -

- Initial cost of installing local area network is quite high.
- Unauthorized user can access critical data of an organization in case LAN admin is not able to secure centralized data repository.

### ❖ MAN (Metropolitan Area Network): -

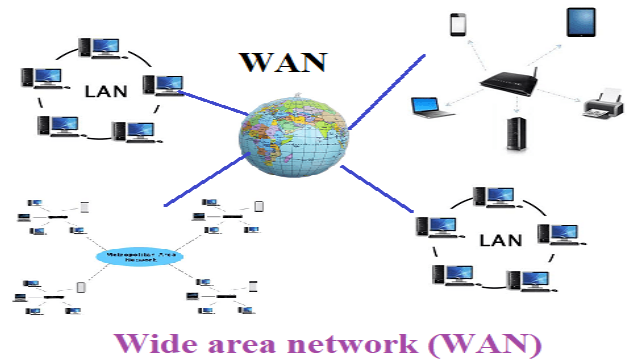
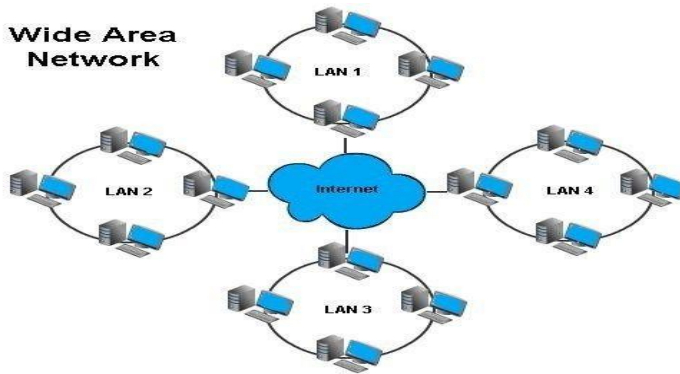
- A Metropolitan Area Network is a Network that covers a larger geographic area by inter connecting a different LAN to form a larger network like banks in a city, Airline Reservation, Military etc.
- This type of networks is larger than a LAN, which is mostly limited to a single building or site.
- A metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.
- A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations.
- A MAN often acts as a high-speed network to allow sharing of regional resources.
- A MAN typically covers an area of between 5 and 50 km diameter.
- Examples of MAN: Telephone company network that provides a high-speed DSL to customers and cable TV network.



- **Advantages of Metropolitan Area Network: -**
  - Its offers fast communication using high-speed carriers, likes fiber optic cables.
- **Disadvantages of Metropolitan Area Network: -**
  - In MAN network, it is tough to make the system secures from hackers.

### ❖ WAN (Wide Area Network): -

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- WAN network system could be a connection of a LAN which connects with other LAN's using Telephone line and radio waves. It is mostly limited to an enterprise or an organization.
- A WAN is two or more LANs connected together. The LANs can be many miles apart.
- To cover great distances, WANs may transmit data over leased high-speed phone lines or wireless links such as satellites.
- Multiple LANs can be connected together using devices such as bridges, routers, or gateways, which enable them to share data.
- The world's most popular WAN is the Internet.



### ■ Advantage of WAN: -

- WAN helps you to cover a larger geographical area. Therefore, business offices situated at longer distances can easily communicate.
- Contain devices like mobile phones, laptop, tablet, computers, gaming consoles, etc.

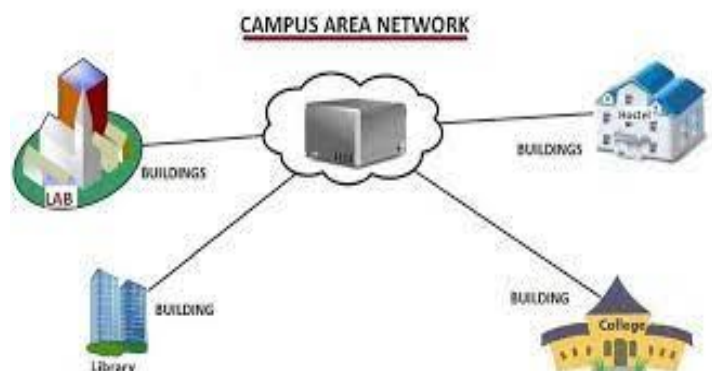
### ■ Disadvantage of WAN: -

- The initial setup cost of investment is very high.
- There are more errors and issues because of the wide's coverages and the use of different technologies.

### ❖ Campus Area Network (CAN): -

- A CAN is a network that covers an educational or corporate campus. Examples include elementary schools, university campuses and corporate buildings.
- A campus area network is larger than a local area network LAN since it may span multiple buildings within a specific area. Most CANs are comprised of several LANs connected via switches and routers that combine to create a single network. They operate similar to LANs in that users with access to the network (wired or wireless) can communicate directly with other systems within the network.
- A CAN is also known as a corporate area network (CAN).
- CAN benefits are as follows:
  - Cost-effective
  - Wireless, versus cable
  - Multidepartment network access

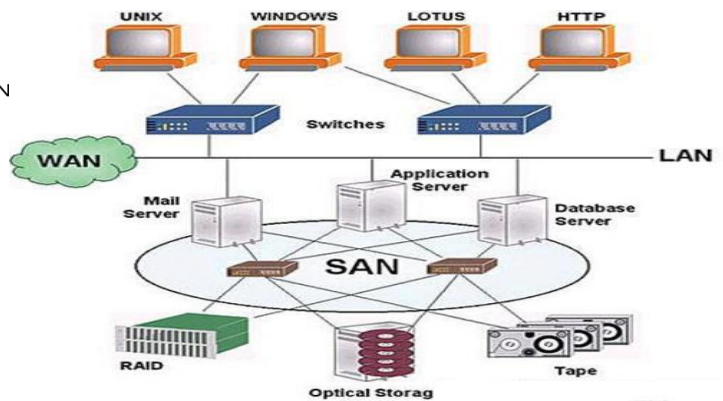
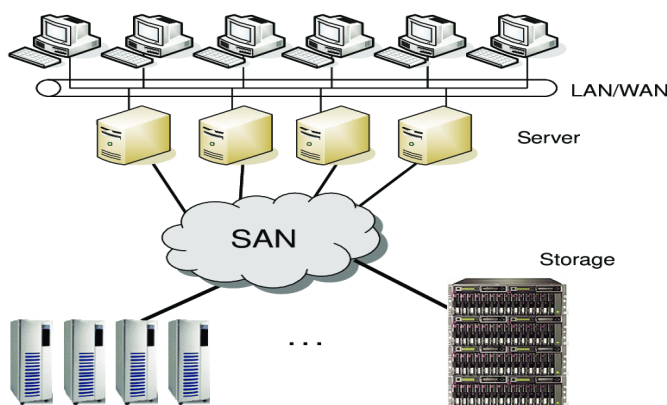
Campus area network (CAN)



- **Advantage of Campus Area Network: -**
  - Campus Interconnection.
  - Better for Every Consumer.
  - Reliability.
- **Disadvantage of Campus Area Network: -**
  - Security risk.

### ❖ **Storage Area Network (SAN): -**

- A Storage Area Network is a type of network which allows consolidated, block-level data storage. It is mainly used to make storage devices, like disk arrays, optical juke boxes and tape libraries.
- A Storage Area Network (SAN) is a specialized, high-speed network that provides block-level network access to storage. SANs are typically composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols.
- This enables each server to access shared storage as if it were a drive directly attached to the server. When a host wants to access a storage device on the SAN, it sends out a block-based access request for the storage device.



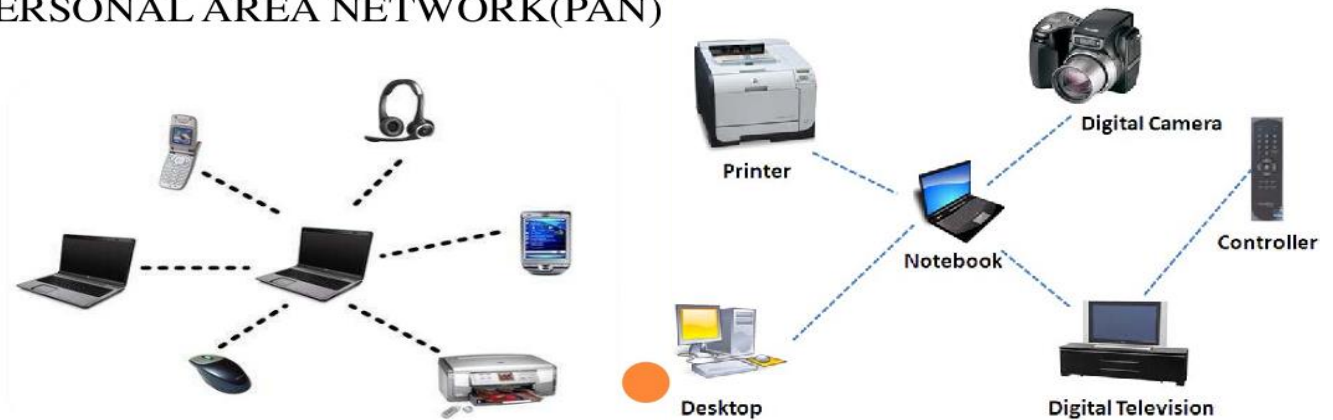
- **Advantages of Storage Area Network: -**
  - Real Time Update
  - Disk Mirroring
  - Administrator Control
- **Disadvantage of Storage Area Network**
  - Security

### ❖ **Personal Area Network (PAN): -**

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- A PAN is a network that is used for communicating among computer devices, usually home.
- PAN's enable the sharing of resources such as files or hardware devices that may be needed by multiple users • • Is limited in size, typically spanning a few hundred meters.

- Personal area network is used for connecting the computer devices for personal area network.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and paly stations.

### PERSONAL AREA NETWORK(PAN)



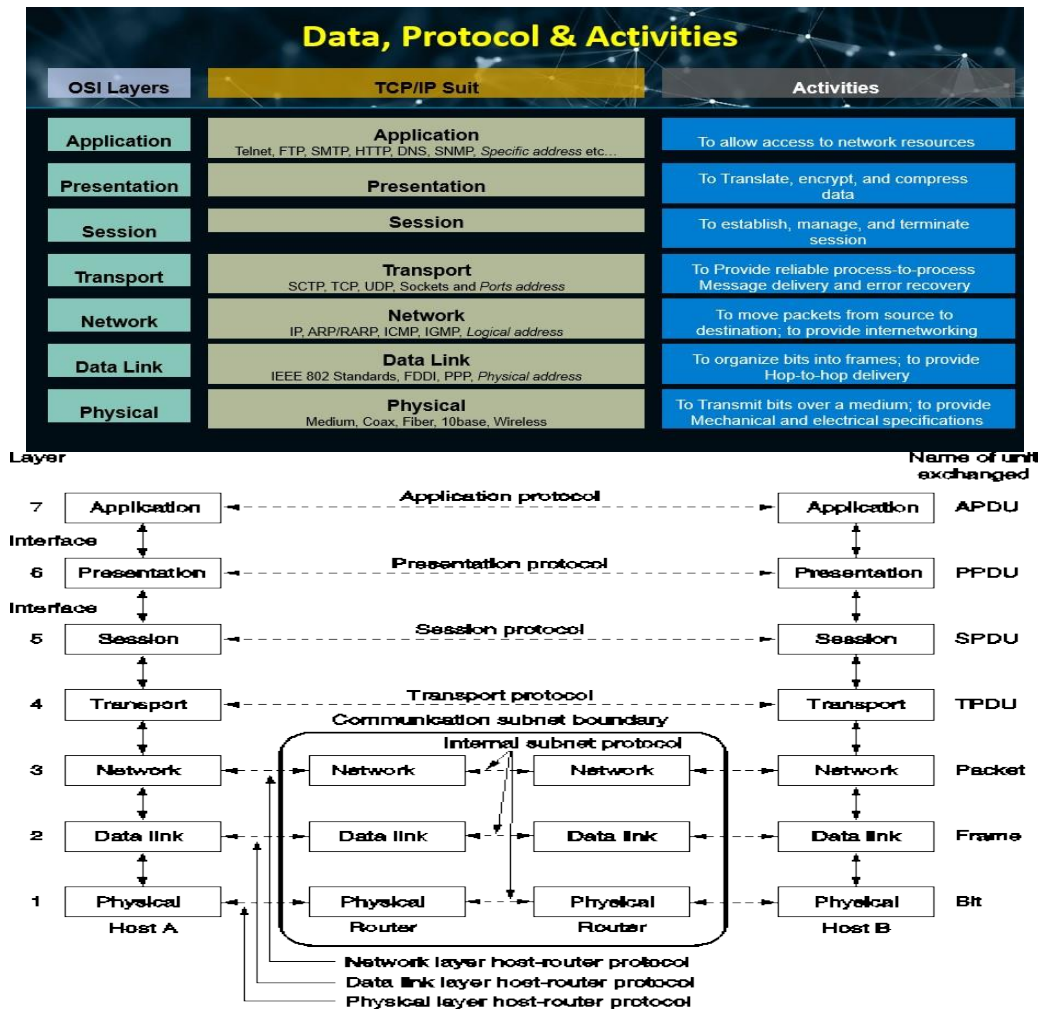
There are two types of personal Area Network: - wired Personal Area Network and Wireless Personal Area Network.

- Advantage of Personal Area Network: -  
- A

### ➤ (Open System Interconnect) OSI Reference Model: -

- Open system interconnection (OSI) Model explains how packet travels through various layers to other devices on a network, even if the sender and destination have different types of network media.





## ❖ Layer 1(Physical layer): -

### Function

- i. To activate, maintain, deactivate the physical connection.
- ii. To define voltage and data rates needed for transmission.
- iii. To convert the digital bits into electrical signals.
- iv. To decide whether the transmission is simplex, half or full duplex.
- v. Physical layer doesn't perform the detection and correction of errors.

## ❖ Layer 2 (Datalink layer): -

### i. Framing (stream of bits into manageable data units): -

The datalink layer divides the stream of bits received from the network layer into frame manageable data units called frames.

### ii. Physical addressing (MAC Address): -

Data link layer adds a header to the frame to define the sender and receiver of the frame.

### iii. Flow Control (mechanism for overwhelming the receiver): -

If the data rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender or vice-versa, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

**iv. Error Control (trailer, retransmission): -**

It has mechanism to detect and re-transmit damaged or lost frames.

**v. Access Control (defining master device in the same link): -**

When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

**❖ Layer 3 (Network layer): -**

- i. To send signals through various channels to the other end.
- ii. To act as network controller by deciding which routes data should take.
- iii. To divide the outgoing message into packets and to assemble incoming packets into message for higher layer.

**❖ Layer 4 (Transport layer): -**

- i. It decides if the data transmission should take place on parallel path or single path.
- ii. It does the functions such as multiplexing, splitting or segmentation on the data.
- iii. It guarantees transmission of data from one end to another.
- iv. Segmentation of a large data so that it can be easily handled by the network layer.

**❖ Layer 5 (Session layer): -**

- i. This layer manages and synchronizes conversation between two different applications. This is the level at which the user will establish system to system connections.
- ii. It allows a process to add check points or synchronization points to a stream of data.
- iii. It allows communication between two processes to take place in either half duplex or full duplex mode.

**❖ Layer 6 (Presentation layer): -**

- i. It makes it sure that the information is delivered in such a form that the receiving system will understand and use it.
- ii. The presentation layer at the sender side changes the information from its sender dependent format into a common format. The presentation layer at receiving machine changes the common format into receiver dependent format.
- iii. Data encryption and compression.

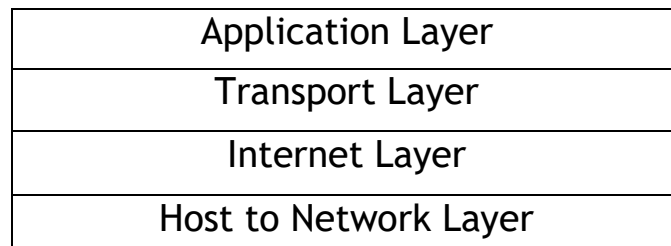
**❖ Layer 7 (Application Layer): -**

- i. It provides user interface and support for services such as email, remote file access and transfer, shared DB management and other types of distributed information services.



## Transmission Control Protocol (TCP/IP Model): -

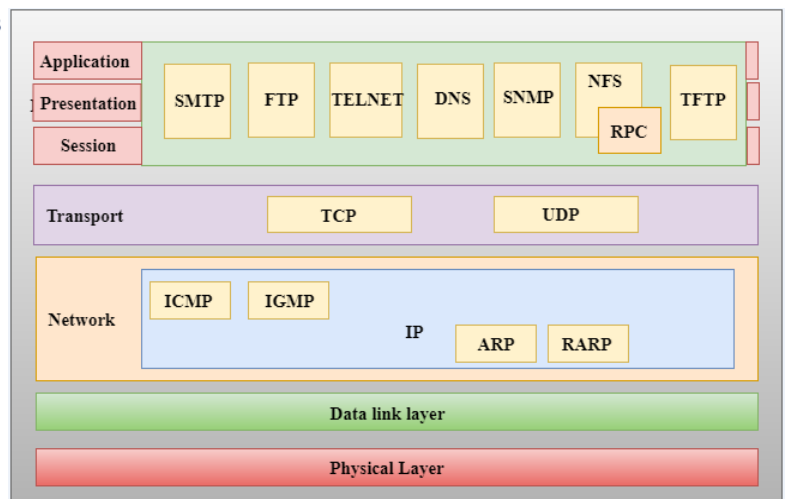
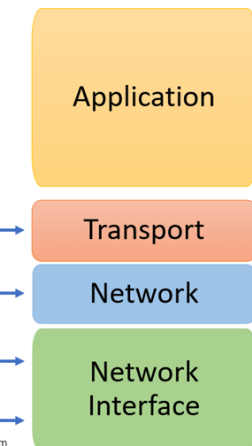
- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards,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



OSI Reference Model



TCP/IP Conceptual Layers



### 1. Host to network layer (Net Access Layer): -

- 1<sup>st</sup> layer of TCP/IP Model.
- Network Access Layer define details of how data is physically sent through the network including how bits are electrically or optically signaled by hardware devices that inter face directly with a network medium such as co-axial cable, optical fiber, or twisted pair, copper cable.
- Protocols such as: - ethernet, token ring x.25, frame relay, etc. are used.
- Ethernet uses an access method called CSMA/ to access media.

### 2. Internet Layer: -

- The job of internet layer is to deliver data packets where they are supposed to go. It defines an official packet format called IP packets and protocols called internet protocols.
- Other protocols used by internet layer ARP (Address Resolution Protocol)  
ICMP (Internet control Manage Protocol)

IGMP (Internet group Management Protocol)  
RARP (Reverse ARP)

### 3. Transport Layer: -

- This layer is responsible for reliability, flow control and correction of data which is being send over the network.
- Two transport protocols.
  - i. Transmission Control Protocol (TCP)
  - ii. User Datagram Protocol (UDP)

#### i. TCP (Transmission control protocol): -

- Reliable, Connection oriented that allows a byte stream originating on one machine tabe delivered without error on any other machine in the internet.
- TCP is a standard that defines how to establish and maintain a network conversation through and maintain a network conversation through which application programs can exchange data.

#### ii. UDP (User Datagram Protocol): -

- Unreliable, connection less.
- Application where minutes error can be neglected such as video transmission.

### 4. Application layer: -

- Top most layer where protocols is such as TELNET, FTP and Email [Simple Mail Transfer protocol (SMTP)]
- Domain Name server/system /service for mapping host name into network address, http for fetching pages on www.
- Real time protocol (RTP) for delivering real-time media such as voices or movies.

- **ARP (Address Resolution Protocol)** - used to associate an IP address with a MAC address.
- **IP (Internet Protocol)** - used to deliver packets from the source host to the destination host based on the IP addresses.
- **ICMP (Internet Control Message Protocol)** - used to detects and reports network error conditions. Used in ping.
- **TCP (Transmission Control Protocol)** - a connection-oriented protocol that enables reliable data transfer between two computers.
- **UDP (User Datagram Protocol)** - a connectionless protocol for data transfer. Since a session is not created before the data transfer, there is no guarantee of data delivery.
- **FTP (File Transfer Protocol)** - used for file transfers from one host to another.
- **Telnet (Telecommunications Network)** - used to connect and issue commands on a remote computer.
- **DNS (Domain Name System)** - used for host names to the IP address resolution.
- **HTTP (Hypertext Transfer Protocol)** - used to transfer files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

### Differentiate between OSI / TCP model: -

The differentiate between OSI/TCP model are listed below: -

OSI	TCP/IP
The refer to (Open System Interconnect) OSI Reference Model	It refers to Transmission Control Protocol (TCP/IP Model)
Transport layer guarantees delivery of packet.	Transport layer Doesn't guarantee delivery of packet.
Separate session and presentation layer	No session and presentation layer. But characteristics are provided by the transport layer and application layer respectively
Network layer provides both connectionless and connective oriented services.	Network layer provides only connection less services i.e., no need connection between two devices to be online.
Protocols of OSI model can be easily replaced as the technology	It is very hard to replace existing protocols.
The minimum size of the OSI header is 5 bytes.	The minimum header size is 20 bytes.

### ➤ Network Standard Organization: -

1. **ISO:** - International organization of standardization makes standard for many different activates.
2. **ANSI:** - American National Standards Institutes. US representative of ISO.
3. **IEEE:** - Institutes of Electrical and Electrical Engineer.
4. **IETF:** - Internet Engineering Task Force. It looks after traffic and controls the congestion.
5. **IANA:** - Internet assign number authority. To gives all IP address

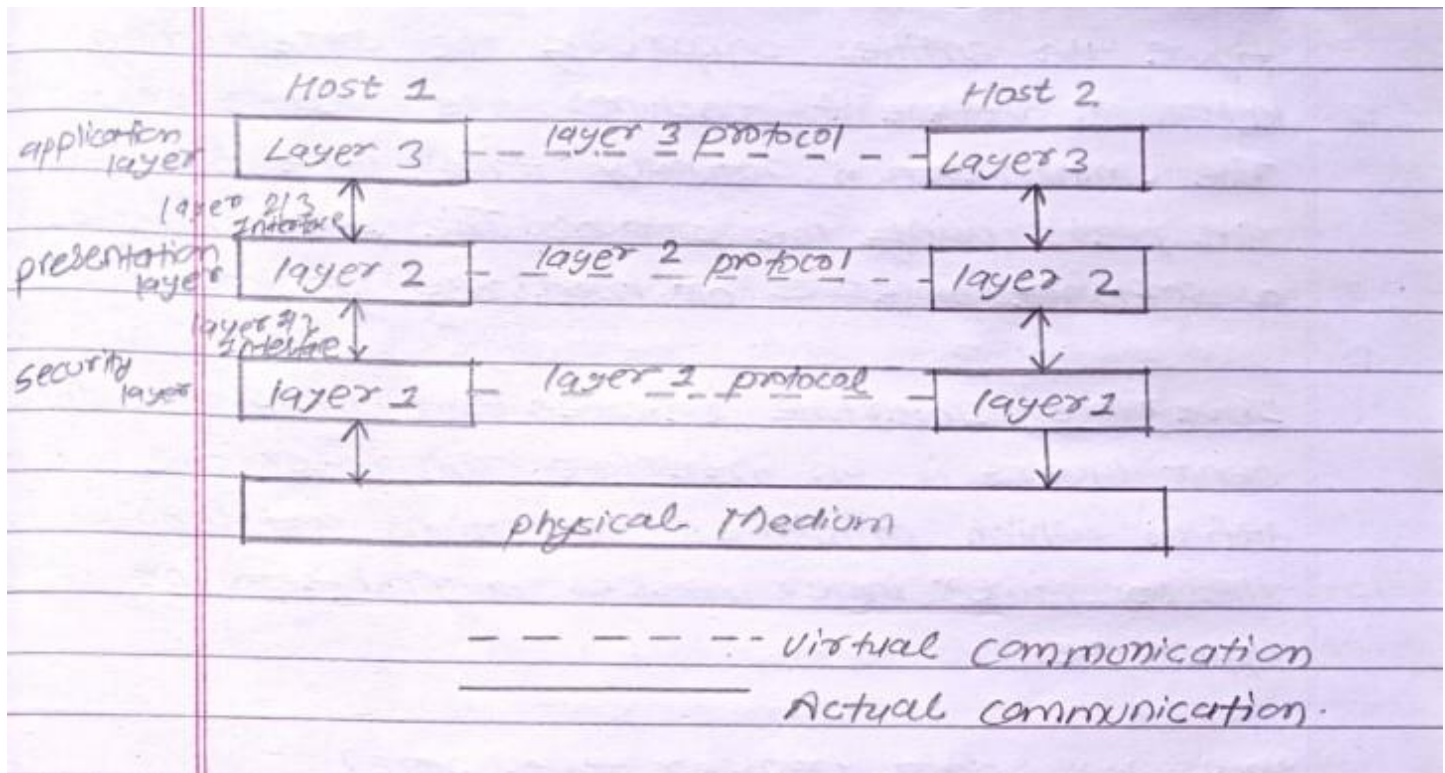
### ➤ Network Protocol: -

- A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially it allows connected devices to communicate with each other regardless of any differences in their internal process, structure or design.

Example: -

TCP (Transmission Control Protocol)  
 UDP (User Datagram Protocol)  
 IP (Internet Protocol)  
 ARP (Address Resolution Protocol)  
 SMTP (Simple Mail Transfer Protocol)

### ➤ Layered Network Architecture: -



The most networks are organized as a series of layers one above others to reduce the design complexity of the network. The no. of each layer, the no. of each layer, the contents of each layer differ from network to network.

The purpose of each layer is to offer certain services to higher layers  $n$  on one machine carries on a conversation with layer  $n$ . on another machine.

The rules and convention used in this conversation are collectively known as protocol. Basically, a protocol is an agreement between the two machines as how communication links should be established, maintained and released.

### Peer: -

A three-layer architecture is shown in figure the entities comprising the corresponding layers on different machines are called peers. The communication actually takes places between the peers using the protocol. The peers may a software processes or hardware devices.

### Interface: -

Interface between each pair of adjacent layers is an interface. The interface defines which primitive's operations and services the lower layer makes available to the upper one.

### How does data transfer take place?

No, data is transferred directly from one much to other on that layer. The layers can only talk to the ones above or below them on their host. The data and information are passed on the lower layer by upper layers until the lowest layer (layer-1) is reached. Below layer-1, there lies the physical medium such as coaxial cable through which the actual communication takes places.

## Virtual communication Between layers: -

Let us consider a 5-layer network architecture and steps of data transfer is explained below: -

### Step 1: -

A message “th” is produced by layers of machine 1 given to layer 4 for transmission

### Step 2: -

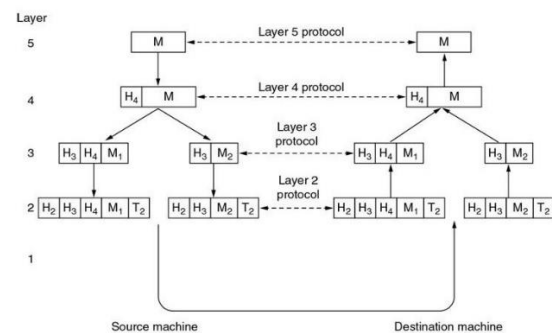
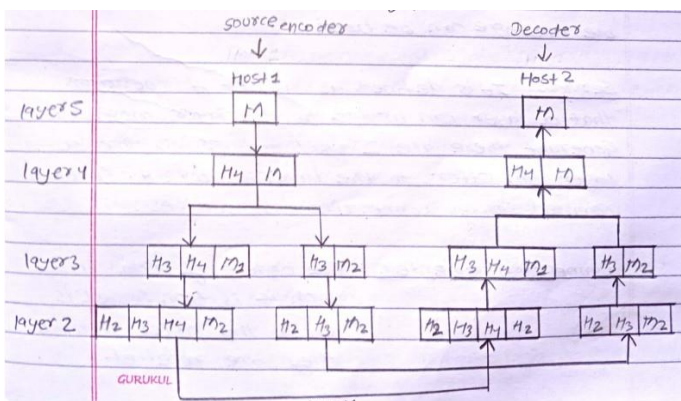
Layer 4 adds a header in front of the message; so as to identify the message to layer 3. A header includes the control information and it allows a layer in machine to deliver the message in right order.

### Step 3: -

Layer 3 breaks up the incoming message into small units. Packets and appends a layer 3 header to each packet th1 and th2 as shown in fig and passes these packets to layer 2.

### Step 4: -

Layer 2 adds header and trailer to each packet obtained from layer 3 and hands over the resultant unit to layer 1 for physical transmission.



## ➤ Design Issues for layers: -

### 1. Addressing: -

Since there are multiple possible receivers, some form of addressing is required in order to specify a specific destination.

### 2. Direction of transmission: -

Another issue is direction of data transfer. It can be simplex, half duplex, full duplex.

### 3. Error Control: -

Error detection and correction both are essential. (Meaning detecting code) methods can be used and mechanism should be implemented to correct those errors.

### 4. Ability of receiving long message: -

- Problem of not receiving long messages.

- Methods like disassemble, transmit and reassemble message can be used.

### ➤ Services: -

It is defined as the set of operations that a layer can provide to the layer above it. Generally, there are 2 types of services that a layer can offer to the layers above it. Connection oriented services, connectionless services.

### ➤ Connection Oriented: -

The order of data in which it is transferred is seen as the order in which they are received.

Example: - telephone system.

### ➤ Sequence: -

- Establish a connection.
- Use a connection.
- Release the connection.

### ➤ Connectionless Services: -

Each message carries the full address of the destination. Each message is routed independently from source to destination. The order of message in which they were sent could be different as the order in which they are received.

### ➤ Quality of Services: -

Each service can be judged by its quality of services. Services can be of 2 types:

1. Reliable (Which never loses data) (guarantee of data)
2. Unreliable (No guarantee of arrival/can loss data)

### ➤ Service Operations/Primitives: -

#### 1. Listen: -

Server listens for connection.

#### 2. Connect: -

Client executes connect to establish a connection with server.

#### 3. Receiver: -

Server execution receiver operation and blocks other processes.

#### 4. Send: -

Client execute send to transmit request and when request packets reach the server unblocks.

#### 5. Disconnect: -

After receiving packet, server issues a disconnect to acknowledge the client and terminate the connection.



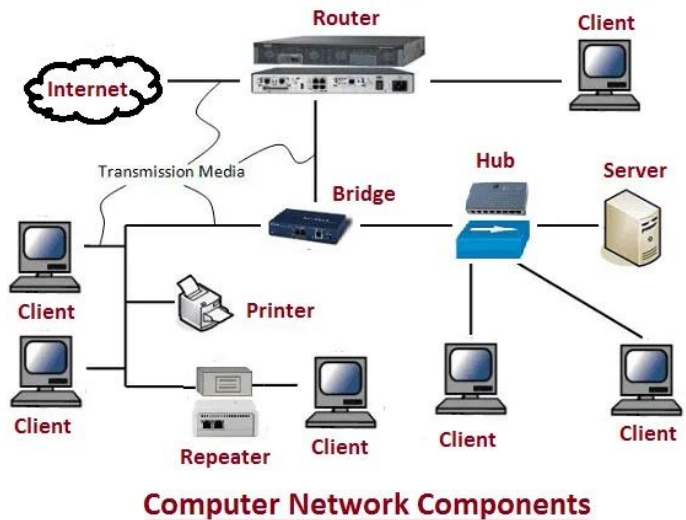
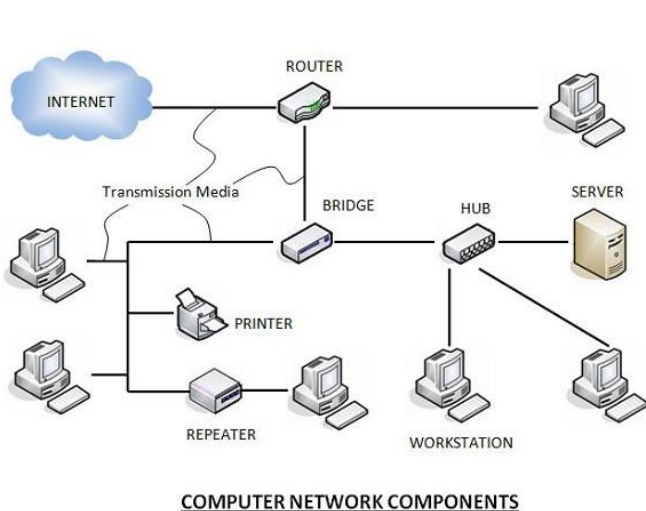
## Unit - 3

# Hardware and Software for Computer Network

### ➤ Computer Network Components: -

Computer Network Devices are comprised both physical parts as well as the software required for installing computer networks both at organizations and at home. The hardware components are operating systems and protocols.

The following figure shows a network along with its components: -



### ➤ Hardware Components: -

- **Servers: -**

Servers are high-configuration computers that manage the resources of the network. The network operating system is typically installed in the server and so they give user accesses to the network resources. Servers can be of various kinds: file servers, database servers, print servers etc.

- **Clients: -**

Clients are computers that request and receive service from the servers to access and use the network resources.

- **Peers: -**

Peers are computers that provide as well as receive services from other peers in a workgroup network.

- **Transmission Media: -**

Transmission media are the channels through which data is transferred from one device to another in a network. Transmission media may be guided media like coaxial cable, fiber optic cables etc. or maybe unguided media like microwaves, infra-red waves etc.

- **Connecting Devices: -**

Connecting devices act as middleware between networks or computers, by binding the network media together. Some of the common connecting devices are:

- a. Routers
- b. Bridges
- c. Hubs
- d. Repeaters
- e. Gateways
- f. Switches

## ➤ Software Components: -

### • Networking Operating System: -

Network Operating Systems is typically installed in the server and facilitate workstations in a network to share files, database, applications, printers etc.

### • Protocol Suite: -

A protocol is a rule or guideline followed by each computer for data communication. Protocol suite is a set of related protocols that are laid down for computer networks. The two popular protocol suites are: -

- a. OSI Model (Open System Interconnections)
- b. TCP / IP Model

## ➤ Network Devices: -

1. Repeater.
2. Hub.
3. Bridge.
4. Router.
5. Gateway.
6. Switch.
7. Network Interface Card (NIC)

### 1. Repeater: -

Devices that regenerate signals to ensure data transmission are called repeater. A repeater receives a signal and before it becomes too weak or corrupted, it regenerates, the original bit pattern. Repeater is not an amplifier because amplifier simply amplifies the entire incoming signal along with noise. Repeater regenerates the original signals and removes noise. Repeater operates at physical layer of OSI Model.

### 2. Hub: -

Hub is a connecting device that allows to connect 2 or more hosts (client) in a network. It is basically used for connecting stations in a physical star topology.

Types: -

- Passive.
- Active.
- Intelligent.

#### a. Passive: -



A passive hub simply combines the signals of the network segments. There is no signal processing or regeneration.

### b. Actives: -

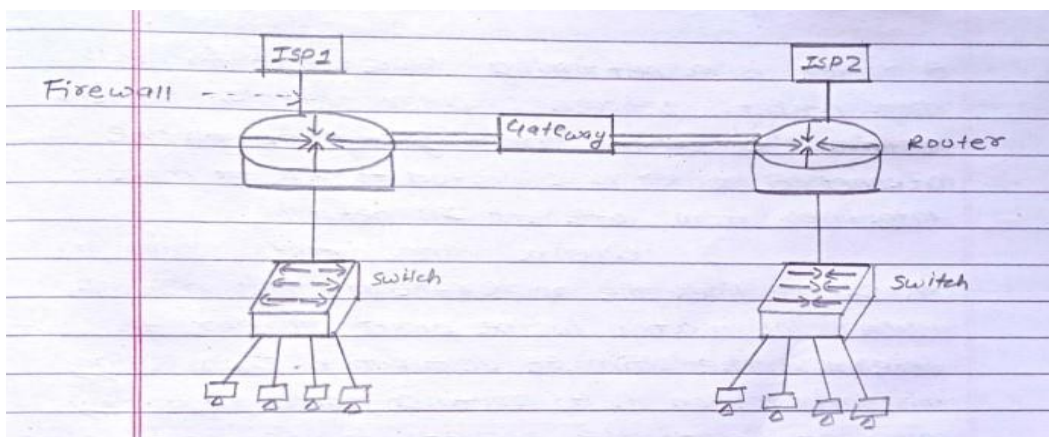
They are like passive hub but have electronic components for regeneration and amplification of signals. The main drawback is that they amplify noise along with the signals. Expensive than passive hubs.

### c. Intelligent: -

In addition to signal regeneration, intelligent hubs perform some network management and intelligent path selection. A switching hub chooses only the port of the devices where the signal needs to go rather than signals along all paths.

## 3. Bridges: -

Bridges operates in physical layer as well as the datalink layer. It can regenerate the signals that it receives and as a datalink layer device it can check the physical MAC address of the source and destination contained in the frame. The main difference between a repeater and a bridge is that a repeater and a bridge is that a repeater simply extends the range of network while a bridge ties 2 networks together. For this bridge's interconnection two or more routers.



### ▪ Classification of Bridges: -

- Routing Bridges
- Transparent Bridges

### i. Transparent Bridge: -

Transparent Bridge is the bridge in which the stations are not at all aware of the existence of the bridges. TB keeps a table of address in memory to determine where to send data.

### ii. Routing Bridge: -

In routing bridge, a sending station defines the bridge that must be visited by the frame. The address of these bridges is included in this frame. Hence, a frame contains not only the source and destination addresses but also the bridge address.

## 4. Router: -

A Router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the internet. A router is connected to two or more data lines from different IP Networks.

When a data packets comes on once of the lines the router reads the network address information in the packet header to determine the ultimate destination. Then, using this information in it's routing tables or routing policy, it directs the packets to the next network on its journey. Routers work at network layer of OSI Model.

## 5. Gateway: -

When the networks that must be connected are using completely different protocols from each other a powerful and intelligent device called a gateway is used. Gateways serve as an entry and exit point for a network as all data must pass through or communicate with the gateways before being routed. Gateways can also act as proxy server and a firewall.

## 6. Switch: -

A switch is a device which provides bridging functionality with greater efficiency. A switch acts as a multiport bridge to connect devices or segments in a LAN. In simplified term, switch is designed computers within a network. Switches are most often used in large networks. A large network may include multiple switches which connect different groups computer system together. These switches are typically connected devices to access the internet.

## 7. Network Interface Card (NIC): -

A NIC is a hardware component without which a computer cannot be over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter, LAN adapter. It is of two types: -

- I. Internal
- II. External

### ■ Internal: -

Motherboard has a slot for the network card where it can be inserted.

### ■ External: -

In desktop/ laptops, that doesn't have internal NIC, External are used. It can be used via USB.

## ➤ Difference Between Server and Workstation: -

The difference between server and workstation are: -

	Server	WorkStation
Definition	A server is an application or devices that perform services for connected clients as a part of client server architecture.	A computer that is used to power applications such as graphic art, 3D designs, video editing or other CPU/RAM intensive Software
OS	Linux, windows server, free BSD etc. (used).	Unix, Linux, windows workstation etc.
GUI	Optional	Installed

Reliability	Often comes with error correcting modules. Disk storage are a typical ally in RAID, more than one power supply unit and more than one network port.	No error correcting module, RAID storage disk isn't used. Only one power supply unit & only one network port.
Example	Web server, DNS Server, Proxy Server etc.	Video and audio workstation

## ➤ Networking Models: -

### A. Client-Server Model: -

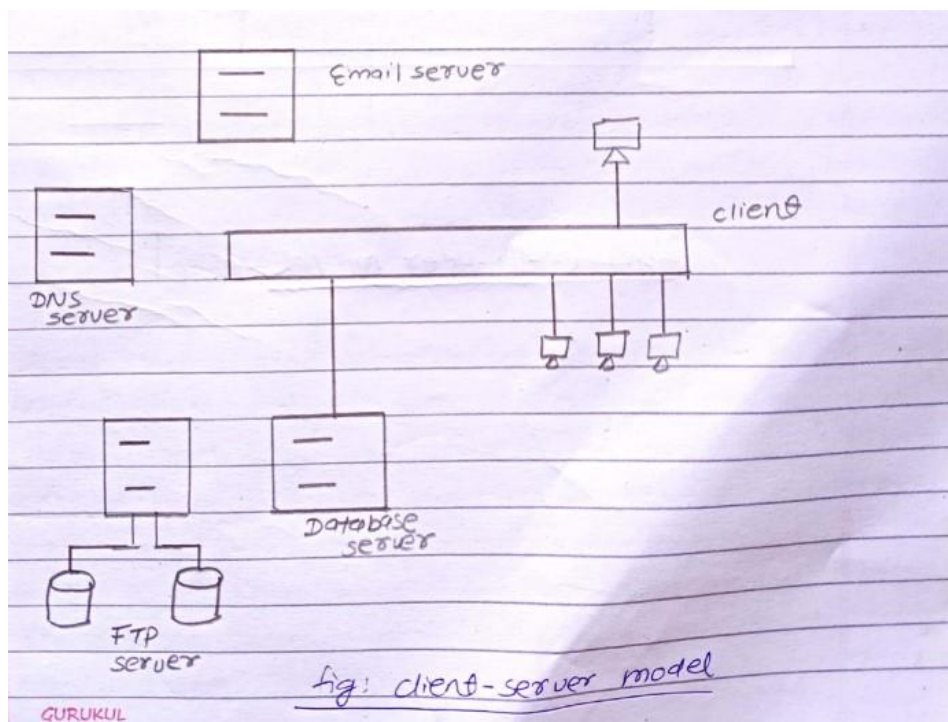
A network is built around one or more dedicated servers and is administrated from a central location. Client connect to the dedicated servers through the network to access the resources such as printer, server, storage and so on. Communication takes the form of the client process sending a message over the network to the server process. The client process then waits for a reply message when the server process gets the request, it performs the requested work or looks up the requested data and sends back a reply. There are two types of client server model.

#### 1. Thin Client: -

It is a network computer with no local storage. It processes information independently but relies on servers for application, storage and administration.

#### 2. Thick Client: -

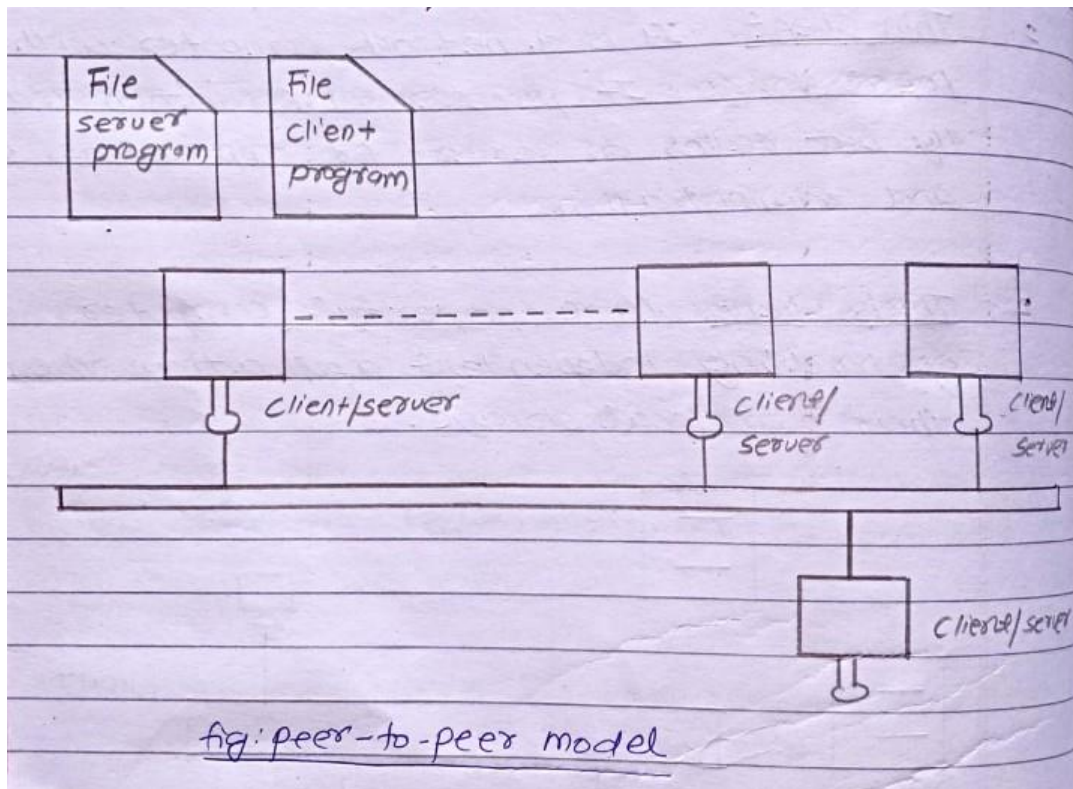
More powerful computer capable of handling independent applications they have their own local storage.



### B. Peer-to-Peer Network Model: -

There is no server and computer simply connect with each other in a workgroup to share files, printers and internet access. All computers and users have equal

authority and rights. Each pc acts as an independent workstation that stores data on its own hard drive but which can share it with all other pcs on the network.



### ➤ Connection oriented vs Connection less services

Comparison Parameters	Connection Oriented Services	Connection less services
Related system	It is designed and developed based on the telephone system.	It is services based on the postal system.
Definition	It is used to creates an end-to-end connection between the senders to the receiver before transmitting the data over the same or different network.	It is used to transfer the data packets between sender to the receiver without creating any connection.
Virtual path	It creates a virtual path between the sender and the receiver.	It doesn't create any virtual connection or path between the receiver.
Authentication	It requires authentication before transmitting the data packets to the receiver.	It doesn't require authentication before transferring data packets.
Data packets path	All data packets are received in the same order as those order as those sent by the sender.	Not all the data packets are received in the same order as those sent by the sender.
Bandwidth requirement	It requires a higher bandwidth to transfer the data packets.	It requires low bandwidth to transfer the data packets.

Data reliability	It is more reliable connection service because it guarantees data packets transfer from one end to the other end with a connection.	It is not a reliable connection services connection services because it does not guarantee the transfer of data packets from one end to another for establishing a connection.
Examples	Transmission Control Protocol (TCP) is an example of connection-oriented services.	User Datagram Protocol (UDP), Internet Protocol (IP), and Internet Control Message Protocol (ICMP) are the examples.

## Unit - 4

### LAN Architecture and Standards

#### ➤ Network Topologies: -

- It is defined as the arrangement of various elements for a communication network. It is of two types: -
  1. Physical Topologies
  2. Logical topologies

#### 1. Physical Topologies: -

- It describes the geometric arrangement of components that makes up the LAN. It refers to the way the computers are cabled together. They are bus topology, ring topology, mesh topology, tree topology, hybrid topology etc.

#### 2. Logical Topologies: -

- It describes the possible communication between pairs of network ends points (Nodes) that can communication token verse, token ring are some examples.

#### A) Bus Topology: -

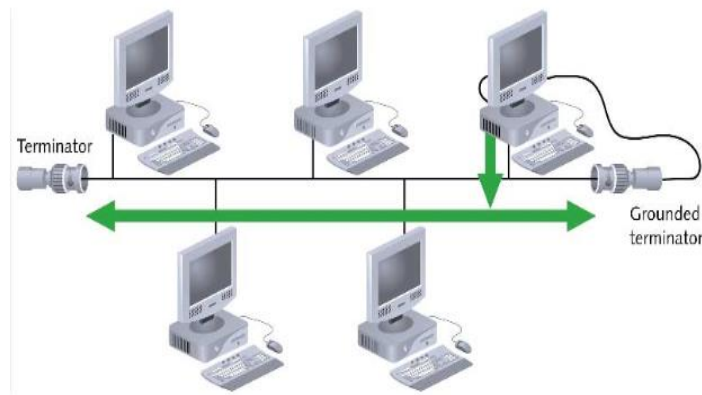
- All nodes are connected to a single common cable known as the backbone.
- Both end of the backbone must be terminated with a terminating resister to prevent signal bounce and complete the circuit.
- If the backbone cable fails, the entire network effectively becomes unusable.
- Bus (backbone) carries all network data.
- Bus networks work best with a limited number of devices.
- When one computer sends a signal up the wire all the computers receive the information but only one with the address that matches accepts the information, the rest disregard the message.

#### ▪ Advantages: -

- Easy to implement.
- Requires least amount of cable to connect the computers together.
- Failures of one station does not affect the others.

▪ **Disadvantages: -**

- A central cable break can disable the entire network.
- Difficult to troubleshoot.
- Collisions occurs when two nodes send message simultaneously.



**B) Star Topology: -**

- Most dominant topology type in contemporary LANs.
- Every node on the network is connected through a central device.
- Each computer on a star network communicates with a central device that resends the message either to each computer or only to the destination computer.
- A central device (hub) connects hubs and nodes to the network.
  - Each node connects to its own dedicated port on the hub.
  - Hubs broadcast transmitted signals to all connected devices.
  - we can connect multiple hubs to form a hierarchical star topology.

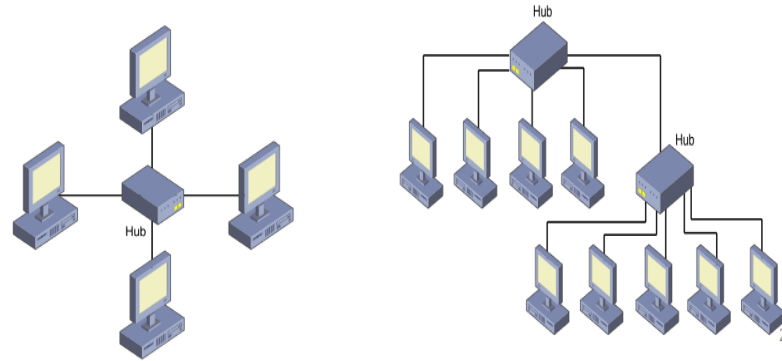
▪ **Advantages: -**

- Single computer failure does not necessarily bring down the whole star network.
- Easy to connect new nodes or devices.
- Centralized management.
- Most popular topology in use; wide variety of equipment available.
- The center of the star network is a good place to diagnose the faults.
- Compared to Bus topology it gives far much better performance.

▪ **Disadvantages: -**

- If central device fails, the entire network goes down.
- Requires more cable than the bus topology.
- Performance is depending on central device.





### C) Ring Topology: -

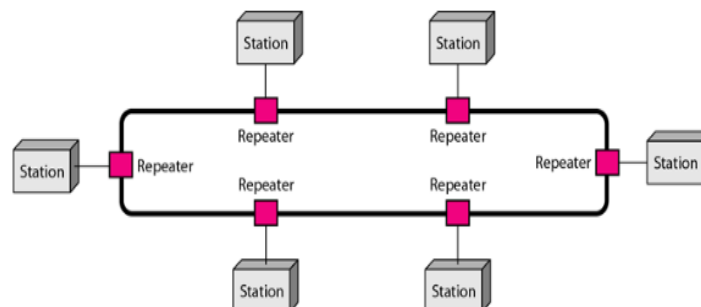
- Each node is connected to the two nearest nodes so the entire network forms a circle.
- Ring network consists of nodes that are joined by point- to- point connections to form a ring.
- Data are transmitted around the ring using token passing either clockwise or counterclockwise.
- No central hub.
- Each node will repeat any signal that is on the network regardless its destination. The destination station recognizes its address and copies the frame into a local buffer as it goes by. The frame continues to circulate until it returns to the source station, where it is removed.
- A failure in any cable or device breaks the loop and can take down the entire network.

#### ■ Advantages: -

- Each computer has equal access to resource.
- Performance is better than that of Bus topology.
- Network is point- to- point connections. Hence, easier to locate defective node.

#### ■ Disadvantages: -

- Failure of one computer on the ring can affect the whole network.
- Each packet of data must pass through all the computers between source and destination, slower than star topology.



### D) Mesh Topology: -

- The Internet is a mesh topology.

**Two Types:**

- Fully Connected
- Partially Connected

**❖ Fully Connected Mesh Topology: -**

- All nodes are interconnected.
- Each and every node has a unique point to point link with all the other nodes. This feature leads to the reliability and fault tolerance.
- In mesh topology it will connect or share traffic between two nodes only.
- Messages sent on a mesh network can take any of several possible paths from source to destination.

**❖ Partial mesh topology: -**

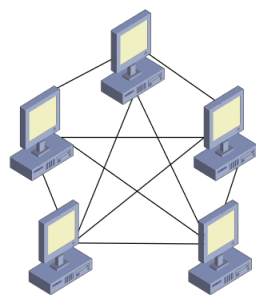
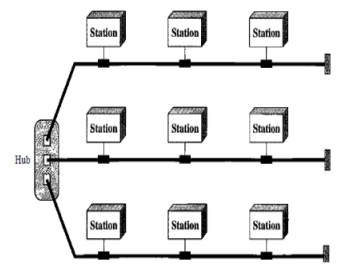
- In Partial mesh topology, nodes are connected to only some, not all, of the other nodes.

**▪ Advantages: -**

- When a link of other nodes fails to connect it will not affect the entire network.
- There is a facility of a unique link between nodes to ensure higher finest data rate and remove traffic issues.
- Error identification and error isolation can be found easy.
- It is robust.

**▪ Disadvantages:**

- It is most expensive network from the point of view of link cost i.e., cost of cable.
- Bulk wiring is required.
- Installation and configuration are difficult if the connectivity gets more.

**Mesh Topology***A hybrid topology: a star backbone with three bus networks*

26

**E) Hybrid Topology: -**

- A star backbone and 3 bus networks.

**F) Tree topology: -**

Variation of star Topology.



## ➤ **MAC (Media Access Control): -**

- The MAC is a sublayer of the datalink layer of the OSI Reference Model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of the data packets via remotely shared channels. It sends data over the Network Interface Controller (NIC).

### **Function of the MAC Layer: -**

- It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- It resolves the addressing of source station as well as the destination station or a group of destination station.
- It performs multiple access resolutions when more than one data frames are to be transmitted.
- It also performs collision resolution and initiating retransmission in case of collisions.
- It generates FCS that helps against transmissions errors.

### • **MAC Address: -**

- Each network card has a unique address that is burned into the card by its manufacturer. This unique address, known as a MAC address, is used in the header of the packet for the source and destination addresses of the packet. The MAC address is a 48-bit address displayed in a hexadecimal format that looks similar to 00-90-4B-4C-C1-59 or sometimes 00:90:4B:4C:C1:59.
- The MAC address is made up of 12 characters and is in hexadecimal format.
- The first half of the MAC address is the manufacturer's address, while the last half of the address is the unique address assigned to that network card by the manufacturer.

### • **Multiple Access Protocol (MAP): -**

- MAP is used to coordinate access to link.
- Nodes can regulate their transmission on to the shared broadcast channel by using Multiple Access Protocol.
- It is used for both wire & wireless Local Area Network and Satellite network.

### • **CSMA/CD (Carrier Sense Multiple Access with Collision Detection).**

- It is a media access control method which uses carrier sensing scheme in transmitting data. If it is idle, then it sends data, otherwise it waits till the channel becomes idles. However, there is still chance of collision in CSMA due to propagation delay i.e., if data being transferred by a station is delayed due to propagation delay, another station might sense the channel being idle and can transmit data. Now both the packets are in the channel which might cause collision.

CSMA/CD is a MAC method that helps a collision detection during CSMA Method. If, collision detection during CSMA method. If, collision is detected, station stops transmitting the frame. Transmits the join signal and waits for random time interval before trying to resend the frame (CSMA/CD) was early

used in ethernet technology / LANs, but nowadays, Ethernet is full duplex and CSMA/CD is not used.

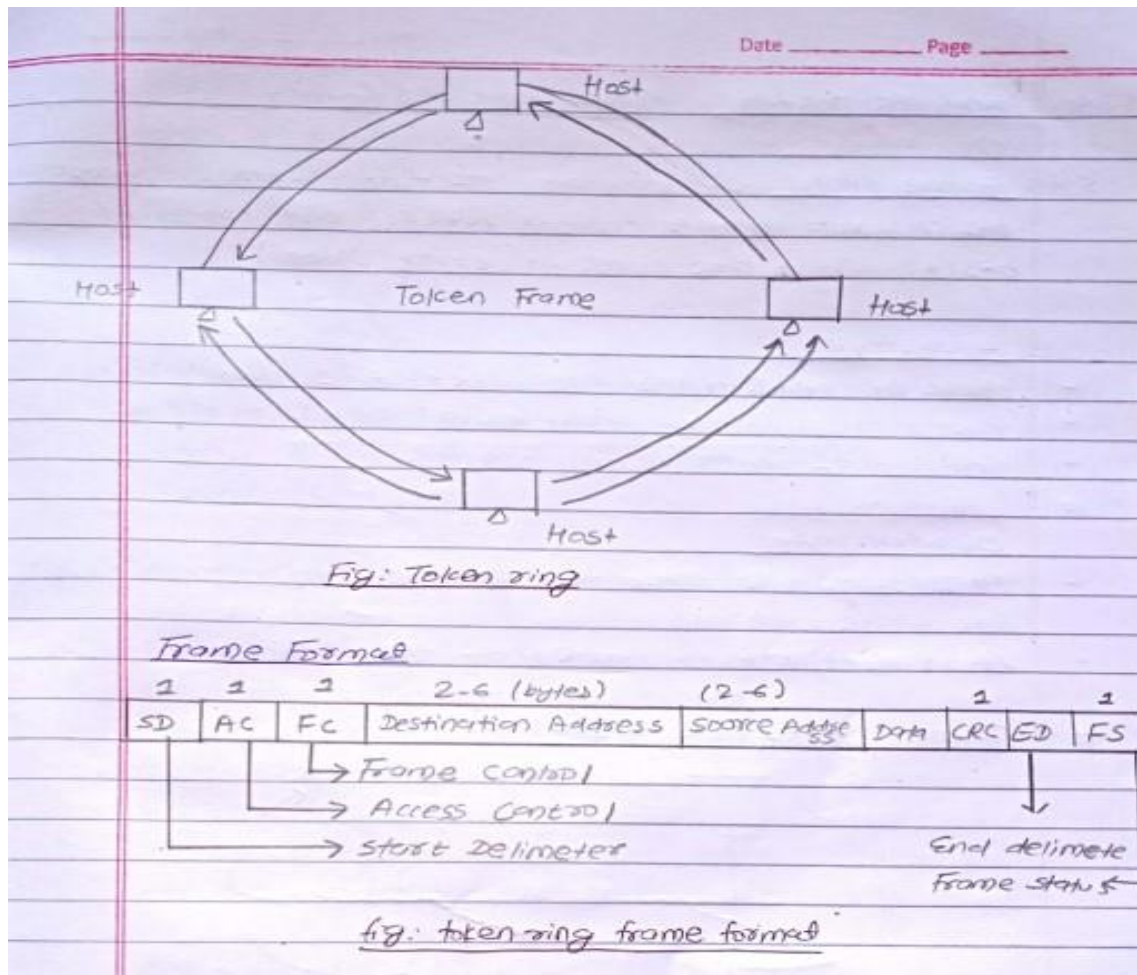
## 1. Token Ring (IEEE 802.5): -

- A Token Ring network is a Local Area Network in which all computers are connected in a ring or star topology and pass one or more logical tokens from host to host. Only a host that holds a token can send data, and token can send data, and token are released when receipt of the data is confirmed. Token ring networks prevent data packets from colliding on a network segment because data can only be sent by a token holder and the number of tokens available is controlled.

The most broadly deployed token ring protocols were IBMs released in the 1980's and the standardized version of it known as IEEE 802.5 the IEEE standard version provides for data transfer rates of 4,16 or 100 Mbps.

### • How Token Ring Works?

1. Systems in the LAN are arranged in a logical ring, each system receives data frames from its logical predecessor on the ring and send them to its logical successor.
2. An empty frame is continuously circulated on the ring.
3. When a computer has a message to send, it waits for an empty frame, when it has one it does the following.
  - a) Insert token indicating that its is sending data in the frame.
  - b) Insert the data if it wants to transmit into the payload section of the frame.
  - c) Sets a destination identifier on the frame.
4. All computers check the data packets when ever it comes, if the destination identifier is different, it regenerates the frames and retransmits to the next host unit the destination is reached.
5. When the packet is reached to the destination, it simply copies the message from the frames and clears the token to indicates receipts.



### 1. Start Delimeter: -

Marks beginning of frame.

### 2. Access Control: -

It consists of the priority bits (P), Token bits (T), monitoring bits (M) & reservation bits (R) for access control.

### 3. Frame Control: -

Specifies types of Frames (data or control frame).

### 4. End delimiter: -

Marks's end of frames.

### 5. Frame Status: -

It consists of two address recognized bits (A), two Frame copied bits (C) and reserved bits (x), which are used in error control.

### • Advantages: -

- Used in real time and interactives application.
- Every computer is given equal access to token.
- Collision of data is overcome.

### • Disadvantages: -

- Failure of one computer on the ring can affect the whole network.
- It is difficult to trouble shoot the ring.

## 2. Token Bus (IEEE 802.4): -

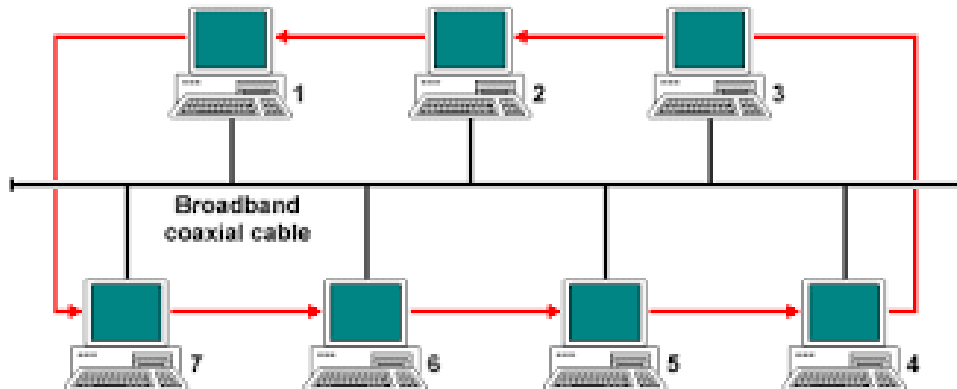


Fig: - Token Bus

- The IEEE 802.4 standard for MAC is known as Token Bus. Token Bus is a linear or tree shaped cable through which different stations are interconnected. The token is passed from one user to another in a sequence (clock-wise or anti clock wise) Each station knows the address of station to its left or ring. A station can only transmits data when it has the token. The working of token bus is some what similar to token ring.

### Operations: -

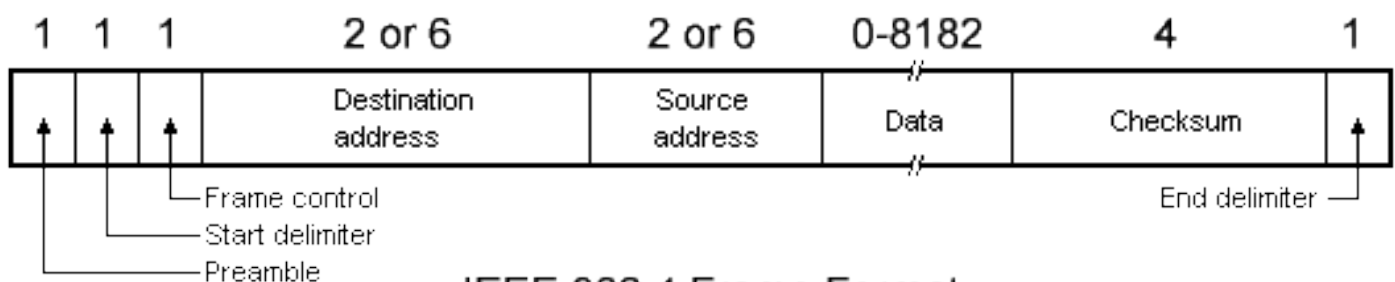
1. At any time, the station which holds the token only can transmit its data frames on the bus. Every frame contains source and destination address.
2. All other stations are ready to receive these data frames.
3. As soon as the transmission time of a station is over, it passes the token to the next station in the logical sequence.
4. In one cycles of operation each station gets an opportunity to transmit one.

### • Advantages: -

- Easy to understand and implement.
- Cheap and easy to expand.

### • Disadvantages: -

- If central cables breaks, brings down the whole network causing wholes network activities to stop.
- Heavy network traffic slows down the bus speed.



IEEE 802.4 Frame Format

1. Preamble: Used for synchronization.
2. Checksum: For error detection.

### ➤ Ethernet (IEEE 802.3): -

- IEEE 802.3 defines the physical layer and the medium access control (MAC) sublayers of the datalink layer for wired ethernet networks. IT is based on the technology called carrier sense multiple access with collision detection (CSMA/CD). The ethernet is a multi-access network meaning that a set of nodes send and receive frames over a shared link. The medium is a coaxial cable with 10 Mbps for earliest days, a 100 Mbps version called gigabits ethernet. Now a days CSMA/CD is useless in ethernet because they use full duplex connection. In full duplex connection both sender & receiver are capable of sending & receiving data at the same time without any collisions.

### Addressing in Ethernet: -

#### 1) Unicast:

One sender one receiver.

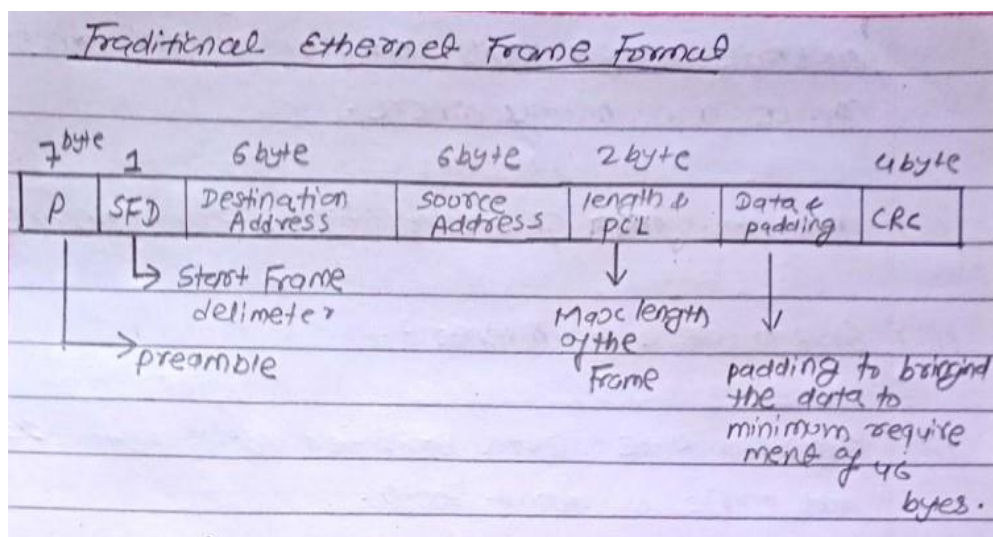
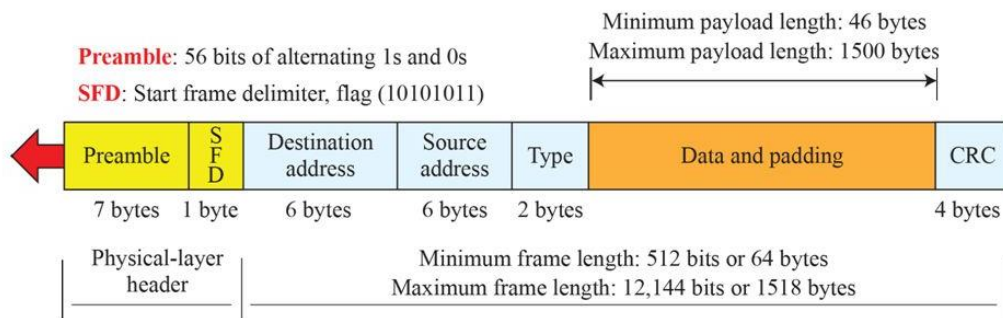
#### 2) Multicast:

One sender multiple specified receivers.

#### 3) Broadcast:

One sender to multiple receivers.

### Traditional Ethernet Frame Format: -



## ➤ Wireless LAN (WLAN): -

- A WLAN is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN), within a limited area such as home, computer, lab, campus, etc. this gives users the ability to move around within the area and still be connected to the network. Wireless LAN's use electromagnetic waves (radio or infrared) to communicate information from one point to another without relying on any physical medium. The IEEE 802.11 group of standards define the technology for wireless LANs, for path sharing, 802.11 standard uses the ethernet protocol and CSMA/CA.
- Examples: - Motorola's ALTAIR  
NCR's Wave LAN

## Advantage's: -

### I. Flexibility: -

Within radio coverages, nodes can communicate without further restriction. Radio waves can penetrate through walls, so sender and receiver can be placed anywhere.

### II. Cost: -

Low cost of installation & maintained.

### III. Easy to use & implement,

### IV. Transfer Rate:

Data transfer speed up to 11mbps and range is about 300m.

## ➤ Bluetooth: -

Bluetooth is a radio frequency wireless technology that allows systems to connect to peripherals over a distance of up to 10 meters away. Bluetooth is more flexible than infrared because it will automatically connect to other Bluetooth devices and does not depend on line of sight. This is a popular technology used by handheld devices to connect to other networking components.

Bluetooth is less susceptible to interference because it uses spread-spectrum frequency hopping, which means that it can hop between any of 79 frequencies in the 2.4 GHz range. Bluetooth hops between frequencies 1600 times per second and provides a transfer rate of up to 1 Mbps.

Bluetooth is a popular technology with handheld devices such as PDAs and cell phones. Bluetooth is popular with these devices so that users can use their wireless headsets with their cell phones and talk "hands free."

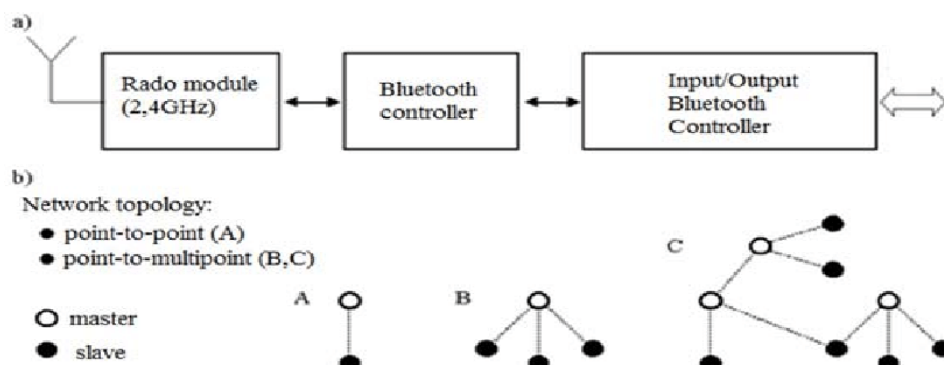


Fig: Bluetooth connection



### ➤ Wi-Fi (Wireless Fidelity): -

- Wi-Fi Stand for Wireless Fidelity. It is based on the IEEE 802.11 family standards and is primarily a LAN technology designed to provide in-building broad cast coverage. Wi-Fi offers remarkably higher peak data rate than 3G systems. One significant advantages of Wi-Fi over Wi-Max is its wide availability of terminal devices. A vast majority of laptops shipped today have a built - in Wi-Fi interface. Nowadays Wi-Fi interfaces are being built in cellular phones, cameras and media players etc.

The Wi-Fi standards define a fixed channel bandwidth of 25 MHZ for 802.11b and 20MHZ for either 802.11a or 802.11g networks. Radio signals are the keys which makes Wi-Fi networking possible. These radio signal transmitted from Wi-Fi antenna are picked up by Wi-Fi receiver, such as computer and mobile phones that are equipped with Wi-Fi card. These Wi-Fi cards reads the signals and thus create an internet connection between the user, and the network.

### ➤ Wi-Max (Worldwide interoperability for Micro wave Access): -

- Wi-Max is one of the hottest broadband wireless technology's around today Wi-Max but at higher speed over general distances and for a greater number of users. Wi-Max was initially designed to provides 30 to 40 Mbps, data rates, with 2011 updates providing up-to 1G bits for fixed stations. Wi-Max has along range about 100m whereas Wi-Max network can reach about 50-90 km. Wi-Max is a family of wireless broadband communication standards based on the IEEE 802.16 set of standards which provides multiples physical layer and MAC option.

## UNIT - 5

### Physical layer and Data Layer

#### ➤ Introduction to Physical Layer: -

- Physical layer in the OSI Model plays the roles of interacting with actual hardware and signaling mechanism. Physical layer is the only layer of OSI network Model which actually deals with the physical connectivity of two different stations. This layer defines the hardware equipment, cabling, wiring, frequencies, pulses used to represent binary signals etc.
- Physical layer provides its services to data-link layer. Data-Link layer hands over frames to physical layers. Physical layer converts them to electrical pulses, which represent binary data. The binary data is then sent over the wired or wireless media.

#### ➤ Signals: -

When data is sent over physical medium, it needs to be first converted into electromagnetic signals. Data itself can be analog such as human voices or digital such as files on the disk. Both analog and digital data can be represented in digital or analog signals.

#### ➤ Digital Signals: -

Digital Signals are discrete in nature and represent sequence of voltage pulses. Digital signals are used within the circuitry a computer system.

### ➤ Analog Signals: -

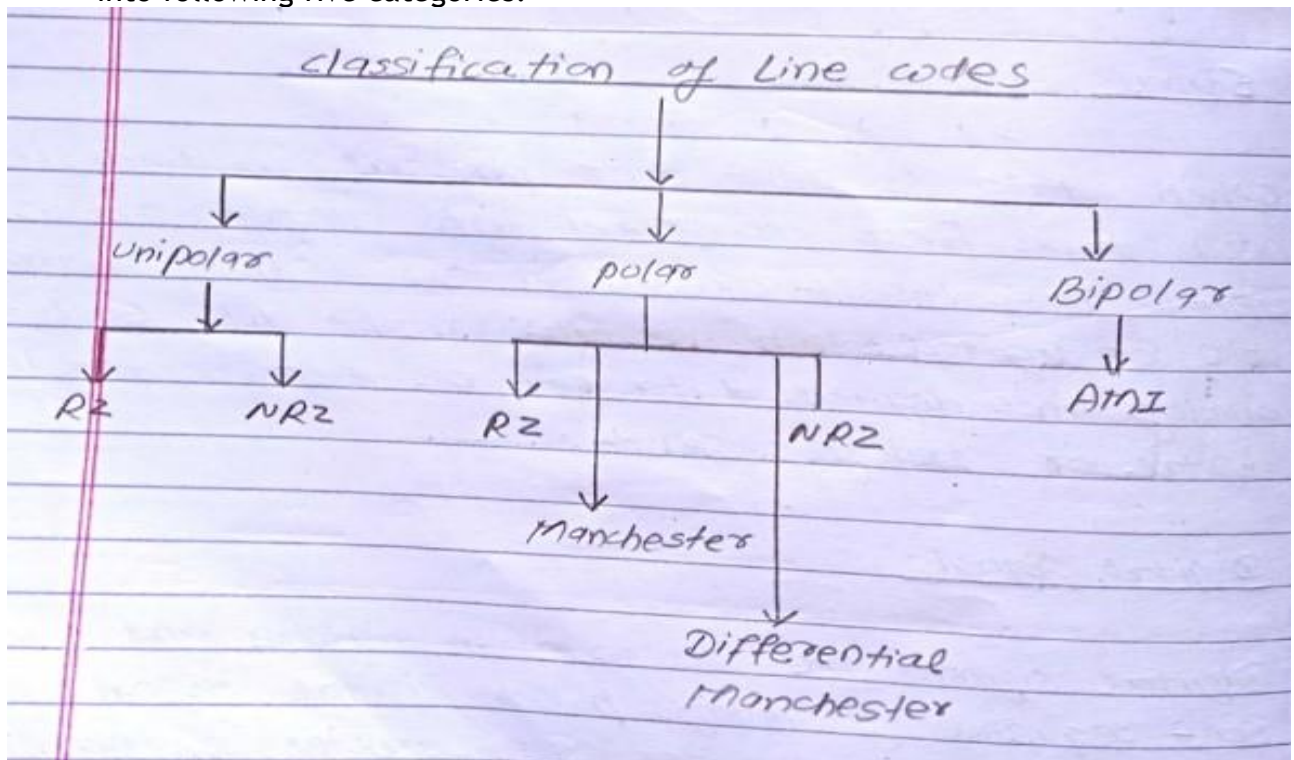
Analog Signals are in continuous waves from in nature and represented by continuous electromagnetic waves.

### ➤ Line Coding formats

#### ❖ Line Coding: -

Line coding is the process of converting digital data to digital signals. By this technique we convert a sequence of bits to a digital signal. At the sender side, digital data are encoded into a digital signal and at the receiver side the digital data are recreated by decoding the digital signal.

We assume that data, in the form of text, numbers, graphical images, audio, or video, are stored in computer memory as sequences of bits. Line coding converts a sequence of bits to a digital signal. Line coding scheme can be categorized into following five categories:



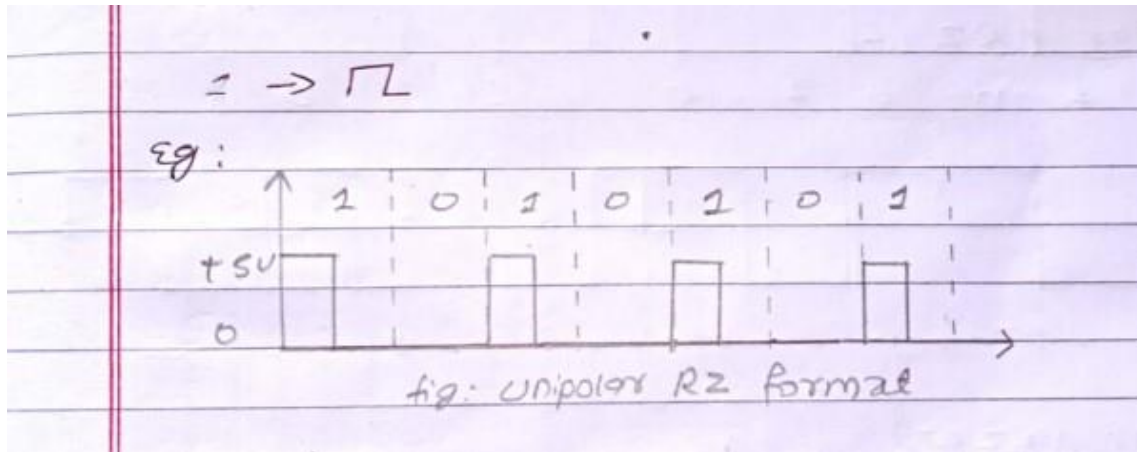
### 1. Unipolar codes: -

Unipolar codes use only one voltage level other than zero. Hence, the encoded signal will have either +V voltage value or 0.

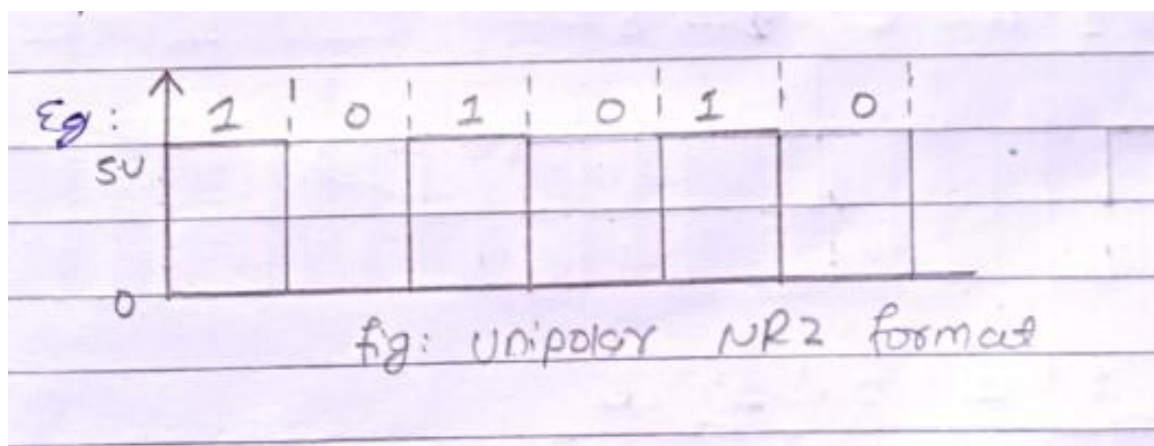
#### i. Unipolar RZ format (Return to Zero): -

In this type of unipolar signaling, a High in data, though represented by a Mark pulse, its duration  $T_0$  is less than the symbol bit duration. Half of the bit duration remains high but it immediately returns to zero and shows the absence of pulse during the remaining half of the bit duration.





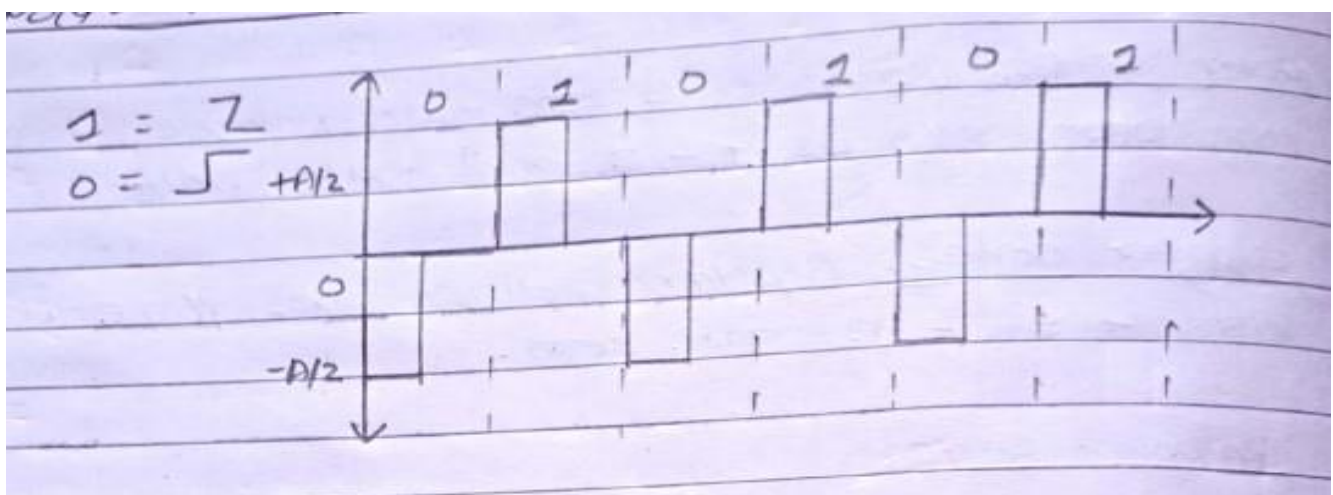
## ii. Unipolar NRZ Format (Non-Return to Zero): -



## 2. Polar Codes: -

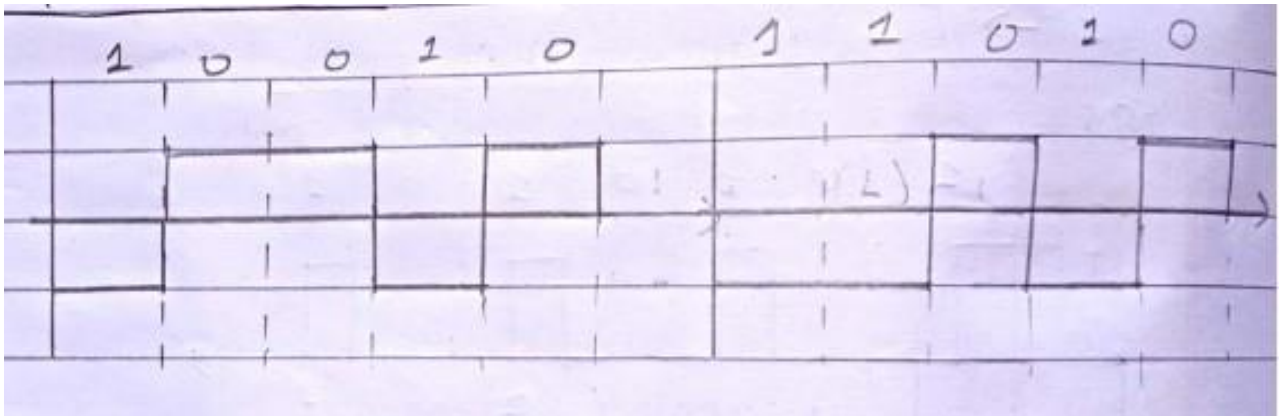
Polar code uses two voltage levels other than zero such as  $+A/Z$  and  $-A/Z$  volts.

### i. Polar RZ format: -

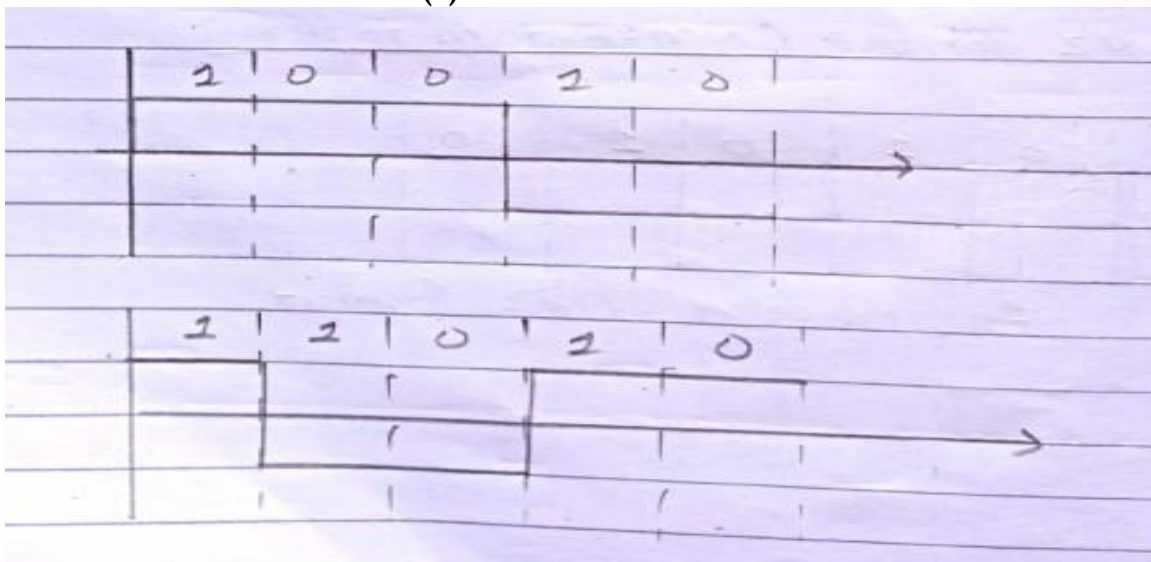


## ii. Polar NRZ Format

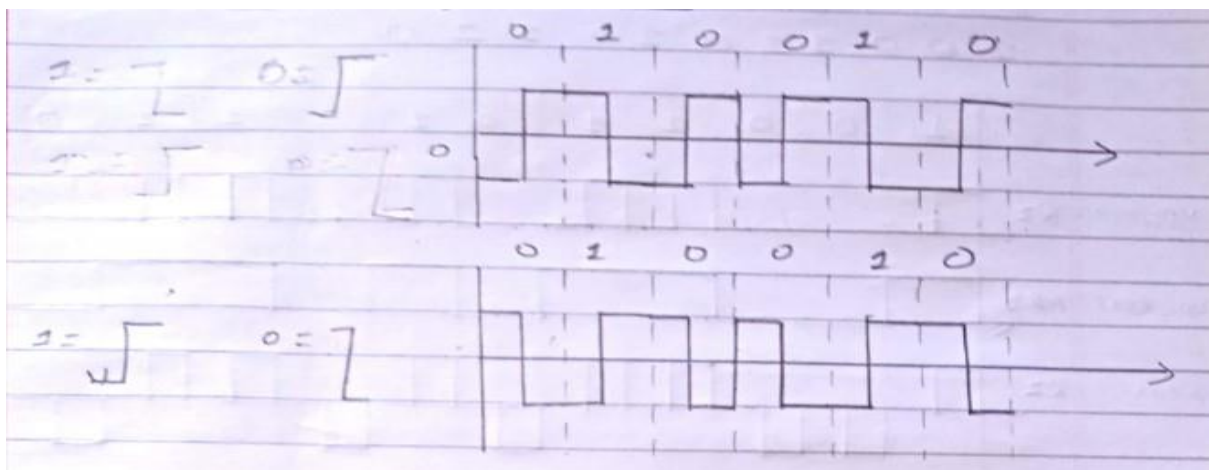
### a. Polar NRZ (L): -



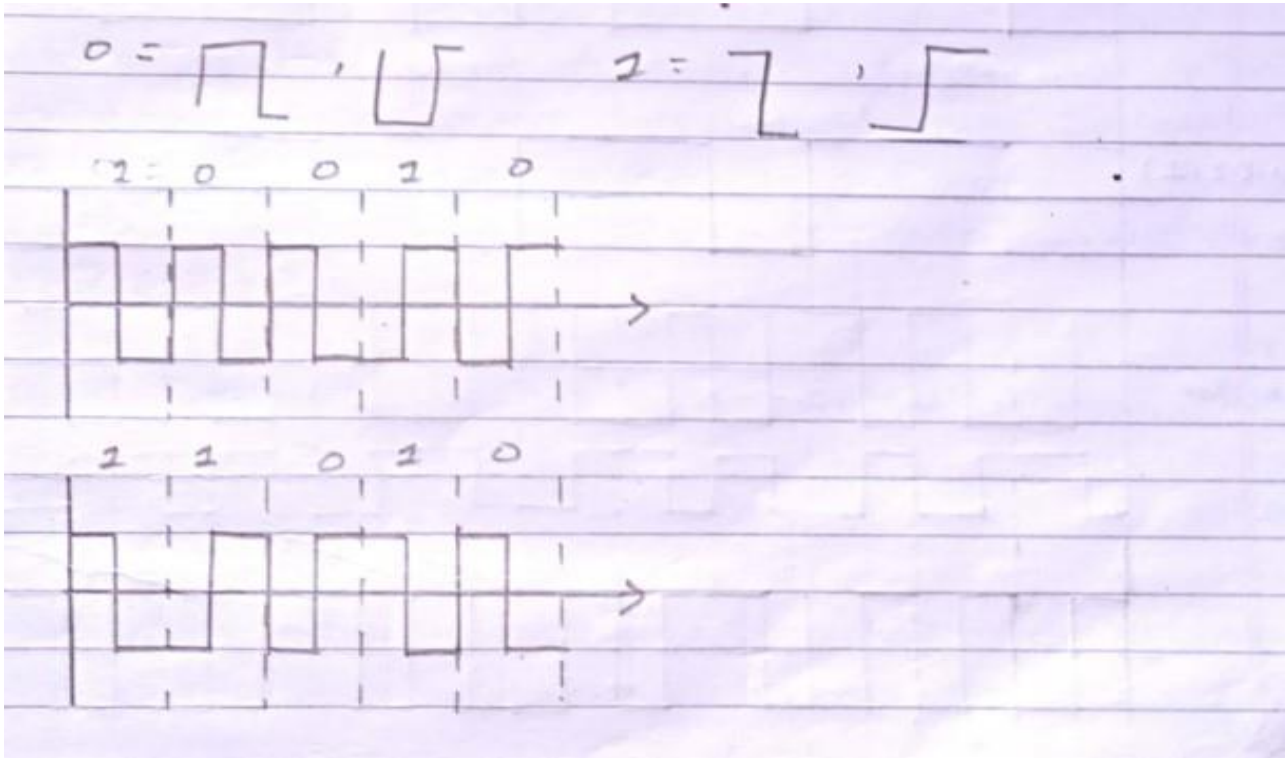
### b. Polar NRZ (I): -



## iii. Manchester Coding Format: -

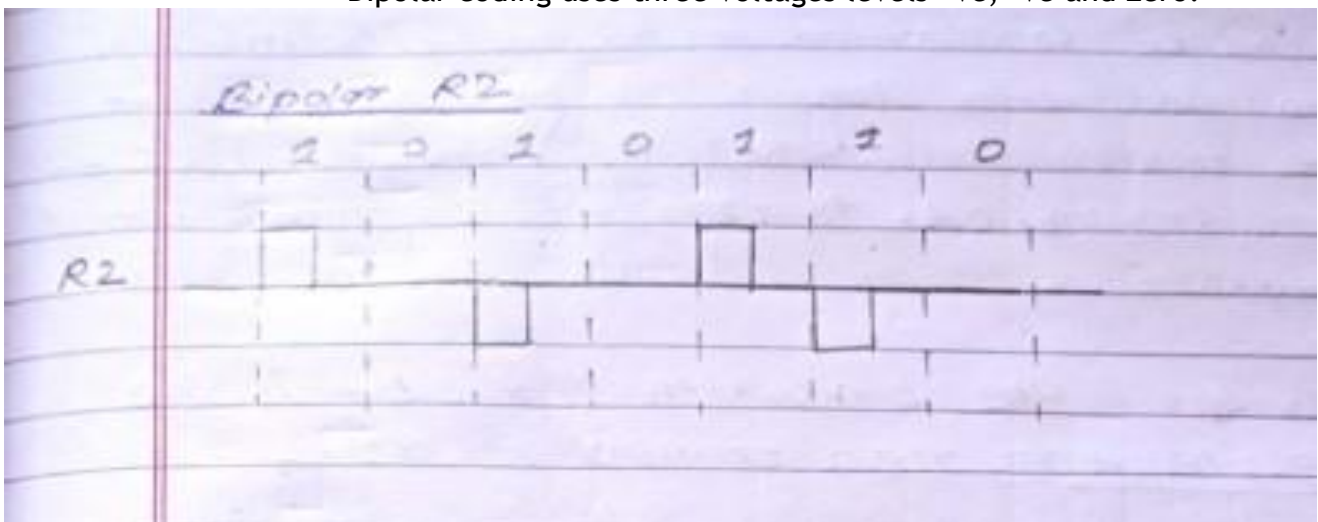


## iv. Polar Differential Manchester Coding: -



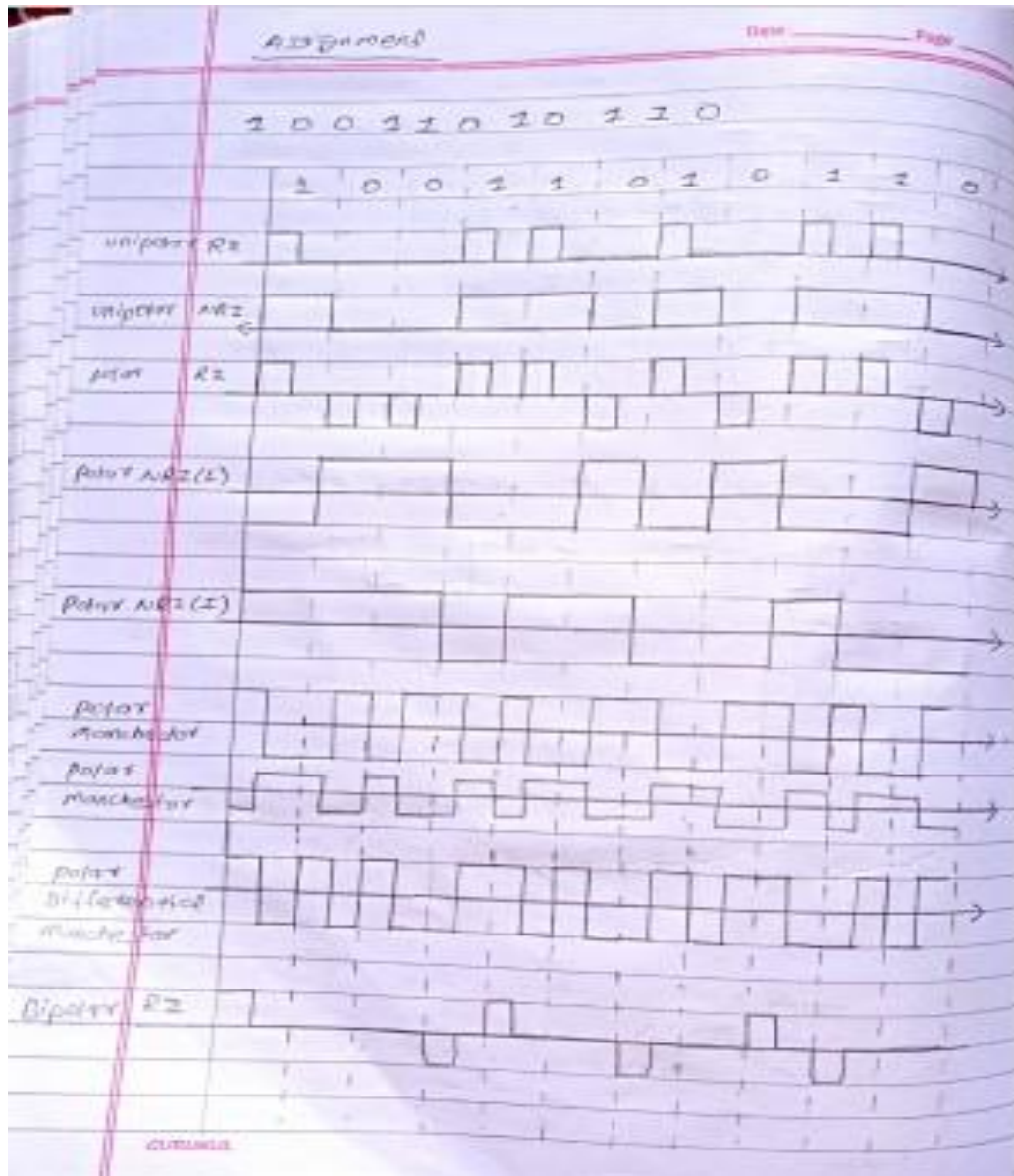
## 3. Bipolar Codes: -

Bipolar coding uses three voltages levels +ve, -ve and zero.



## ➤ Assignment: -

I. 10011010110



### ➤ Channel Bandwidth (Capacity): -

- Network bandwidth is a measurement indicating the maximum capacity of a wired or wireless communication links to transmit data over a network connection in a given amount of time. Typically, bandwidth is represented in the number of bits, kilobits, megabits or giga bits that can be transmitted in 1 second.

### ➤ Propagation Time and Transmission Time: -

#### ▪ Transmission Delay: -

- The time to transmit a packet from the host to the transmission medium is called transmission delay.





For example, if bandwidth is 1 bps (every second 1 bit can be transmitted on to the transmission medium) and data size is 20 bits then what is the transmission delay? If in one second, 1 bit can be transmitted. To transmit 20 second would be required.

Let B bps is the bandwidth and L bit is the size of the data then transmission delay is,

$$T_t = L/B$$

- This delay depends up on the following factors: -
  1. If there are multiple active sessions, delay will become significant.
  2. Increasing bandwidth decreases transmission delay.
  3. MAC protocol largely influences the delay if link is shared among multiple devices.
  4. Sending and receiving a packet context switch in the operating system, which takes finite time.

#### ■ Propagation Delay: -

- After the packet is transmitted to the transmission medium, it has to go through the medium to reach the destination. Hence the time taken by the last bit of the packet to reach the destination is called propagation delay.



Fig of Propagation Delay.

#### ○ Factors affecting propagation delay: -

##### 1. Distance: -

It takes more time to reach the destination if the distance of the medium is longer.

##### 2. Velocity: -

If the velocity(speed) of the signal is higher, the packet will be received faster.

$$T_p = \text{Distance} / \text{Velocity}$$

### ➤ Introduction To Data Link Layer and Its Issues: -

#### • Data link layer and its issues

- The data link layer is responsible for maintaining the data link between two hosts or nodes.
- The data link layer is divided into two sub-layers

##### a. Logical Link Control: -

- Provides the logic for the data link, thus it controls the synchronization, flow control and error checking functions of the data link layers. Functions are: -
  - i. Error Recovery.
  - ii. It performs the flow control operations.
  - iii. User addressing.

#### b. Media Access Control (MAC): -

- Its controls the flow and multiplexing for transmission medium. Transmission of data packets is controlled by this layer. This layer is responsible for sending the data over the network interface card.
- Functions are: -
  - i. To perform the control of access to media.
  - ii. It performs the unique addressing to stations directly connected to LAN.
  - iii. Detection of errors.

### ➤ Design issues with Data Link Layer

#### • Services provided to the network layer: -

- The data link layer act as a service interface to the networking layer. The principal services are transferring data from network layer on sending machine. This transfer also takes place via DDL (Dynamic Link Library).

#### a. Frame Synchronization: -

- The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frame can be recognized by the destination machine.

#### ▪ Flow Control: -

- Flow Control is done to prevent the flow of data frame at the receiver end. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

#### ▪ Error Control: -

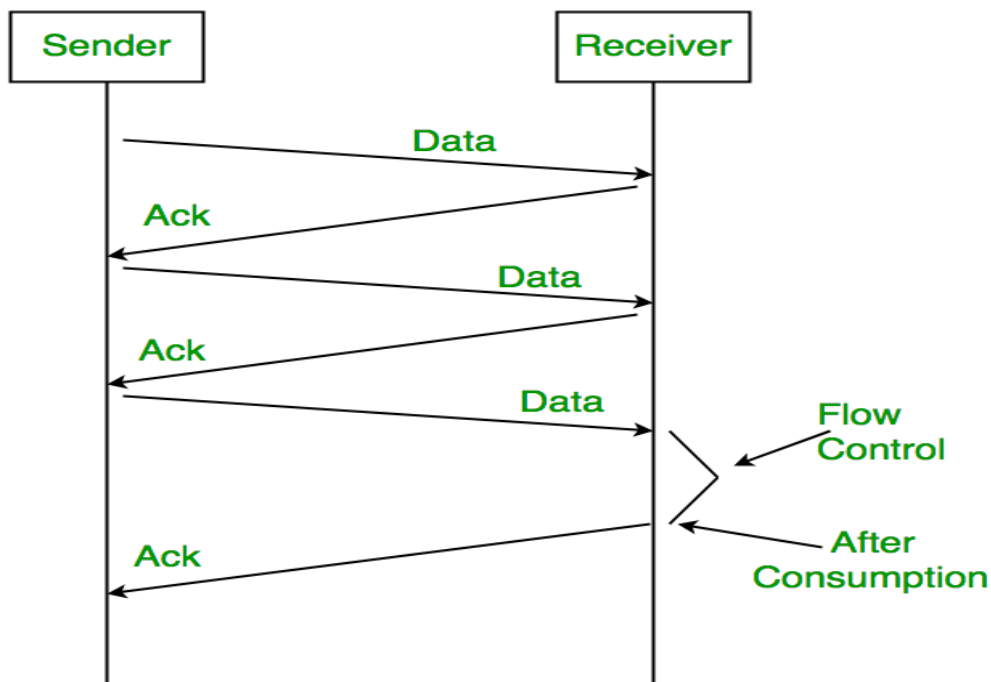
- Error Control is done to prevent duplication pf frames. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

### ➤ Flow control: -

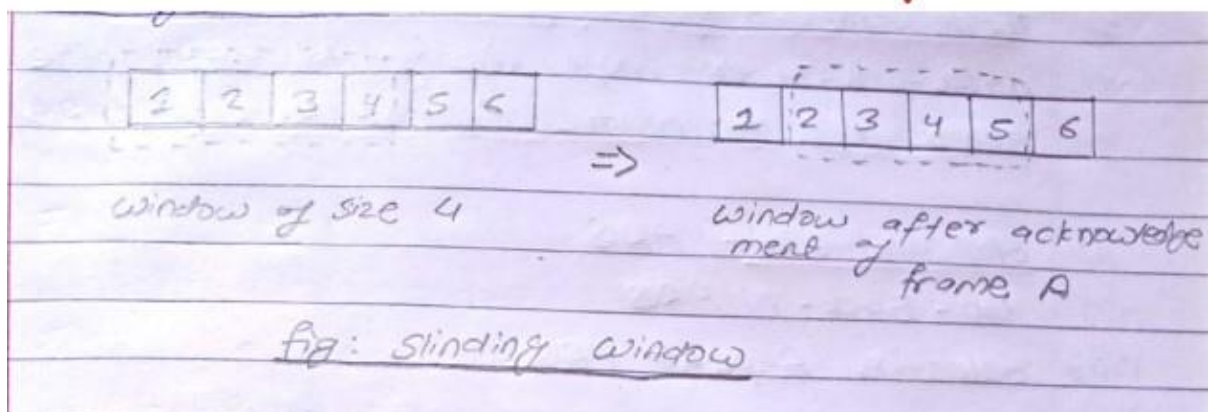
- When a data frame is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is sender sends at a speed on which the receiver can process and accept the data. What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded and data might be lost.
- Two mechanisms for Flow control are: -
  1. Stop and wait
  2. Sliding window

## 1. Stop and wait: -

- This Flow control mechanism Forces the sender after transmitting a data frame to stop and wait until the acknowledgment of the data. Frame is received. The problem with stop and wait is that only one frame can be transmitted at a time and that often leads to inefficient transmission, because until the sender receives the ACK it cannot transmit any new packet. During this time, both the sender and receiver are unutilized.



## 2. Sliding window: -



- In this flow control mechanism, both sender & receiver agree on the number of data frames called window after which the acknowledgement should be sent. Sender slides its window on receiving the acknowledgements for the sent frames. As we learned, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

## ➤ Error Control: -

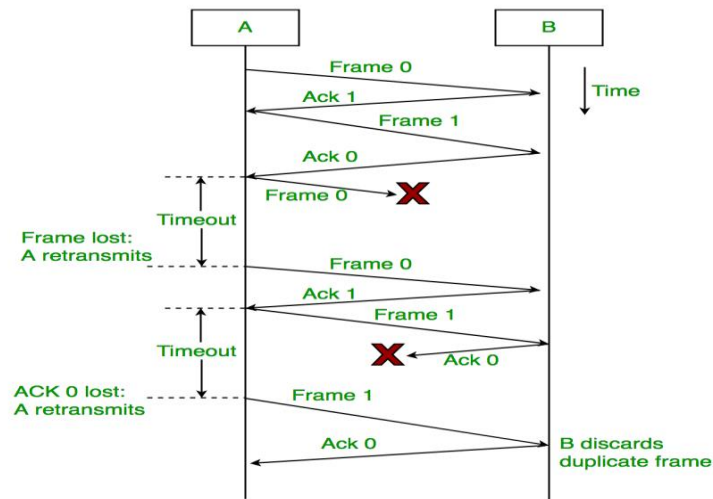
- When a data frame is transmitted, there is a probability that the data frame may be lost in the transit or it is received corrupted. In both the cases, the receiver doesn't



receive the corrupt data frame and sender doesn't know anything about any loss. In such cases, both sender and receiver are equipped with same protocol which help them to detect transit errors such as loss of data frames. Hence either the sender transmits the data frames or the receiver requests to resend the previous data frames.

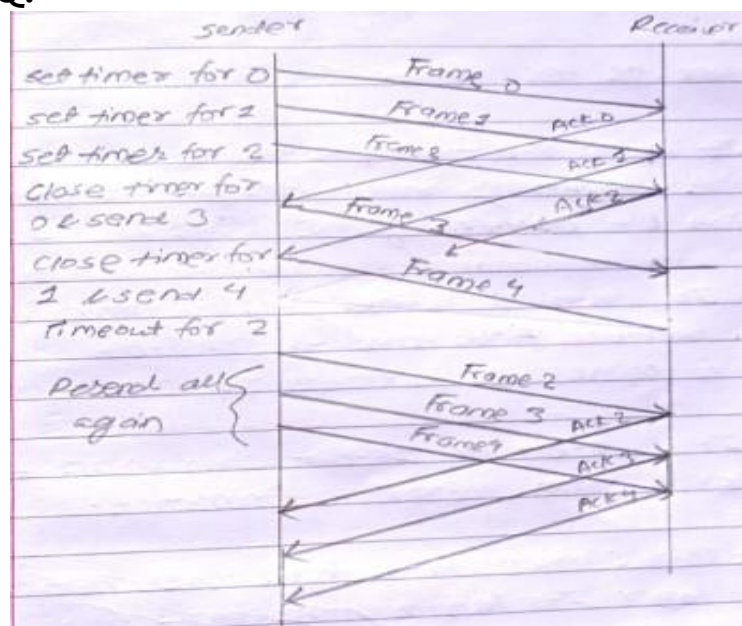
- There are 3 types of techniques available which data link-layer may deploy to control the errors by automatic repeat Request (ARQ).
  - i. Stop and Wait ARQ.
  - ii. Go- Back-N ARQ.
  - iii. Selection Repeat ARQ

i. Stop & Wait ARQ: -



- The following transition may occur in stop and wait ARQ: -
  - i. When a frame is sent, the sender sends the timeout counter.
  - ii. If the ack of the frame comes in time, the sender transmits the next frame in queue.
  - iii. If Ack doesn't come in time, the sender assumes that either the frame or the acknowledgement is lost in transit. Sender retransmits the frame and starts the time out counter.
  - iv. If a negative acknowledgement (NACK) is received, the sender retransmits the frame.

## ii. Go-Back -NARO: -



- Send no. of frames per window.
- If not received ack, sends all frames from not received mistakes point.

iii. Selective sends only not received frames: -

## ➤ Data Link layer Protocols (HDLC, PPP)

a. High level Data Link control (HDLC): -

### ○ HDLC Frame: -

- HDLC is a bit-oriented protocol where each frame contains up to six fields. The structured varies according to the types of frames.
- The fields of HDLC Frames are: -

#### i. Flag: -

It is an 8-bit sequence that makes the beginning and end of the frames. The bit pattern of the flags is 01111110.

#### ii. Address: -

It contains address of the receiver. The address field consists of 8-bit hence, it is capable of addressing -256 address.

#### iii. Control: -

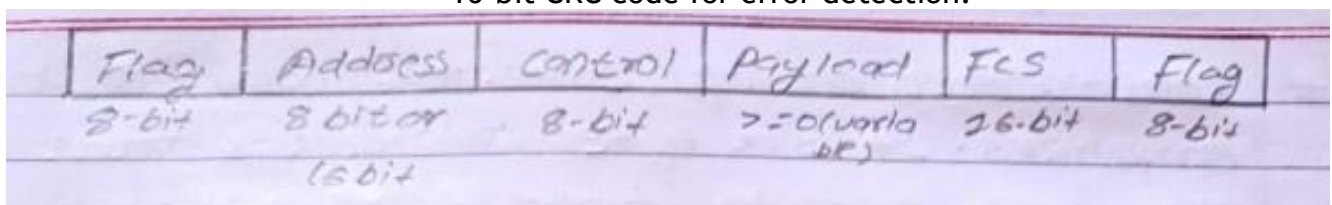
It is 8-bits or 16-bits containing flow and error control in formation.

#### iv. Payload: -

This carries data from the network layer. Its length may vary from one network to another.

#### v. FCS (Frame Check Sequence): -

16-bit field used for detecting of error in the address, control and information field. It is nothing else but a 16-bit CRC code for error detection.



### Information Field

- Only in information and some unnumbered frames
- Must contain integral number of octets
- Variable length

### Frame Check Sequence Field

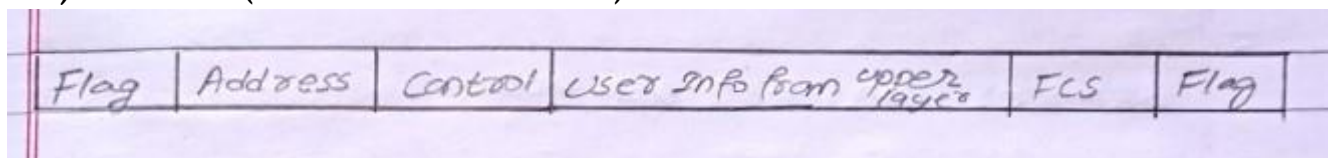
- FCS
- Error detection
- 16 bit CRC
- Optional 32 bit CRC



84

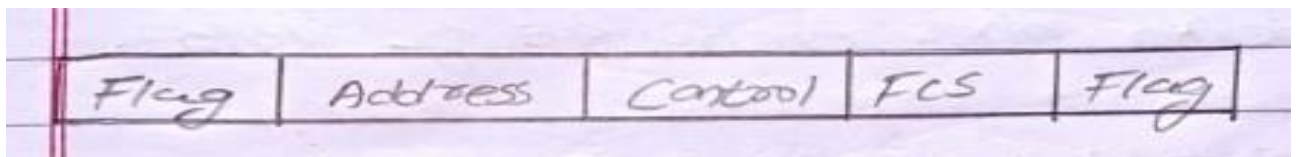
## ➤ Frame Types

### 1) I-Frame (Information Frame): -



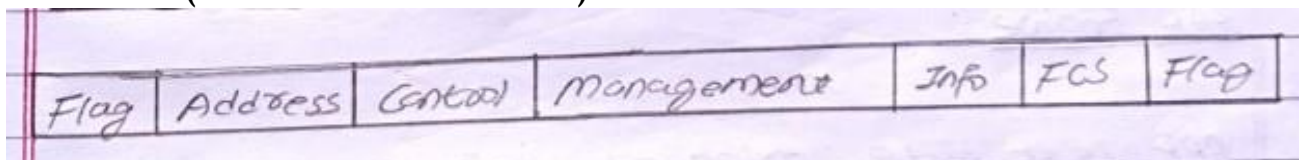
- It is supposed to carry user information (Data) From the Network Layer.

### 3) S-Frame (Supervisory Frame): -



- An S-Frame doesn't contain any information field. These frames are used for flow & error control.

### 4) U-Frame (Unnumbered Frame): -



- These frames are used for exchanging the session (link) management and control information between the communication devices.

## ➤ Point-to-Point Protocol (PPP): -

- PPP is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a bytes-oriented protocol, that is widely used in broad band communications having loads and high speeds. Since H is a data link layer protocol, data is transmitted in frames.

- Services provides by PPP: -
  - i. Defining the frame format of the data to be transmitted.
  - ii. Defining the procedure of establishing link between 2 points and exchange of data.
  - iii. Stating authentication rules of the communicating devices.
  - iv. Supporting a variety of network layer protocols by providing a ranger of services.

### o PPP Frame: -

- PPP is a byte-oriented protocol where each field of the frames is composed of one or more bytes. The fields of a PPP frames are: -

#### i. Flag 1: -

1 byte that makes the beginning and end of the frame. The bit pattern is 01111110.

#### ii. Address: -

1 byte which is set to 11111111 in case of broad cast.

#### iii. Control: -

1 byte set to a constant value of 11000000.

#### iv. Protocol: -

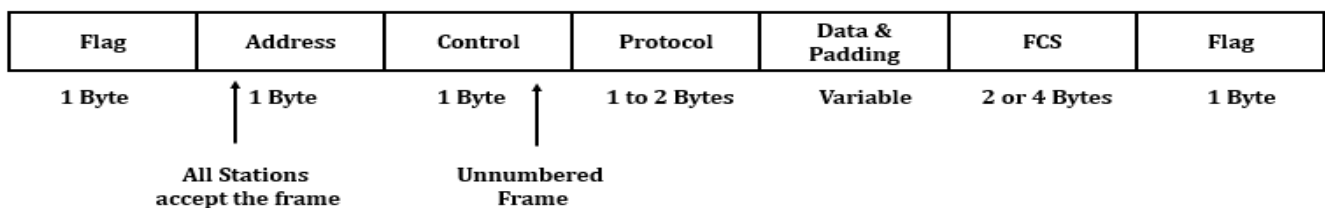
1 or 2 byte that define the types of data contained in payload field.

#### v. Payload: -

This carries data from the network layer max length 1500 bytes.

#### vi. FCS: -

It is 2 bytes or 4 bytes frames check sequence for error detection.



# Network Layer

## Unit - 6

### ➤ Inter-Working: -

- Internetworking is combined of 2 words, inter and networking which implies an association between totally different nodes or segments.
- Once a network communication with another network having constant communication procedures it called inter-networking. Internetworking was designed to resolve the matter of delivering a packet of information through many links.
- Internetworking is the process of connecting different networks by using intermediate devices such as routers or gateways devices. Internetworking using different routing protocols.
- There are chiefly 3 unit of Internetworking: -
  - i. Extranet.
  - ii. Intranet.
  - iii. Internet.

#### i. Extranet: -

- It is a networking of the internetworking that is restricted in scope to one organization or entity.
- From time to time, an application that has been built for the company's intranet and used by internal employees will need to be extended to select business partners or customers. If you extend your intranet out to select business partners or customers, you have created an extranet. An extranet cannot be used by anyone else external to the company except for those selected individuals. Figure 1-3 displays the basic configurations of Internet, intranet, and extranet.

#### ii. Intranet: -

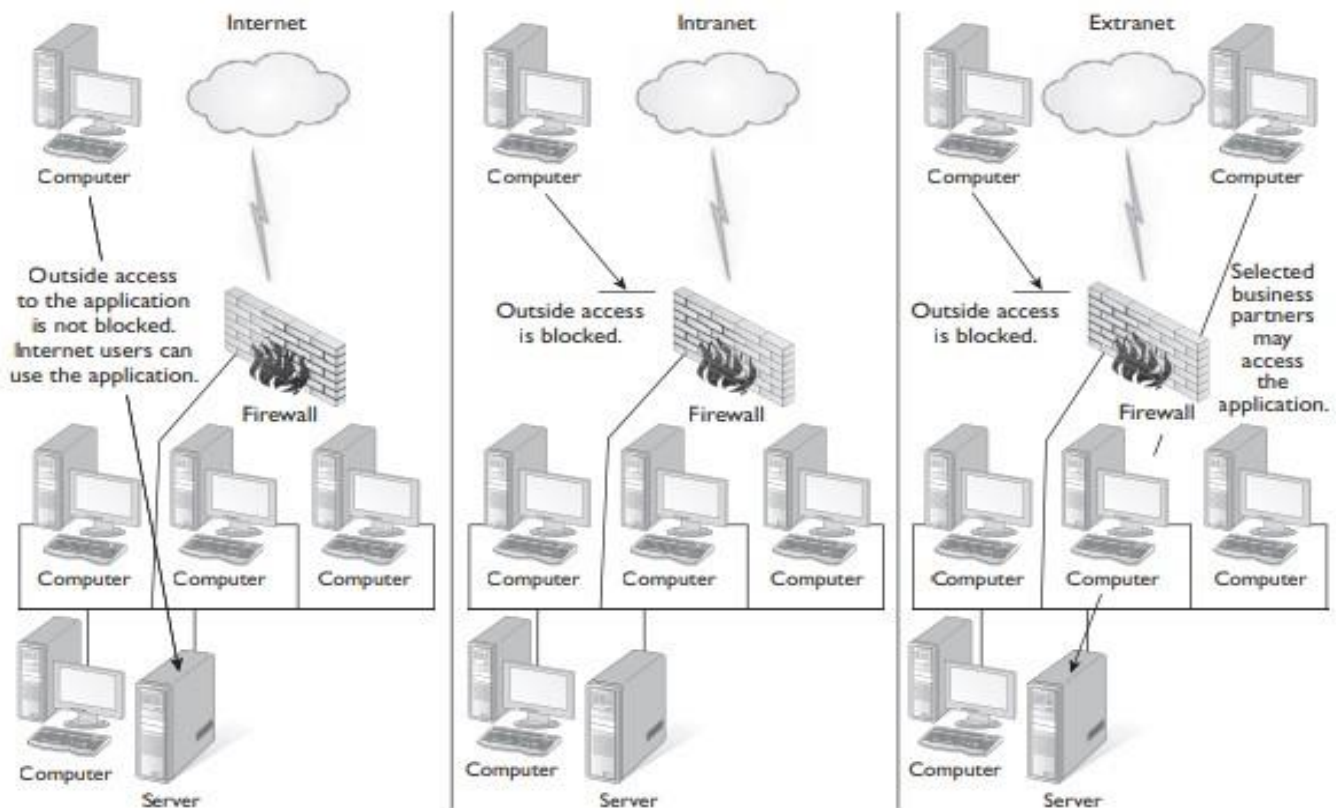
- This network is the internal network of a corporation or different enterprise. An outsized computer network can usually have its own internet server to supply to supply users with browse able data.
- An application is considered to be on the company's intranet if it is using Internet-type protocols such as HTTP or FTP but the application is available only within the company. The information on a company's intranet would not be accessible to persons on the Internet because it is not for public use. For example, a few years ago I was sitting with my banking officer going over my account and noticed that the bank had moved all of its customer account information to a web site and that the banking officer was using a web browser to retrieve my account details. Although the application was being used by a web browser, it was still an "internal" application meant only for banking officers.

#### iii. Internet: -

- A selected internetworking, consisting of a worldwide interconnection of governmental, academic public and personal networks.
- If you wish to expose information to everyone in the world, then you would build an Internet-type application. An Internet-type application uses Internet protocols such as HTTP, FTP, or SMTP and is available to persons anywhere on the Internet. We use the Internet and web applications as ways to extend who the application can reach. For

example, I no longer need to go to the bank to transfer funds. Because the bank has built a web site on the Internet, I can do that from the comfort of my own home.

**FIGURE 1-3** Visualizing the difference between Internet, intranet, and extranet



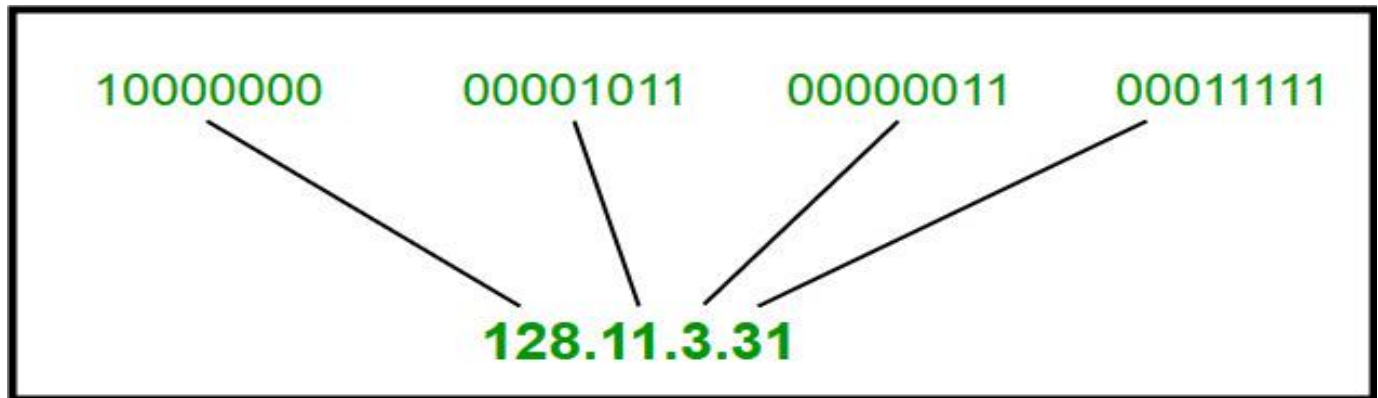
### ➤ IP Addressing: -

- IP Addressing is an address having information about how to reach a specific host, especially outside the LAN. An IP Address is a 32-bit unique address having an address space of  $2^{32}$ .
- The IP address is a 32-bit value that uniquely identifies the system on the network (or the Internet). An IP address looks similar in appearance to 192.168.1.15. There are four decimal values in an IP address separated by periods (.). Each decimal value is made up of 8 bits (1s and 0s), and there are four decimal values, so 8 bits times 4 equals the 32-bit address.

Since each of the decimal values is made up of 8 bits (for example, the 192), we refer to each of the decimal values as an octet. There are four octets in an IP address. It is very important to understand that the four octets in an IP address are divided into two parts—a network ID and a host ID. The subnet mask determines the number of bits that make up the network ID and the number of bits that make up the host ID. Let's see how this works.

- Dotted Decimal Notation: -





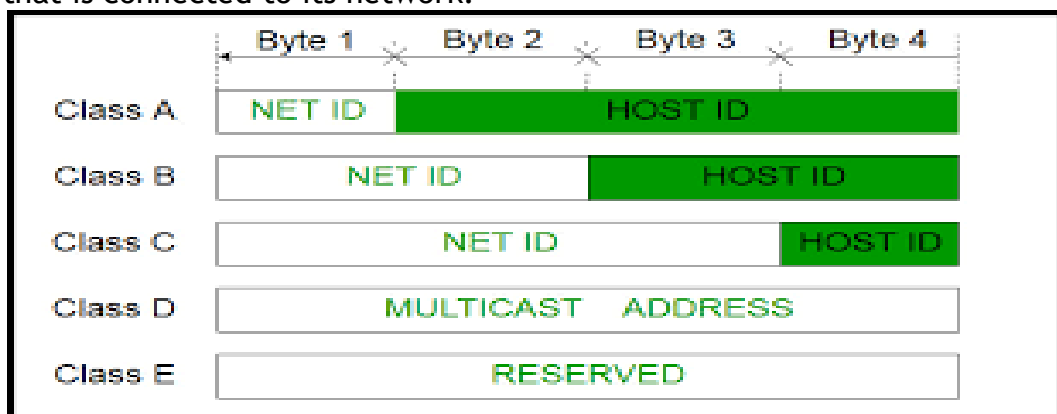
- Some Points to be noted about dotted decimal notation: -
  - I. The value of any segment (Bytes) is between 0 and 255 (Both included).
  - II. There are no zeros preceding the value in any segment (054 is wrong, 54 is correct).

### ➤ Classful Addressing: -

- The 32-bit IP address is divided into five sub-classes. These are: -
  1. Class-A ranges from 0 to 127
  2. Class-B ranges from 128 to 191
  3. Class-C ranges from 192 to 223
  4. Class-D ranges from 224 to 239
  5. Class-E ranges from 240 to 255

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purpose respectively. The order of bits in the first 0 del determine the classes of IP address.

- IP V4 Address is divided into two parts: -
  1. Network ID
  2. Host ID
- The class of IP address used to determine the bits used for network ID and host ID and the number of total networks and host ID and the number of total networks and hosts possible in that particular Class. Each ISP or network administer assigns IP address to each device that is connected to its network.



### 1. Class A: -

- IP address belonging to class A are assigned to the network that contain a large number of hosts.
- The network ID is 8 bits long.
- The host ID is 24 bits long.
- The higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used



to determine the host in any network. The default subnet mask for class A is 255.x.x.x. Therefore, class A has a total of:

$2^7 - 2 = 126$  network ID (Here 2 address is subtracted because 0.0.0.0 and 127.x.y.z are special address).

$2^{24} - 2 = 16,777,214$  host ID

- IP Address belong to Class A ranges from 1.x.x.x - 126.x.x.x

**Class A:**

0	Network ID	Host ID
---	------------	---------

**Very large Network**  
( $2^{24}$  hosts !)

## 2. Class B: -

- IP address belonging to class B are assigned to the network that ranger from medium-sized to large-sized networks.
- The network ID is 16 bits long.
- The host ID is 16 bits long.
- The higher order bits of the first octet of IP addresses of Class B are always set to 10. The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network. The default sub-net mask for class B is 255.255.x.x Class B has a total of:

$2^{14} = 16384$  network address

$2^{16} - 2 = 65534$  host address

- IP Address belonging to class B ranges from 128.0.x.x - 191 - 255.x.x.x

**Class B:**

1	0	Network ID	Host ID
---	---	------------	---------

**Medium size Network**  
(Most popular !!!)

## 3. Class C: -

- IP address belong to Class C are assigned to small-sized network.
- The network ID is 24 bits long.
- The host ID is 8 bits long.
- The Higher order bits of the first octet of IP address of class c are always set to 110. The remaining 21 bits are sued to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:

$2^{21} = 2097152$  network address

$2^8 - 2 = 254$  host address

- IP addresses belonging to class c ranges from 192.0.0.x - 233.255.255.x

**Class C:**

1	1	0	Network ID	Host ID
---	---	---	------------	---------

**Small Network**

## 4. Class D: -

- IP address belonging to class D are reserved for multi-casting bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.
- Class D does not possess any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 - 239.255.255.255

**Class D:**

1	1	1	0
---	---	---	---

<b>Multicast Group ID</b>
---------------------------

**Multicast Address**

## 5. Class E: -

- IP addresses belonging to class E are reserved for experimental and research purpose. If addresses of class E ranges from 240.0.0.0 - 255.255.254. This class doesn't have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.

**Class E:**

1	1	1	1
---	---	---	---

--

**Reserved (unused)**

### ➤ Private IP Address: -

Private IP Address of a system is the IP address which is used to communicate within the same network. Using private IP data or information can be sent or received within the same network.

### ➤ Public IP Address: -

Public IP address of a system is the IP address which is used outside communicate outside the network. Public IP address is assigned by the ISP (Internet Service provides).

### ➤ Difference Between Private and Public IP Address: -

S. N	Private IP Address	Public IP Address
1	Scope is local.	Scope is global.
2	It is used to communicate within the network.	It is used to communicate outside the network.
3	It works only in LAN.	It is used to get internet service.
4	It is used to load network operating system.	It is controlled by ISP.
5	It is available in free of cost.	It is not free of cost.
6	Private IP address of a system is the IP address which is used to communicate within the same network.	Public IP addresses of the systems connected in a network differ in a uniform manner.
7	10.0.0.0 – 10.255.255.255; 172.16.0.0 – 172.31.255.255; 192.168.0.0 – 192.168.255.255	Any number not included in the reserved private IP address range

	Example: 10.11.12.13	Example: 8.8.8.8.
--	----------------------	-------------------

### ➤ Subnet Mask: -

A subnet mask is a 32-bit number that masks an IP address and divides the IP address into network address and host address. Subnet mask is made by setting network bits to 1's and host bits to 0.

bits to 0.	First bit of first octet
1, N.H.H.H	0 1-126
2, Host per Net ( $2^8, 16, 24, 32-2$ )	10 126-191
3, Net Range	110 192-223
4, Default subnet mask	1110 224-239
N → 1	- 240-255
H → 0	
	↓
	224.0.0.0 - 191.255.0.0

### ➤ Subnetting: -

- Subnetting is the practice of dividing a network into two or more smaller networks. It increases routing efficiency, enhances the security of the network and reduces the sizes of the broadcast domain. The smaller networks are called as subnets. Subnets are designed over the internet. The subnetting process allows the administrator to divide a single class C network into subnetwork. The subnet can be subnetted again into sub-nets.

#### ■ Classless Inter Domain Routing / Classless Addressing: -

Drawbacks of classful Addressing are: -

- Classful addressing is a waste of address space i.e., users with more than 254 hosts had been assigned a B class.
- A route to reach classful subnet must be specified separately. These drawbacks led to a better solution called CIDR which provides the flexibility of borrowing bits of host part of the IP address and using them as network bits.

CIDR IP addresses are composed of two sets of numbers. The network address is written as a prefix (192.168.1.0). The second part is the suffix which indicates how many bits are in the entire address used for network portion (24). That is CIDR IP address would look like (192.168.1.0/24). The above part of the address the first 24 bits are for host address.

↑ Host + Net Address in same bit
(192.168.1.0-255)/24
Network address
↳ Bits used for Net (only representation)

## ➤ Subnetting Numerical: -

### 1. Divide the network address 192.168.1.0/24 into a subnet.

Soln:

Given address is 192.168.1.0/24. It is a class C address because it uses 24-bits for network and 8-bits for host field.

Now, no. of subnets =  $2^n$ , where 'n' is the number of bits that are shifted from host bit to network bit.

According to question

No. of subnets = 4

$$2^n = 4$$

$$2^n = 2^2$$

$$n = 2 \text{ (i.e./26)}$$

So, subnet mask for the subnets will be

11111111.11111111.11111111.11000000 = 255.255.255.192

Therefore, no. of host per subnet =  $2^6 - 2 = 62$ .

no. of host bits = 6

no. of IP address per subnet =  $2^6 = 64$

For Subnet 1

- Network address = 192.168.1.0/26
- Range of Host address = 192.168.1.1/26 - 192.168.1.62/26
- Broadcast Address = 192.168.1.63/26
- Subnet mask = 255.255.255.192

For Subnet 2

- Network address = 192.168.1.64/26
- Range of Host address = 192.168.1.65/26 - 192.168.1.126/26
- Broadcast Address = 192.168.1.127/26
- Subnet mask = 255.255.255.192

For Subnet 3

- Network address = 192.168.1.128/26
- Range of Host address = 192.168.1.129/26 - 192.168.1.190/26
- Broadcast Address = 192.168.1.191/26
- Subnet mask = 255.255.255.192

For Subnet 4

- Network address = 192.168.1.192/26
- Range of Host address = 192.168.1.193/26 - 192.168.1.253/26
- Broadcast Address = 192.168.1.254/26
- Subnet mask = 255.255.255.192

### 2. An organization has four department A, B, C and D with 30, 16, 12, 25 computers respectively. Specify the range of IP address and

subnet mask for each department with minimum wastage of addresses pool 202.77.19.0/24

Soln: -

The starting IP address is 202.77.19.0/24. since, There are four departments we need 4 subnets.

For Department A

To support 30 computers, it will require 32 IP address

$$2^n = 31 \Rightarrow n = 5$$

So, we need 5 - bits for host field and remaining 27 bits will be used by network field.

Therefore:

- Network address = 202.77.19.0/27
- Range of Host address = 202.77.19.1/27 - 202.77.19.30/27
- Broadcast Address = 202.77.19.31/27
- Subnet mask = 255.255.255.224

For Department B

To support 16 computers, it will require at least 18 IP address i.e.,  $2^n < 18 < 25$

$$n = 5$$

So, we need 5 bits for host field i.e.,

Therefore:

- Network address = 202.77.19.32/27
- Range of Host address = 202.77.19.33/27 - 202.77.19.62/27
- Broadcast Address = 202.77.19.63/27
- Subnet mask = 255.255.255.224

For Department C

To support 12 computers, it requires at least 14 IP addresses. i.e.,  $2^n = 4$

So, we need 4 bits for host field i.e., /28

Therefore:

- Network address = 202.77.19.64/28
- Range of Host address = 207.77.19.64/28 - 207.77.19.78/28
- Broadcast Address = 207.77.19.79/28
- Subnet Mask = 255.255.255.240.

For Department D

25 computers

25 = 32 IP addresses

N = 5

25 - 2 = 30 Host IP address

Host bits used = 5 i.e., /27(32-5)

Therefore:

- Network address = 202.77.19.80/27
- Range of Host address = 207.77.19.81/27(130) - 207.77.19.111/27
- Broadcast Address = 207.77.19.110/27

- Subnet Mask = 255.255.255.224

### ➤ Routing Algorithm: -

- The main function of Net Layer is routing packets from the source machine to the destination machine. Routing is the process of forwarding of a packet in a network so that it reaches its intended destination.

A routing algorithm is a set of step-by-step operations used to direct internet traffic efficiently. When a packet of data leaves its source there are many different paths it can take to its destination. The routing algorithm is used to determine mathematically the best path to take.

### ❖ Properties: -

1. Correctness.
2. Simplicity.
3. Robustness.
4. Stability.
5. Optimality.

#### 1. Correctness: -

The routing should be done properly and correctly. So that packet may reach their proper destination.

#### 2. Simplicity: -

The routing should be done in a manner so that the over head is as low as possible.

#### 3. Robustness: -

The algorithm designed for routing should be robust enough to handle h/w & s/w failures.

#### 4. Stability: -

The routing algorithm should coverage quickly and should be stable under all possible circumstances.

#### 5. Optimality: -

The routing algorithms should be optional in terms of throughout and minimizing mean packet delays.

### ➤ Types of Routing: -

#### Static Vs Dynamic Routing

S. N	Static Routing	Dynamic Routing
1	It is manually configured.	It is automatically configured.
2	Routing locations in the routing table are hand typed.	Routing locations in the routing table are dynamically filled.

3	The router from source to destination are user defined.	Routes are updated according to the change in topology.
4	Only good for small network.	It is used in large networks.
5	It doesn't use complex routing algorithms (example: - flooding, shortest path algorithm).	It uses complex routing algorithms (examples: - Distance vector routing, link state routing).
6	Provides higher security.	Less secure due to broad casting & multicasting of packets.
7	No any routing protocols are used for static routing.	Routing Protocols such as RIP, OSPF, IGRP etc. are involved in the routing process.

### ➤ Interior & exterior routing/ intradomain and interdomain Routing: -

- A system having multiple host and routers which is controlled by a single administrator is known as autonomous system.
- Routing of packets within an autonomous system is known as interior routing / intradomain routing.
- Routing of packets between different autonomous systems is known as exterior routing / inter-domain routing.
- The protocol followed by packets during interior routing is interior gateways protocol (IGP).

### ➤ Introduction to IPv4 and IPv6

#### ❖ IPv6: -

- It is the most recent version of the IP. This new IP address is belong deployed to fulfill the need for more internet address.
- An IP address basically a 128-bit address that uniquely universally defines connection of host or a router to the Internet. IP address is unique.
- Introduced by IANA (Internet Assigned Numbers Authority).
- total of 4,294,967,296 unique IP addresses can be assigned to hosts.
- IP is like 2001:db8:1234::f350:2256:f3dd/64
- It supports Unicast. Telecast & Multicast.



- It doesn't have Classes like ipv4.

# KEY COMPARISONS

## Between IPv4 vs IPv6

	IPv4	IPv6
<b>Address</b>	32 bits (4 bytes)	128 bits (16 bytes)
<b>Packet Size</b>	576 bytes required, fragmentation optional	1280 bytes required without fragmentation
<b>Packet Fragmentation</b>	Routers and sending hosts	Sending hosts only
<b>Packet Header</b>	Does not identify packet flow for QoS handling	Contains Flow Label field that specifies packet flow for QoS handling
	Includes a checksum	Does not include a checksum
	Includes options up to 40 bytes	Extension headers used for optional data
<b>DNS Records</b>	Pointer (PTR) records, IN-ADDR.ARPA DNS domain	Pointer (PTR) records, IP6.ARPA DNS domain
<b>IP To MAC Tesolution</b>	Broadcast ARP	Multicast Neighbor Solicitation
<b>Local Subnet Group Management</b>	Internet Group Management Protocol (IGMP)	Multicast Listener Discovery (MLD)
<b>Broadcast</b>	Yes	No
<b>Multicast</b>	Yes	Yes
<b>IPSec</b>	Optional	Required

### ➤ Difference between IPv4 and IPv6: -

The Difference between IPv4 and IPv6 are listed below

S. N	IPv4	IPv6
1	IPv4 is a 32 - bit IP address.	IPv6 is 128 - bit IP address.
2	IPv4 is a numerical addition and is separated by a dot (.)	IPv6 is made up of hexadecimal characters and are separated by colon (:)
3	In the packet header, it has check sum filed.	In the packet header, it doesn't have checksum field.
4	Fragmentation of large packets is done by sending and forwarding routes.	Fragmentation of large packet is done by the sender (not routers).
5	Less secure as no encryption techniques are used.	More secure as IPSEC (Internet Protocol Security) is built into the IPv6 protocol.
6	Example: - 127.255.255.255	Examples: - 2001:odb8:85a3:0000:0000:8a2e:0370:7334

# Unit - 7

## Transport and Application

### ➤ Transport Layer Issues

#### 1. Congestion Control: -

- Congestion is a situation in which many sources over a network attempt to send data and the network buffers start overflowing due to which loss of packets occurs. As a result, retransmission of packets from the source increases the congestion further.

Transport layer provides different congestion control techniques to overcome this problem.

#### 2. Flow Control: -

- The transport layer provides a flow control mechanism between adjacent layers of the TCP/IP model. It can be implemented using different windowing techniques such as go back n, selective repeat etc.

#### 3. Quality of Service: -

- Quality of service can be implemented in other layers but its actual effect is felt in the TC. The transport service may allow the user to specify required acceptable and min values of various service parameters at the time of setting up a connection.

The Typical QoS parameters for TL are: -

##### a. Connection Establishment Delay: -

- The time difference between the instant at which a transport connection is requested and the instant at which it is confirmed is called as connection establishment delay. The shorter the delay the better is the service.

##### b. Through put: -

- It measures the no. of bytes of user data transferred per second measured over some time interval.

##### c. Protection: -

- This parameter provides a way to protect the transmitted data from being read or modified by some unauthorized parties.

##### d. Transmit Delay: -

- It is the time between a message being sent by the transmit user on the source machine and its being received by the transport user on the destination machine.

##### e. Residual Error Ratio: -

- It measures the no. of lost messages as a function of total messages sent. Ideally the value of this ratio should be zero & practically it should be small as possible.

$$\text{i.e., RER} = \frac{\text{Total Lost Message}}{\text{Total Sent Message}}$$

#### 4. Multiplexing / Demultiplexing: -

- Multiplexing allows simultaneous use of different applications over a network which is running on a host. The Transport Layer provides this mechanism which enables us to send packet stream from various application simultaneously over a network.

Similarly, DeMux is required at the receiver side to obtain the data coming from various processes.

#### 5. Data Integrity and Error Correation: -

- Transport Layer Checks for error in msg coming from application layer by using error detection codes, computing check sums, it checks whether the received data is corrupted or not & user the ACK and NACK services to inform the sender if the data has arrived or not and checks for the integrity of data.

#### 6. Process to Process Delivery: -

- Transport Layer requires a port no to correctly deliver the segments of data to the correct process among the multiple process running on a particular host. A port no is a 16-bit address used to identify any client server program uniquely.

#### 7. Transport Layer Protocol [TCP, UDP]

##### A)TCP (Transmission Control Protocol): -

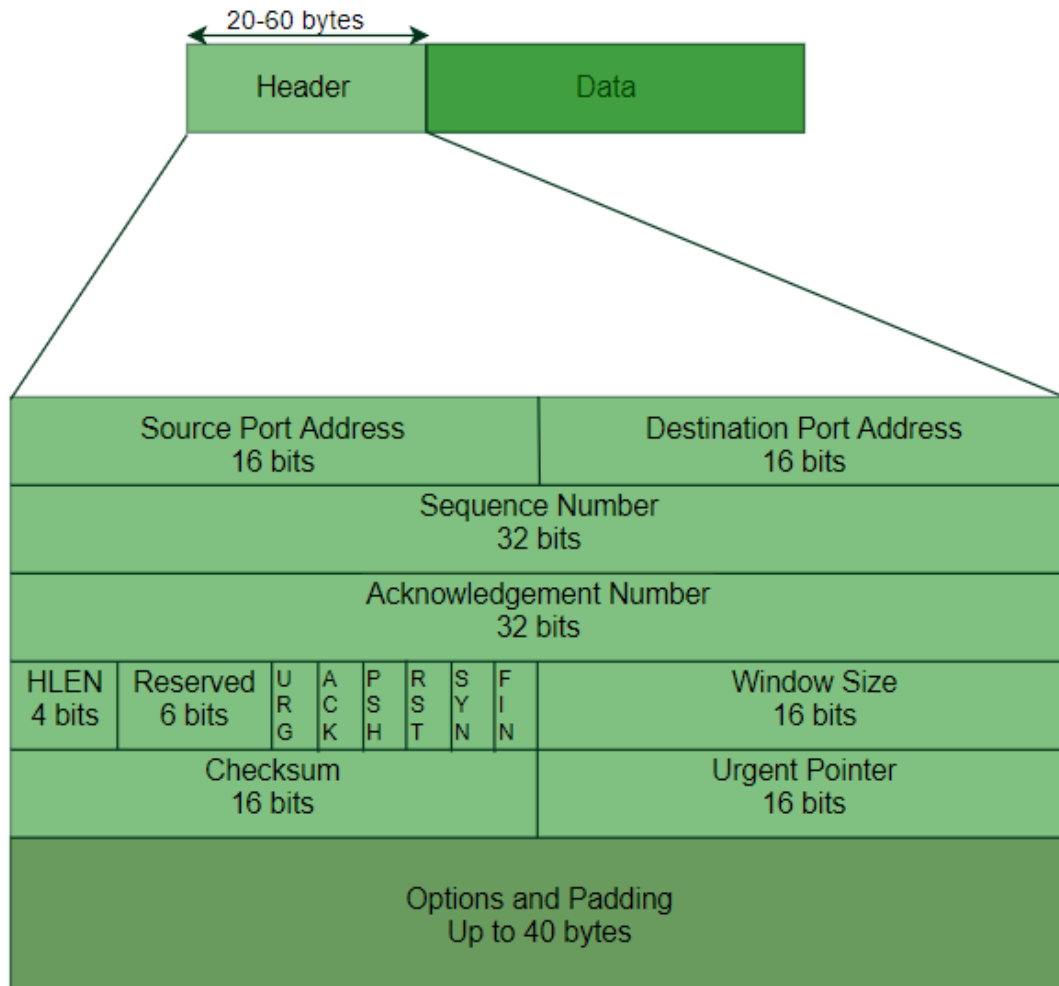
- Transmission Control Protocol is a standard that defines how to establish and maintain a network connection through which application programs can exchange data.
- TCP is a Connection Oriented Protocol which means a connection is established and maintained until the application program at each end have finished exchanging messages. It determines how to break application data into packets that networks can deliver, sends packets to and accept packet from network layer and Manages flow control.
- TCP is meant to provide error free data transmission and retransmission of the packets which are lost or corrupted. This is why it is known as reliable protocol.

##### ■ TCP Header

- Each message has 2 parts over the computer network. One is actual user or application data and another is the information in protocol defined format called header.

Header contains controls information for the purpose of handling of messages on receiver side. Header should react first to the receiver then user data to process the msg as per the protocol.

Format: -



### 1. Source Port: -

- A 16-bit no identifying the application, the TCP segment originally from sending host.

### 2. Destination Port: -

- A 16-bit no identifying the application, the TCP segment is destined for a receiving host.

### 3. Sequence Number: -

- A 32-bit number identifying the current position of the first data byte in the segment within the entire byte streams for TCP Connection.

### 4. Acks Number: -

- A 32-bit number identifying the need data byte, the sender expects from the receiver this field is only used when the ack control bit is turned ON.

### 5. Header length / offset: -

- A four-bit field that specifies the total TCP header length. It is variable in nature and always multiple of 32-bits.

### 6. Reserved Fields: -

- A 6-bit field currently unused and is reserved for future use.

## 7. Flags: -

- The flag field contains control information about the packet. There are 6 flags used in TCP header and they are: -
  - 1) Urgent Pointer (urg)
  - 2) Acknowledge (ACK)
  - 3) Push Function (PSH)
  - 4) Reset the Connection (RTC)
  - 5) Synthesis (SYN)
  - 6) No more data form sender (FIS)

## 8. Window: -

- A 16-bits integer is used by TCP for flow control is the form of data transmission size.

## 9. Checksum: -

- The checksum is a 16-bit value sender computes the check sum and set in the header before sending to the receiving a receiving side, again checksum is computed and matched. If the check sum doesn't match means the segment is corrupted and it is discarded.

## 10. Urgent Pointer: -

- In certain circumstances, it may be necessary for a TCP Seder to notify the receiver a urgent that should be processed by the receiving application as show as possible. This is 16-bit fields that fells the receiver when the last bytes of urgent data in the segment ends.

## 11. Options: -

- These are optical parameters.

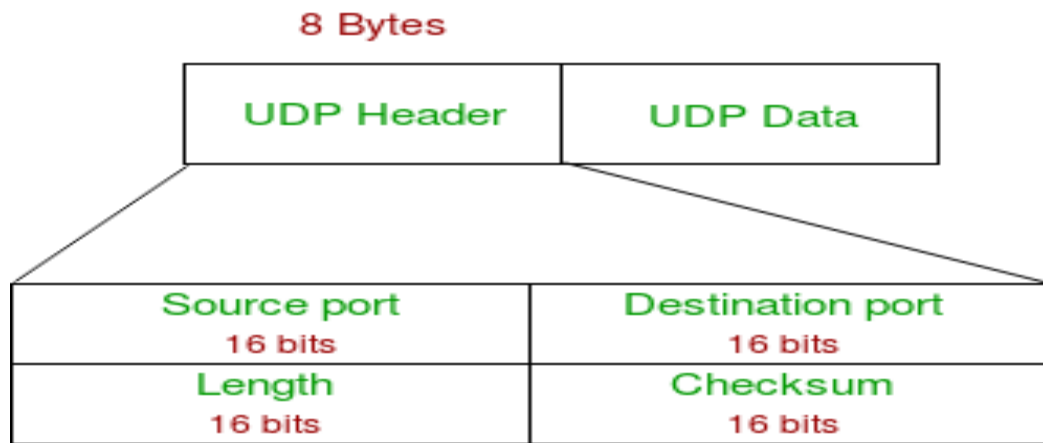
## 12. User Data: -

- This field contains actual data sent by the user. TCP header user data is known as a TCP Segment.

## B)UDP (User Datagram Protocol): -

- UDP is a transport layer protocol. UDP is a part of internet protocol. Unlike, it is unreliable and connection less protocol so, these is no need to established connection before transferring data.
- Through TCP is the dominant transport layer protocol but it is expensive to use because of additional overhead and loading. For the real time services like gaming, voice or video communication, live conferencing. We need UDP. Since high performance needs permits packet to be dropped instead of retransmission. There is no error checking in UDP so it Saves bandwidth.

### ▪ UDP Header



### 1. Source Port: -

- Source port is a 2-byte long fields used to identify port number of sources.

### 2. Destination Port: -

- It is 2 bytes long field, used to identify port number of destinations.

### 3. Length: -

- Length is the length of UDP including UDP header and the data. It is 16-bit field.

### 4. Check Sum: -

- It is used to verify the integrity of UDP header. It is also 16-bit field.

## ➤ Difference between TCP and UDP

The difference between TCP and UDP are listed

S. N	Transmission Control Protocol	User Datagram Protocol
1	TCP is a connection-oriented protocol i.e., a connected is established before transmission of data.	UDP is a connectionless protocol i.e., there is no overhead of a established a connection.
2	TCP is reliable i.e., it gurantees delivery of data to the destination.	UDP is unreliable i.e., it doesn't gurantees delivery of data packet.
3	TCP Provides extensive error checking mechanian by using checksum.	UDP has only basic error checking mechanism.
4	TCP is comparatively slower than UDP.	UDP is faster, simple and more efficient than TCP.
5	Retransmission of lost packet is possible in TCP.	There is no retransmission policy in UDP.
6	TCP doesn't support board casting.	UDP support broad casting.
7	TCP has a variable length header (20 to 80 bytes).	UDP has a 8 bytes fixed length header.
8	Flow control using sliding window and congestion avoidance algorithms are used in TCP.	No Flow Control and congestion control mechanism inn UDP.

## ➤ Application layer and its function

- The Application layer is at the top level of the OSI Model. It provides interfaces and support for services such as E-mail, remote file Access and transfer, shared data base management, directory services etc.
- The application layer contains a variety of protocol that are commonly required by user, some of them are SMTP, FTP, HTTP and Telnet etc.

## Functions

- Transport Access and management
  - It allows a user to access, retrieve and manages files in a remote computer.
- Mail Services
  - It provides basic for email forwarding and storage facilities.
- Virtual terminal
  - For Various reasons, it can be said that the standardization of terminals has completely failed. The OSI solution of this problem is to define a virtual terminal that is really just an abstract data structure that takes the abstract state of the actual terminal. This abstract data structure can be operated by both the keyboard and the computer and reflects the current state of the data structure on the displays. The computer can query this abstract data structure and change this abstract data structure so that output appears on the screen.
- Other Function
  - In addition to the three function above, these are some other functions: directory services, remote job entry, graphics, information communication and so on.

## ➤ Electronic Mail (E-mail): -

- Electronic Mail (e-mail is one of the most widely used services of Internet. This Service allows an Internet user to send a message in formatted manner (mail) to the other internet user in any port of world. Message in mail not only contain text, but it also contains images, audio and videos data. The person who receives mail is called recipient. It is just like postal mail service.

## ➤ SMTP (Simple Mail Transfer Protocol): -

- SMTP is a simple ASCII Protocol. In Internet, the source machine establishes a connection to port-25 of the destination machine so as, to deliver can email. The port-25 is being listened by SMTP and performs Following tasks.
  1. Accept the incoming connection and copy messages from them into appropriate mail borces.
  2. Returns an error message to the sender, if a message is not delivered.
- Once a TCP Connection between a sender and port 25 of the receiver is established, the sending machine operates as a client and the receiving machine acts as a server. The client then waits for the sender to talk first. The server sends a line of text to announce that it is ready to receive mail. After that client also announces about email and its recipient to the sender. If such recipient exists at the destination, then the



sender tells the client to send the message. The client then sends the message about the server acknowledge it.

After exchanging all the emails, the connection is released some of the command used for communication are: HELO, DATA, QUIT etc.

The main problem with SMTP is that it can only send ASCII text. It cannot send other files such as: Images, videos etc.

## ➤ File Transfer Protocol (FTP): -

- FTP is a standard network protocol used transfer of file from a server to a client server to a client using client server architecture.
- FTP is a client server protocol for transmission of file between computer on the internet over TCP/IP connections.

## Working

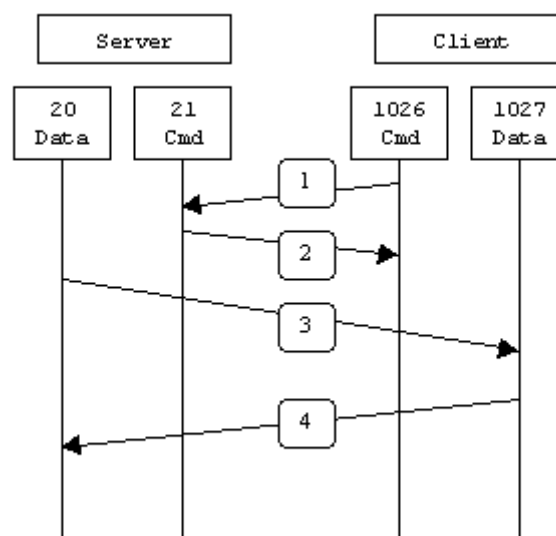
- FTP relies on two communication channels between the client and server. A command channel for controlling the conversation and data channel for transmitting files. FTP session work in passive or active modes. In active mode, after a client initiates a session via a command channel request, the server initiates a data connection back to the client and begins transferring data.

In passive mode, the server instead uses the command channel to send the client information, it needs to open a data channel.

## ➤ Modes

### 1. Active FTP: -

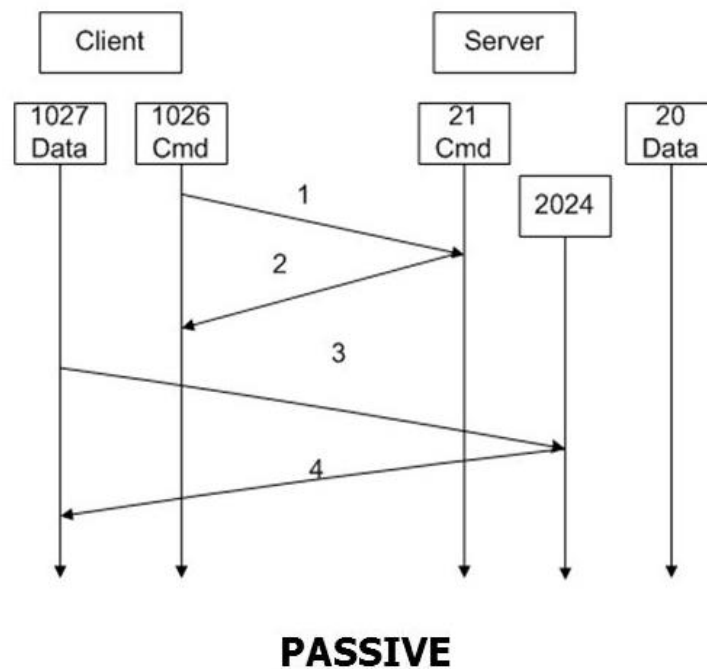
- In active mode FTP, the client connects from a random port no ( $n > 1023$ ) to the FTP servers command port no.21. then the client starts listening to port no ( $N+1$ ) and also sends this port no to the FTP server. The server will then connect local data port no 20.



### 2. Passive FTP: -

- When opening an FTP connection, the client opens two ports locally ( $P > 1023 \& N$ ). The first port contacts the server on port 11, but instead of them issuing a port

CMD & allowing the server to connect back to its data port, the client will issue the PASV (Passive) cmd. The result of this is that the server then opens a random port ( $P > 1023$ ) and send this port no to client in response to PASV CMD. The client then initiates connection from port  $N+1$  to server specified port for data transfer.



## ➤ Protocols: -

### • DHCP (Dynamic Host Configuration Protocol): -

- DHCP is an application layer protocol that automatically provides and assigns IP Addresses, default gateways, DNS address and other network parameters to client devices. DHCP is based on client- server model and users UDP services' is controlled by DHCP servers that dynamically distributes network configuration parameters. DHCP port no for server is 67 and for client is 68.

### Advantages

- Centralized management of IP addresses.
- Ease of adding new clients to a network.

### Disadvantages

- IP conflicts may occur.

➤ There are different messages that are exchange between DHCP server and a host for providing DHCP Service.

### 1. DHCP Discover: -

- When a new node is connected to the network, it broadcast the DHCP Discover message which Contains source IP as 0.0.0.0 to every node on the network including server.

## 2. DHCP Offer: -

- DHCP server on receiving the message, returns the DHCP offer message to the requested host which contains the server address & new IP address & new IP address to the node.

## 3. DHCP Request: -

- The request host on receiving the offer message, it again broadcasts the DHCP request message on the network with the address of the server whose offer message is accepted by the host.

## 4. DHCP Ack: -

- Now, the server sends DHCP ACK Packet to the request host which contains network information (IP address, subnet, mask, gateways address etc.). In case, the address is already assigned, the server sends DHCP NACK of DHCP REQUEST for IP address to the requested host.

## 5. DHCP Release: -

- When host wants to disconnect, it sends the DHCP RELEASE packet to the server indicating that it wants to disconnect. Then the server marks the IP address of that host as available in the storage so that its can be assigned to another machine.

## ➤ DNS (Domain Name System/Server): -

- DNS is a hierarchical and decentralized naming system in which internet domain names are located and translated into IP addresses. DNS uses hierarchical structure for DNS namespace mapping as show in following.

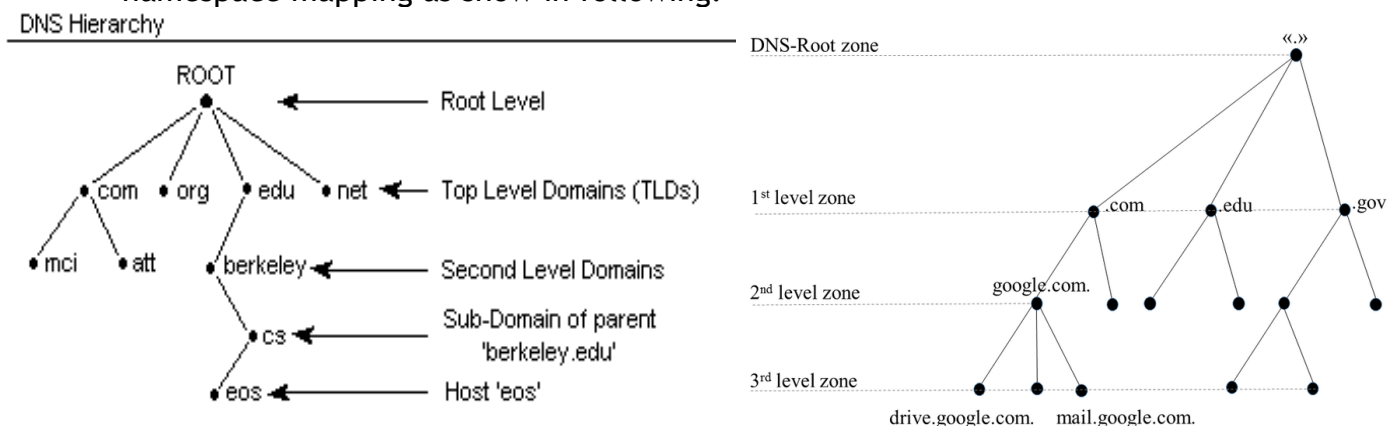


Fig: - Hierarchical Structure of DNS (Domain Name System/Server) name space

## Working: -

- The working of DNS (Domain Name System/Server) can be explained using following figure.

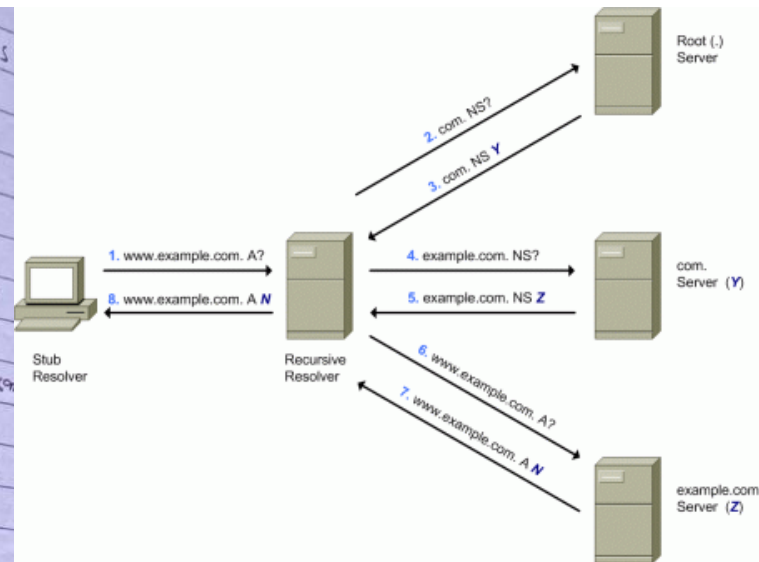
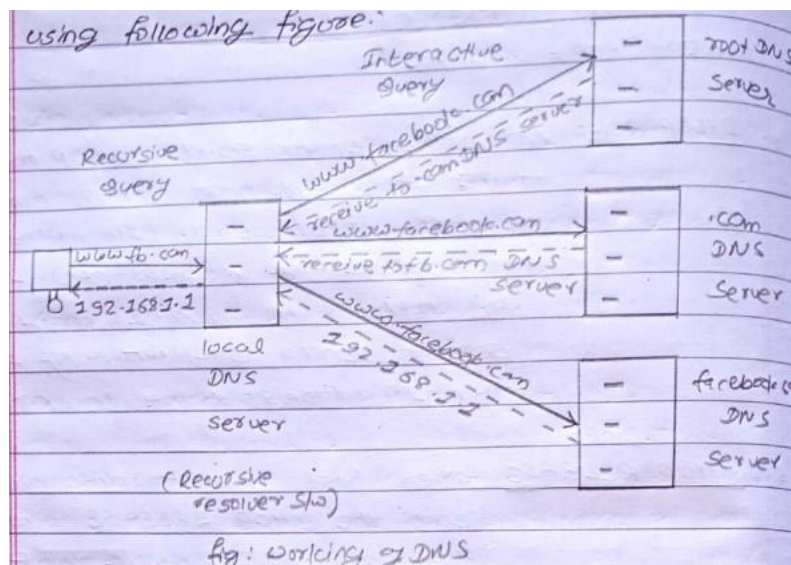


Fig working of DNS

When client searches facebook.com in browser, the request is sent to local DNS Server (Local Name Server). If the DNS server doesn't find the address in its DB, it forwards the request to the root DNS server. The root DNS server in turn will route the query to an intermediate authoritative name server. Once the authoritative name server has found the IP address of the local DNS Server which in turn returns to the host.

## ➤ World Wide Web (WWW): -

- www simply or simply web is the collection of all the resource and users on the internet. The web consists of a vast world-wide collection of documents or web pages. Each page may contain link to other pages any where in the web. These web resources are identified by uniform Resource locators (URLs) over the internet. The resource of www is transferred via HTTP/HTTPS and may be accessed by users by a S/W application called a web browser.
- The internet and www aren't the same things. The internet is a global system thing. The internet is a global system of interconnected network devices. In contrast, the www is a global collection of documents and other resources linked by hyperlinks and URIS (Uniform Resource Identifiers).

## ➤ HTTP (Hyper Text Transfer Protocol): -

- The hyper text Transfer protocol is an application layer protocol for distributed, collaboratives hyper media information system. This is the foundation for data communication for the www since 1990. Basically, HTTP is a TCP/IP Based communication protocol that is used to deliver data such as HTML files, images port no is 80: but other port member can also be used there are two types message used for communication.

### 1. HTTP Request: -

- The HTTP Client sends a request to the server in the form of a request to the server in the form of a request method (GET, POST, PUT etc.), URI and Protocol Version.

### 2. HTTP Response: -

- The http server responds with a status line including the message protocol version & a success or error code.

## Unit - 8

# Computer Network Security

### ➤ Security Concept [Confidentially, Integrity and Availability] Digital Signature: -

- In present day scenario security of the system is the sole priority of any organization. The main aim of any organization is to protect their data from attackers. In cryptography, attackers are of two types such as passive attack and active attacks.
- Passive attack is those that retrieve information from the system with out affecting the system resource while active attacks are those that retrieve system information and make changes to the system resource and their operations

### ❖ The principle of security can be classified as follows: -

#### 1. Confidentiality: -

- The degree of confidentiality determines the secrecy of the information. The principle specifies that only the sender and receiver will be able to access the information shared between them. Confidentiality compromise if an unauthorized person is able to access a message.
- For examples, let us consider sender A wants to share some confidential information with re

#### 2. Authentication: -

- Authentication is the mechanism to identify the user or system them entity. It ensures the identity of the person trying to access the information. The authentication is mostly secured by using username and password. The authorized person whose identify is preregistered can prove his/her identity and can access the sensitive information.

#### 3. Integrity: -

- Integrity gives the assurance that the information received is exact and accurate. If the content of the message is change after the sender sends it but before reaching the intended receiver, then it is said that the integrity of the message is lost.

#### 4. Non - Repudiation: -

- Non-Repudiation is a mechanism that prevents the denial of the message content sent through a network. In some cases, the sender sends the message and later denies it. But the non-repudiation does not allow the sender to sender to refuse the receiver.

#### 5. Access Control: -

- The principle of access control is determined by roles management and rules management roles management and roles management roles management determines who should access the data while rules management determines up

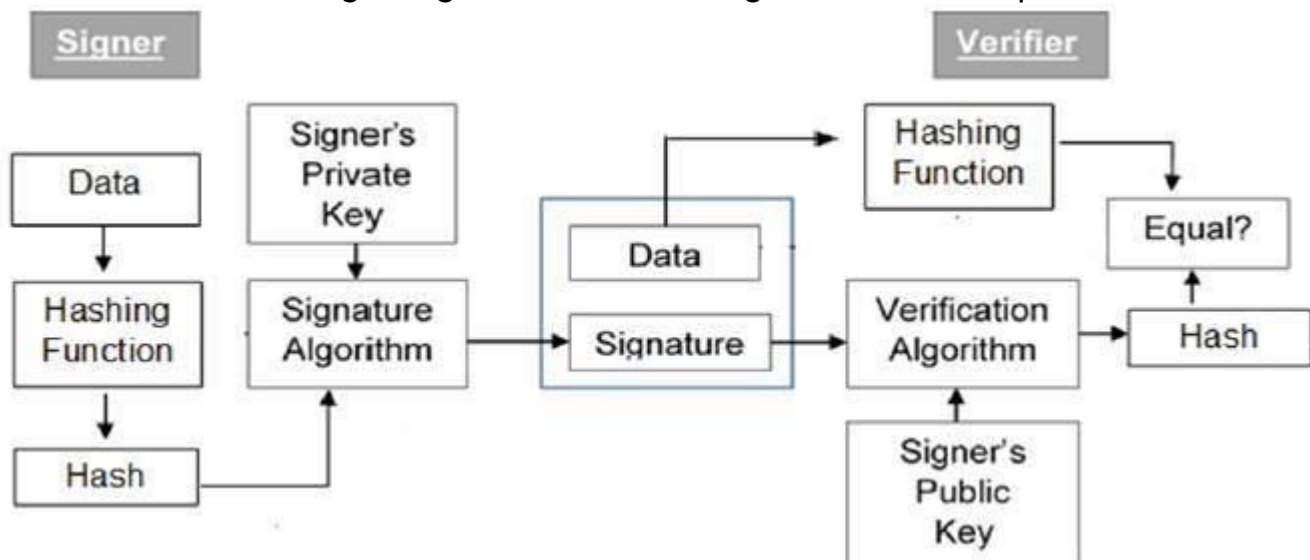
to what extent one can access the data. The information displayed is dependent on the person who is accessing it.

## 6. Availability: -

- The principle of availability states that the resources will be available to authorize party at all times. Information will not be useful if it is not available to be accessed system should have sufficient availability of information to satisfy the user request.

## ➤ Digital Signature: -

- DS is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signers. Generally, it uses public key encryption algorithm known as RSA algorithm.
- The model of digital signature is shown in figure and can be explained as follows: -



- Each person adopting these schemes has a public private key pair.
- Generally, the private keys are used for signing (also called signature key) and the public key is used as a verification key by the receivers.
- Signer feeds data to the # function and generates Hash (#) of data.
- Hash values signature key and feed to the signature algorithm which produces digital signatures on given hash signatures is appended to the data and then both are sent to the verifier (receiver).
- Verifier feeds the digital signature and the verification algorithm gives some values as output.
- Verifier also runs same # functions on received data to generate hash value.
- For verification, these hash value and o/p of verification algorithm are compared. Based on the verification algorithm are compared. Based on the comparison result, the verifier decides whether the digital signature is valid or not.
- Since digital signature is created by private key at signer and no one else can have these keys the signer cannot replicate signing the data in future.

## ➤ Cryptography



- Cryptography is a technique of securing information and communication through use of codes so that only those persons for whom, the information is intended can understand it and process it. Thus, preventing unauthorized access to the information.
- In cryptography which are used to protect information are obtained from mathematical concepts and a set of rules-based calculations known as algorithms to convert message in ways that makes it hard to decode it. These algorithms are used for cryptography key generation, digital signing, web browsing, verification of data privacy and to protect confidential transactions such as credit card and debit card and debit card transactions.

### ❖ Types: -

1. Symmetric key Cryptography.
2. Asymmetric key Cryptography.

#### 1. Symmetric key Cryptography: -

- It is an encryption standard in which sender and receiver use a single common key to encrypt and decrypt messages. SKC is faster and easy to implement but the problem is that the sender and receiver have to somehow exchange key in a secure manner. One of the SKC algorithm is Data Encryption standard (DES).

#### 2. Asymmetric key Cryptography: -

- In this technique, a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public keys are known to everyone and the private key is known by a single person who can decrypt the message. RSA is used as a symmetric key's cryptography.

### ➤ Keys Management: -

- In cryptography it is a very tedious task to distribute the public and private key between sender and receiver. If key is known to the third party (Forger/eavesdropper) then the whole security mechanism becomes worthless. So, there comes the need to secure the exchange of keys.
- The main aim of key management is to generate a secret key between two parties and store it to prove the authenticity between communicating users.
- Key management is the techniques which support key generation, storage and maintenance of the key between authorized users.
- Key management plays an important role in cryptography as the basis for securing cryptographic goals like confidentiality, authentication, data integrity and digital signatures.
- It is not the case where communicating parties are using same key for encryption and decryption or whether two different keys are used for encryption and decryption.
- Basic purpose of key management is key generation, key distribution controlling the use of keys, updating destruction, controlling the use of keys, updating destruction of keys and key backup/recovery.

### ❖ Following point to be executed in key management: -

1. User Registration.
2. User initialization.
3. Key generation.

4. Key registration.
5. Normal use.
6. Key backup.
7. Key update.
8. Key de-registration and revocation.

## ➤ Fire wall: -

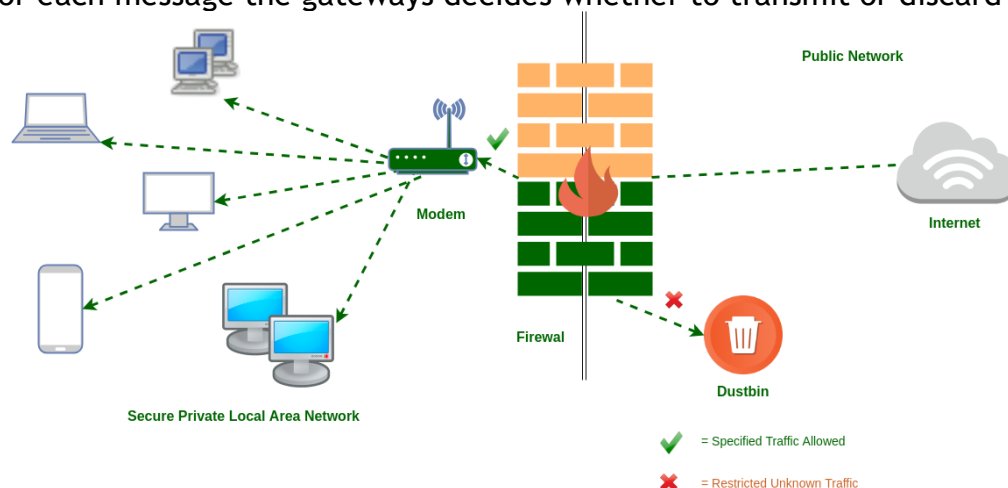
- Firewall is a network security that analyses the incoming and outgoing network traffic based on the predetermined security rules. It analyzes the network and allows the network traffic in or out if they are trusted.

### 1. Packet Filtering Firewall: -

- It protects users from the external network threats.
- Packet filtering is the process of passing or blocking packets based on source and destination address, port no or protocols at a network interface.
- The header of packet is analyzed and based on predefined rules, it allows packets to pass or prevent packets from passing.

### 2. Application Gateways (Proxy server): -

- The gateways operate at application layers.
- Application gateway for specific application can be installed.
- It filters incoming node traffic using predefined rules and is allowed to access the network if the packet do not contain restricted or malicious data.
- For eg: a mail gateway can be set up to examine each message going in or coming out for each message the gateways decides whether to transmit or discard the message.



## ➤ VPN (Virtual Private Network): -

- VPN stands for virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. Virtual private network is a way to extend a “private network” i.e user can be the part of local network sitting at a remote location.
- It allows remote users to securely access application and other resources.
- Data travels through secure tunnel.
- VPN users must use authentication method to gain VPN access.

- It ensures appropriate level of security to connected system.
- Speed of internet connection of user affects VPN performance.

### ❖ Types of Virtual Private Network: -

Generally, we can classify VPN into the following types: -

1. Remote Access VPN.
2. Intranet-based site to site VPN.
3. Extranet -based site to site VPN.

### ❖ Application of VPN: -

- VPN can easily by pass geographic restrictions on websites or streaming audio and video.
- Using a VPN, we can protect ourselves from snooping from untrustworthy Wi-Fi, hotspots.
- One can gain privacy online by hiding one's true location.
- One can protect themselves from being logged while torrenting.

### ➤ Wireless Security Threats: -

- The wireless network we use is responsible for transferring and sending data like username, password, card details and other sensitive data. If the wireless network, we use is not secure then we are at risk and face undesirable consequences.
- The most common and easily employable threats to Wi-Fi networks include.
- Evil twin- also known as a rogue Wi-Fi hotspot, this is a situation where an attacker sets up an illegitimate access point in the area where a company has installed its network. This illegitimate access point will use an independent internet connection and connected users will believe they are on the valid network.
- Man in the middle- a MITM attack is similar to the evil twin but differs in its application. A "man in the middle" access point masquerades as a legitimate device to which users connect. This device, in turn connects to the legitimate network, providing connected users with full access to both the internet and internal enterprise network services.
- Packet sniffers in general, wireless signals are freely propagated through open space. This means that any Wi-Fi device (laptop, tablet, mobile phone) can intercept signals from users and access points all around it. With the appropriate software, these signals can be detected and the packets they carry can be captured. Squed and analyzed. Such software is called packet sniffer.

### ➤ Mitigations are: -

- Use Wireless controller: - Wireless Controller is a device which controls and manages functionalities of all the access points in the network. Thus, a wireless controller configures and manages all the access points within the network. This mitigates evil twin and MIMA attacks.
- WPA 2 should be used: - WPA 2 encryption protocol should be used by defaults. If available, WPA 3 should be used.
- Employ AAA for recording user activity: - Authentication, Authorization and Accounting (AAA) server such as a RADIUS Server should be made use of for authentication and authorization of users. Also, their activity should be logged and recorded.
- VPN: - Makes use of VPN if needed or possible.