PNS SCHOOL OF ENGINEERING & TECHNOLOGY
Nishamani Vihar, Marshaghai, Kendrapara

LECTURE NOTES
ON

DATA COMMUNOCATION & COMPUTER NETWORK

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

4TH SEMESTER

PREPARED BY

MR. BISWARANJAN SWAIN

Lecturer, Department of Computer Science & Engineering

SYLLABUS

Unit-I: Introduction to Computer Networks and Network Models

Introduction to computer networks

Network Models: OSI Reference Model

TCP/IP Model

Unit-II: Transmission Media, Topologies, and Data Link Layer

Transmission Media: principles, issues and examples

Wired Media: Coaxial, UTP, STP, Fiber Optic Cables

Wireless Media: HF, VHF, UHF, Microwave, Ku Band

Network topologies

Data Link Layer: design issues,

Example protocols (Ethernet, WLAN, Bluetooth)

Switching Techniques

Unit-III: Network Layer and Routing Protocols

Network Layer: design issues

Example protocols (IPv4)

Routing: Principles/Issues,

Algorithms : Distance-vector, Link-state

Protocols RIP, OSPF

Unit- IV: Transport and Application Layer Protocols

Transport Layer - design issues

Example protocols: TCP

Application Layer Protocols: SMTP, DNS.

Unit- V: Network Devices and Management Systems

Functioning of Network Devices – NIC, Hub, Switch, Router, Wi-Fi Devices,

Network Management System

Example protocol: SNMP.

UNIT-1

INTRODUCTION TO COMPUTER NETWORKS AND NETWORK MODELS

1.1 Introduction:

Data communications and networking are changing the way we do business and the way we live. Business decisions have to be made ever more quickly, and the decision makers require immediate access to accurate information. One goal is to be able to exchange data such as text, audio, and video from all points in the world. This chapter addresses four issues: data communications, networks, the Internet, and protocols and standards. First we give a broad definition of data communications.

1.2 Data communication:

When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance. The term telecommunication, which includes telephony, telegraphy, and television, means communication at a distance (tele is Greek for "far").

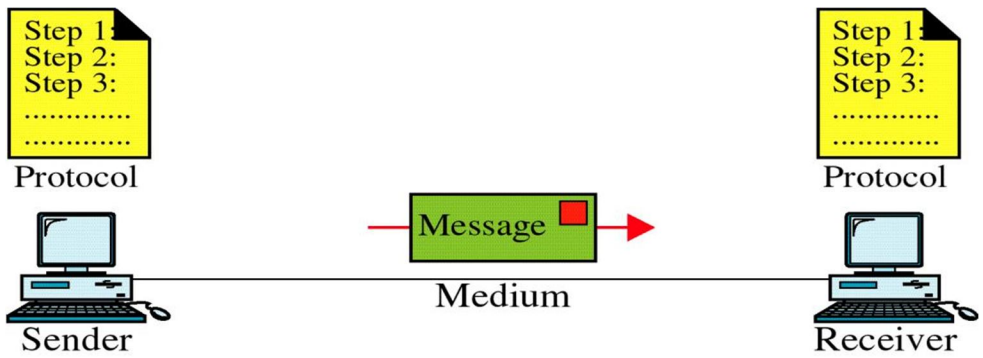
- Data communications are the exchange of data between two devices via some formof transmission medium such as a wire cable.
- It includes the transfer of data, the method of transfer and the preservation of data during transfer process.
- To initiate data communication the devices should be collection of both physicalequipments (hardware) and programs(software).

The effectiveness of a data communications system depends on four**fundamental characteristics**: delivery, accuracy, timeliness and jitter.

1. **Delivery:** The system must deliver data to the correct destination. Data must bereceived by the intended device or user and only by that device or user.
2. **Accuracy:** The system must deliver the data accurately. Data that have beenaltered in transmission and left uncorrected are unusable.
3. **Timeliness:** The system must deliver data in a timely manner. Data delivered late are Useless.
4. **Jitter:** Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

1.3 Components of Data Communication:

A data communications system has five components.



i) ***Message.*** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

ii) Sender. The sender is the device that sends the data message. It can be a computer,workstation, telephone handset, video camera, and so on.

iii) Receiver. The receiver is the device that receives the message. It can be a computer,workstation, telephone handset, television, and so on.

iv) Transmission medium. The transmission medium is the physical path by whicha message travels from sender to receiver. Some examples of transmission mediainclude twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

v) Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understoodby a person who speaks only Japanese.

Note: The devices generally called as nodes in networking concept.

1.4 Data Representation :

Information today comes in different forms such as text, numbers, images, audio, and video.

i) Text: In data communications, text is represented as a bit pattern, a sequence of bits (Os or Is). Different sets of bit patterns have been designed to represent text symbols.

ii) Numbers : Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations. Appendix B discusses several different numbering systems.

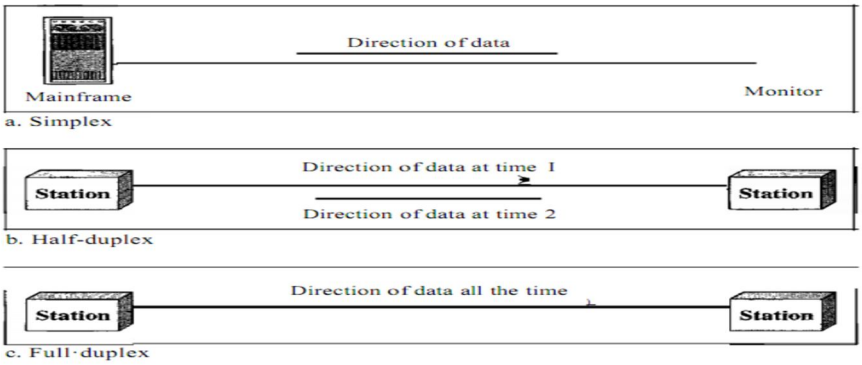
iii) Images **:** Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution.

iv) Audio : Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete.

v) Video**:** Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

1.5 Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex as shown in figure below.



i) Simplex

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive (see Figure 1.2a).

Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output.

ii) Half-Duplex

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is

sending, the other can only receive, and vice versa (see Figure 1.2b).
In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

iii) Full-Duplex

In full-duplex m.,lle (als@ called duplex), both stations can transmit and receive simultaneously (see Figure 1.2c). The full-duplex mode is like a tW<D-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction.
One common example of full-duplex communication is the telephone network.
When two people are communicating by a telephone line, both can talk and listen at the same time.

1.6 Network:

A network is a set of devices (often referred to as *nodes)* connected by communication links. A node can be a computer, printer, or any other device capable ofsending and/or receiving data generated by other nodes on the network.

Network Criteria:
A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

a. Performance: Performance can be measured in many ways, including Transit and response time.
   i. Transit time is the amount of time required for a message to travel from one device to another.
   ii. Response time is the elapsed time between an inquiry and a response.
   iii. The performance of a network depends upon number of users, type of transmission medium, capabilities of hardware, efficiency of software.

b. Reliability: Network reliability is measured by the frequency of failure, the time ittakes a link to recover from a failure, and the network's robustness in catastrophe.

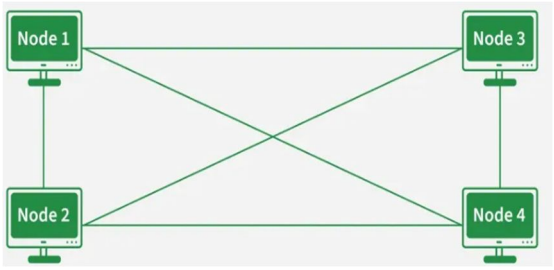
c. Security: Network security issues include protecting data from unauthorized access,protecting data from damage.

1.7 Physical Topology

The term physical topology refers to the way in which a network is laid out physically. 1 or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring.

i) Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. Every device is connected to another via dedicated channels. These channels are known as links.



- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is $N - 1$. In Figure , there are 4 devices connected to each other, hence the total number of ports required by each device is 3. The total number of ports required = N * (N-1).
- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is ${}^{N}C_{2}$ i.e. N * (N-1)/2. In Figure, there are 4 devices connected to each other, hence the total number of links required is 4 * 3/2 = 6.

Advantages of Mesh Topology

- Communication is very fast between the nodes.
- Mesh Topology is robust.

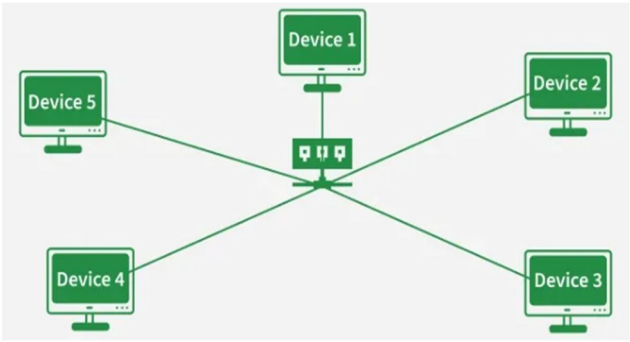
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Disadvantages of Mesh Topology

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

ii) Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them.



Advantages of Star Topology

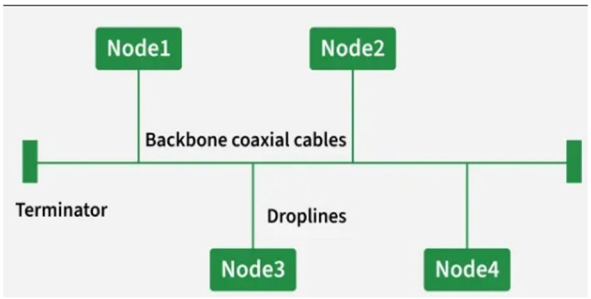
- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

Disadvantages of Star Topology

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

iii) Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.



Advantages of Bus Topology

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.

- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.
- CSMA/CD was the only MAC method used in traditional bus Ethernet. Modern switched Ethernet does not use CSMA/CD because full-duplex operation eliminates collisions.

Disadvantages of Bus Topology

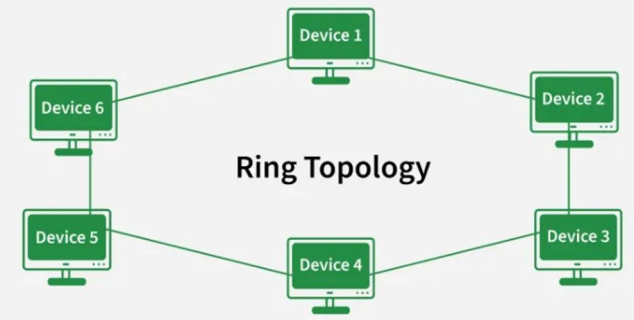
- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

Note: *A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks.*

iv) Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data where, Token passing is a network access method in which a token is passed from one node to another node & Token is a frame that circulates around the network.



Operations of Ring Topology

- One station is known as a monitor station which takes all the responsibility for performing the operations.
- To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
- When no station is transmitting the data, then the token will circulate in the ring.

Advantages of Ring Topology

- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.

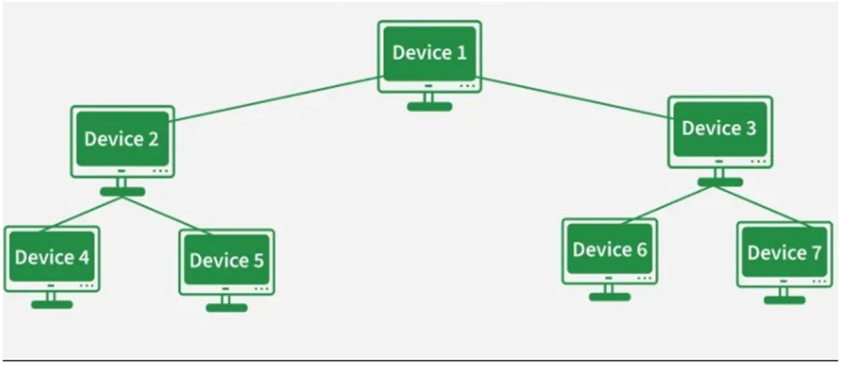
Disadvantages of Ring Topology

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- Less secure.

v) Tree Topology

Tree topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and SAC (Standard Automatic Configuration) are used.

- Here, various secondary hubs are connected to the central hub which contains the repeater.
- This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub.
- It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.



Advantages of Tree Topology

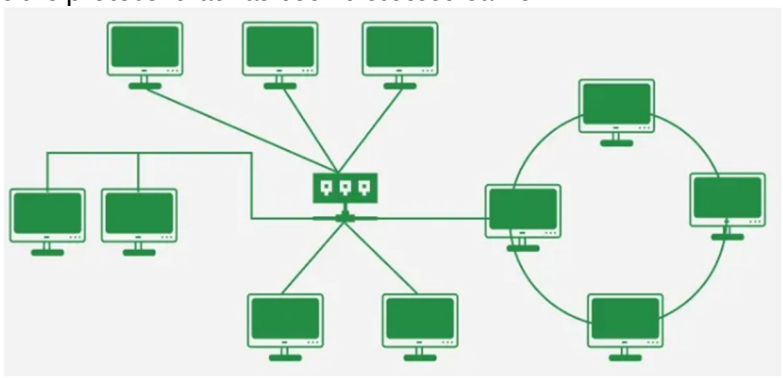
- It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.
- It allows the network to get isolated and also prioritize from different computers.
- We can add new devices to the existing network.

Disadvantages of Tree Topology

- If the central hub gets fails the entire system fails.
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

vi) Hybrid Topology

Hybrid Topology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.



Advantages of Hybrid Topology

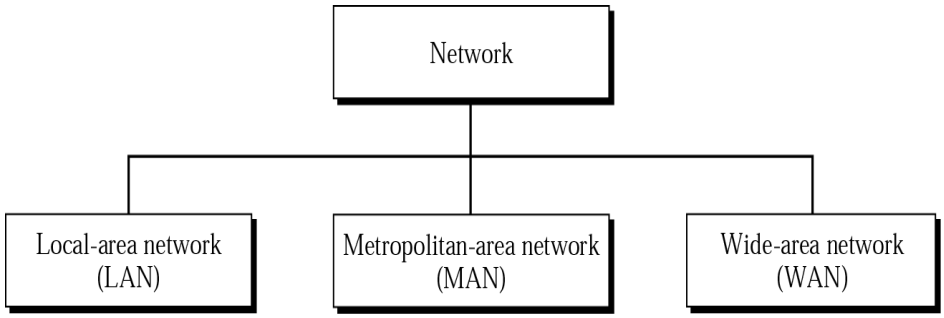
- This topology is very flexible.
- The size of the network can be easily expanded by adding new devices.

Disadvantages of Hybrid Topology

- It is challenging to design the architecture of the Hybrid Network.
- Hubs used in this topology are very expensive.
- The infrastructure cost is very high as a hybrid network requires a lot of cabling and network devices .

TYPES OF NETWORKS

Network divided in to three primary categories: LAN, MAN, WAN. In to which category a network falls is determined by its Size, Ownership, Distance it covers, and Physical architecture.



i) Local Area Network (LAN) :

- LAN is usually Privately owned and Links devices in single office, building or campus.
- LAN size is Limited to few kilometres.
- LANs are designed to allow resources (i.e. hardware or software) to be shared between PCs and workstations.
- LAN will use a single transmission media.
- The most common LAN Topologies are Ring, bus, star.

ii) Metropolitan Area Network (MAN):

- A MAN is designed to extend over an entire city.
- It may be single network such as cable television network, or it may be a means ofconnecting number of LANs in to a larger networks.
- A MAN be wholly Owned and operated by a private company, or it may be a Serviceprovider by Public company such as a local telephone company.

iii) Wide Area Network (WAN):

WAN provides long-transmission of data, voice, image and video information over large geographic areas that may comprise a country, a continent or even the whole world.

WAN that is wholly owned and used by a single company is often referred to as an enterprise network.

Ex: Bank network which depends upon the satellite communication.

Computer Network & Administration: The managing and administrating of group of networks is called CAN.

Intranet: A network within itself is called intranet.

INTERNET:

- Interconnection of two or more networks is called internetworks, or internet.
- Network of networks is also called internet.
- Internet is different from internet(i.e. Internet is the name of a specific worldwidenetwork & internet is the interconnection networks).

PROTOCOL:

A network protocol defines rules and conventions for communication between networkdevices. It defines

- What is communicated
- How it is communicated
- When it is communicated

Key element of Protocol

- Syntax

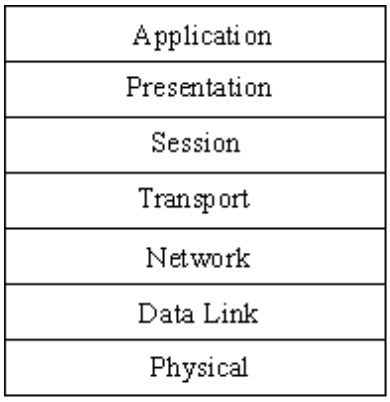
- Semantics
- Timing

THE OSI MODEL:

- An ISO(International Standard Organization) standard that covers all aspects of network communications is the **Open Systems Interconnection model.**
- An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware andsoftware standards.
- The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.
- The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.
- It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network
- An understanding of the fundamentals of the OSI model provides a solid basis for exploring data communications.

Layered Architecture:

It mainly consists of seven layer: **Physical** (layer 1), **Data link** (layer 2), **Network** (layer 3), **Transport** (layer 4), **Session** (layer 5), **Presentation** (layer 6), and **Application** (layer 7).



The OSI 7-layer Reference Model

Physical Layer

- The physical layer coordinates the functions required to carry a bit stream overa physical medium.
- It deals with the mechanical and electrical specifications of the interface andtransmission medium.
- It also defines the procedures and functions that physical devices and interfaces haveto perform for transmission to Occur.
- The physical layer defines the characteristics of the interface between the devices andthe transmission medium. It also defines the type of transmission medium.
- The transmission rate-the number of bits sent each second is also defined by thephysical layer.
- The physical layer is concerned with the connection of devices to the media.
- In a point-to-point configuration, two devices are connected through a dedicated link.In a multipoint configuration, a link is shared among several devices.
- The physical layer also defines the direction of transmission between two devices:simplex, half-duplex, or full-duplex.

2. Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link.It makes the physical layer appear error-free to the upper layer.

- **Framing**. The data link layer divides the stream of bits received from the networklayer into manageable data units called frames.
- **Physical addressing**. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame.
- **Error control**. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames.
- **Access control**. When two or more devices are connected to the same link, datalink layer protocols are necessary to determine which device has control over the link at any given time.

3. Network Layer

The network layer is responsible for the source-to-destination delivery of a packet, possiblyacross multiple networks (links).

- **Logical addressing.** The network layer adds a header to the packet coming from theupper layer that, among other things, includes the logical addresses of the sender andreceiver.
- **Routing.** When independent networks or links are connected to create *intemetworks*(network of networks) or a large network, the connecting devices (called*routers* or *switches)* route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

4. Transport Layer

The transport layer is responsible for process-to-process delivery of the entire message. Aprocess is an application program running on a host.

- **Service-point addressing** .The transport layer header must therefore include a type of address called a *service-point address* (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to thecorrect process on that computer.
- **Segmentation and reassembly**. A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enablethe transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
- **Flow control**. Like the data link layer, the transport layer is responsible for flow control.
- **Error control**. Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to process rather thanacross a single link.

5. Session Layer

The services provided by the first three layers (physical, data link, and network) are notsufficient for some processes. The session layer is the network *dialog controller.*

It establishes, maintains, and synchronizes the interaction among communicating systems.

- **Dialog control**. The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one wayat a time) or full-duplex (two ways at a time) mode.
- **Synchronization**. The session layer allows a process to add checkpoints, or synchronization points, to a stream of data.

6. Presentation Layer

The presentation layer is concerned with the syntax and semantics of the informationexchanged between two systems.

- **Translation:** The presentation layer at the sender changes the information from its sender-

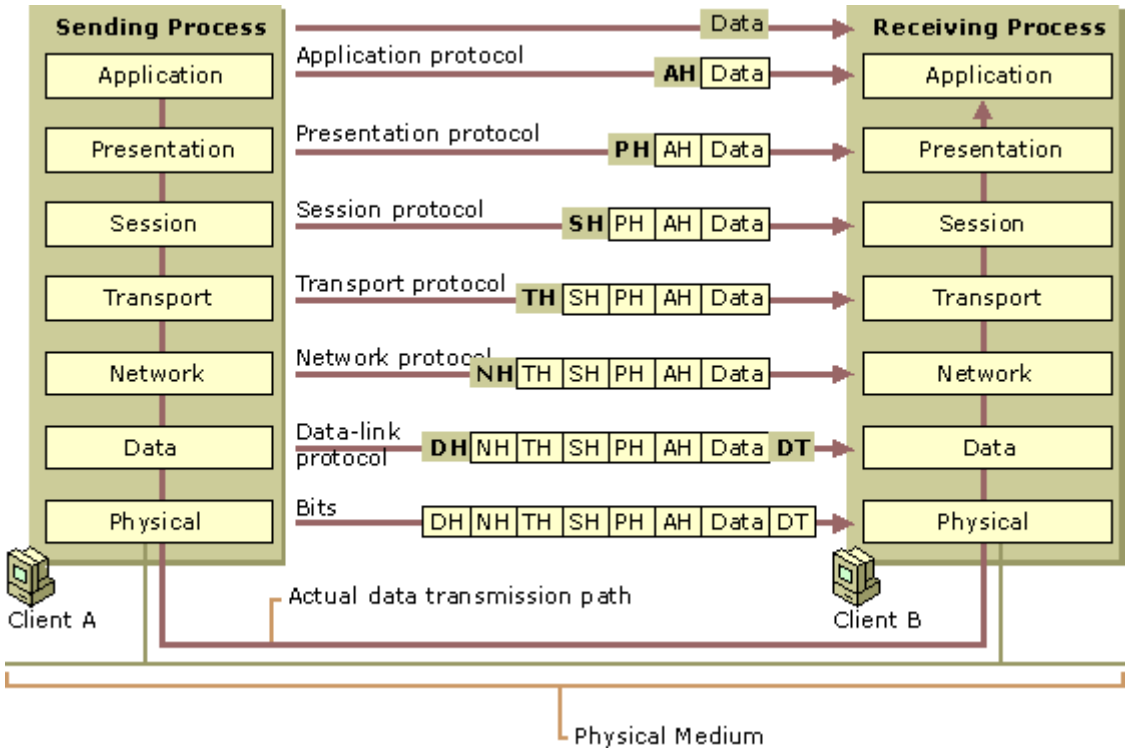
dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

- **Encryption**. To carry sensitive information, a system must be able to ensure privacy.Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
- **Compression.** Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

7. *Application Layer*

The application layer enables the user, whether human or software, to access the network.
It provides user interfaces and support for services such as electronic mail, remote file accessand transfer, shared database management, and other types of distributed informationservices.

- **Network virtual terminal**. A network virtual terminal is a software version of a physicalterminal, and it allows a user to log on to a remote host.
- **File transfer, access, and management.** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **Mail services**. This application provides the basis for e-mail forwarding and storage.
- **Directory services**. This application provides distributed database sources and access for global information about various objects and services.

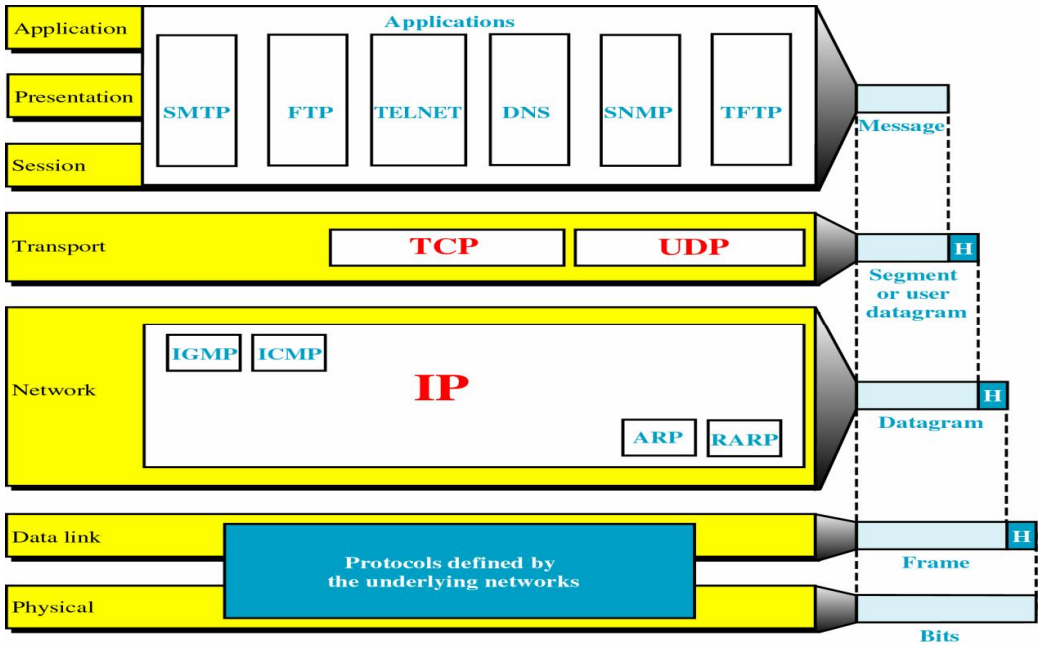


TCP/IP PROTOCOL SUITE:

- The TCP/IP protocol suite was developed prior to the OSI model. Therefore, thelayers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- It is a set of protocols or a protocol suite that defines how all transmission areexchanged across the internet.
- TCP/IP protocol suite is made of five layers:
  1. **Physical**
  2. **Datalink**

3. **Network**
4. **Transport**
5. **Application**

- The first four layers provide physical standards, network interface, internetworking, andtransport functions that correspond to the first four layers of the OSI model.
- The three topmost layers in the OSI model, however, are represented in TCP/IP by asingle layer called the application layer.
- It is hierarchical protocol made up of interactive modules, each of which provides aspecific functionality.
- However the modules are not necessarily interdependent.



DESCRIPTION ABOUT LAYERS:

1. Physical and Data Link Layers

At the physical and data link layers, TCP/IP does not define any specific protocol. It supportsall the standard and proprietary protocols. A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

2. Network Layer

At the network layer (or, more accurately, the internetwork layer),TCP/IP supports the **Internetworking Protocol, IP**. Also it uses four supporting protocols:

ARP, RARP, ICMP, and IGMP

Internetworking Protocol (IP)

- It is the transmission mechanism used by TCP/IP protocol.
- It is an unreliable and connectionless protocol.
- IP transports data in packets called datagrams.
- Each packet transport separately.

Address Resolution Protocol(ARP)

The Address Resolution Protocol (ARP) is used to associate a logical address with aphysical address.

Reverse Address Resolution Protocol(RARP)

It allows a host to find its internet address when it know only physical address. It is usedwhen

computer connected to n/w first time.

Internet Control Message Protocol(ICMP)

The Internet Control Message Protocol (ICMP) is a mechanism used by hosts andgateways to send notification of datagram problems back to the sender.

Internet Group Message Protocol(IGMP)

The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

3. Transport Layer

- Traditionally the transport layer was represented in *TCP/IP* by two protocols**: TCP andUDP.**
- IP is a host-to-host protocol, meaning that it can deliver a packet from one physicaldevice to another.
- But **UDP and TCP** are transport level protocols responsible for delivery of a messagefrom a process (running program) to another process.
- A new transport layer protocol, **SCTP**, has been devised to meet the needs of somenewer applications.

User Datagram Protocol(UDP)

- It is a process-to-process protocolThat adds only port addresses, checksum errorcontrol and length information to the data from the upper layer.
- It is simple & fast but a unreliable connectionless delivery service.

Transmission Control Protocol(TCP)

- The Transmission Control Protocol (TCP) provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term *stream* means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.

Stream Control Transmission Protocol (SCTP)

The Stream Control Transmission Protocol (SCTP) provides support for newer applicationssuch as voice over the Internet.

4. Application Layer

The *application layer* in TCP/IP is equivalent to the combined session, presentation,and application layers in the OSI model Many protocols are defined at this layer.

They are SMTP,FTP,HTTP,DNS,SNMP,TELNET etc.

SMTP(Simple Mail Transfer Protocol)

It is used to send email from one system to another.

FTP(File Transfer Protocol)

It is used to send an application program(file) to another system. i.e files are transferred fromserver to client.

HTTP(Hypertext Transfer protocol)

- Used mainly to access data on WWW.
- Used to transfer data in the form of plain text, hypertext, audio, video and so on.

DNS(Domain Name Server or System)

- Provides the protocol that allows clients and server to communicate with each other.
- It allows computer to have names like kp.kiit.edu rather than just IP address like 144.162.120.233.

SNMP(Simple N/W Management Protocol)

It provides a systematic way of monitoring and managing or maintaining an internet orcomputer n/w.

TELNET(Terminal Network)

- It is a client-server application program.
- Responsible for establishment of a connection to a remote system so that the terminalappears as a local terminal at the remote system.

UNIT - 2

TRANSMISSION MEDIA, TOPOLOGIES AND DATALINK LAYER

DATA TRANSMISSION:

The way in which data is transmitted from one place to another is called *data transmission mode*. Itis also called the *data communication mode*. It is indicates the direction of flow of information. These are of 3 types: Simplex, Half-duplex, Full-duplex.

Data transmission can either be analog or digital.

Transmission:

Communication between two devices can be simplex, half-duplex, or full-duplex .

1. Simplex

- In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive.
- The simplex mode can use the entire capacity of the channel to send data in onedirection.
- Keyboards and monitors are traditional examples of simplex devices.

2. Half-Duplex

- In half-duplex mode, each station can both transmit and receive, but not at thesame time When one device is sending, the other can only receive, and vice versa.
- The half-duplex mode is like a one-lane road with traffic allowed in both directions. half-duplex transmission, the entire capacity of a channel is taken over by whicheverof the two devices is transmitting at the time.
- Walkie-talkies and CB (citizens band) radios are example of half-duplex systems.

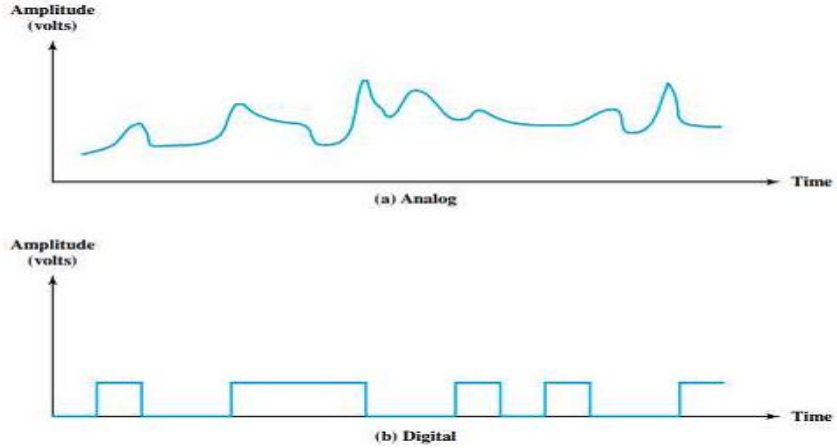
3. Full- Duplex

- In full-duplex mode (also called duplex), both stations can transmit and receivesimultaneously.
- The full-duplex mode is like a two way street with traffic flowing in both directionsat the same time.
- The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the twodirections.
- One common example of full-duplex communication is the telephone network.
- When two people are communicating by a telephone line, both can talk and listen at the same time.

Analog transmission :-

An analog signal is one in which the signal intensity varies in a smooth fashion over time. In other words there are no breaks or discontinuities in the signal.

A digital signal is one in which the signal intensity maintains a constant level for some period of time and then abruptly changes to another constant level.



Analog transmission consist of sending information over a physical transmissionmedium in the form of wave .
Both analog and digital signals can take one of two forms: periodic or non periodic.
Periodic Signals are signals that repeat themselves after a certain amount of time.

ANALOG AND DIGITAL DATA

Analog data take on continuous values in some interval. For example, voice and video are continuously varying patterns of intensity.

Digital data take on discrete values; examples are text and integers.

Analog and Digital Signals

In a communications system, data are propagated from one point to another by means of electromagnetic signals.

An **analog signal** is a continuously varying electromagnetic wave that may be propagated over a variety of media, depending on spectrum; examples are wire media, such as twisted pair and coaxial cable; fiber optic cable; and unguided media, such as atmosphere or space propagation.

A **digital signal** is a sequence of voltage pulses that may be transmitted over a wire medium; for example, a constant positive voltage level may represent binary 0 and a constant negative voltage level may represent binary 1.

Terminology used related to Data Transmission

Channel:

- Physical medium like cables over which information is exchanged is called channel. Transmission channel may be analog or digital.
- In popular network terminology, path over which data is sent or received is called data channel.

Data Transfer Rate:

- The speed of data transferred or received over transmission channel, measured per unit time, is called data transfer rate. The smallest unit of measurement is bits per second (bps). 1 bps means 1 bit (0 or 1) of data is transferred in 1 second.

Bit rate:-The bit rate is the number of bits transmitted in one second. It is expressed inthe terms of bps.

Baud rate:-The number of signals transmitted in 1 second is defined as baud rate/signal rate or pulse rate.

Data rate/bit rate VS **signal rate/baud rate**:-

*S = N *1/R baud*

where,

N=data rate S=signal rate R=log2L

L=no of level used in a signal

1. **Carrier signal:-** In analog transmission the sending device produces a high frequency signal that act as a base for the information signal. The base signal is called as carriersignal/carrier frequency.

2. **Bandwidth:-** The bandwidth of a signal is the difference between the highest to lowestfrequency content in the signal. Data transfer rates that can be supported by a network is called its bandwidth. It is measured in bits per second (bps). Modern day networks provide bandwidth in Kbps, Mbps and Gbps.
3. **Dc component:-** When the voltage level in a digital signal is constant for a while the spectrum creates a very low frequency (around 0) called as DC component which creates some problem during transmission.
4. **Throughput** is the measure of how fast the data is being sent through a network. It is normally expressed in bps.
5. **Latency:-**

Latency=propagation time + transmission time + queuing time + process delay.

Propagation time= distance/propagation speed

Transmission time=message size/bandwidth

Queuing time:- this time needed for each intermediate device to hold the message beforeit can be processed.

Processing delay:- processing delay or bandwidth delay .it defines the number of bits canfill the link.

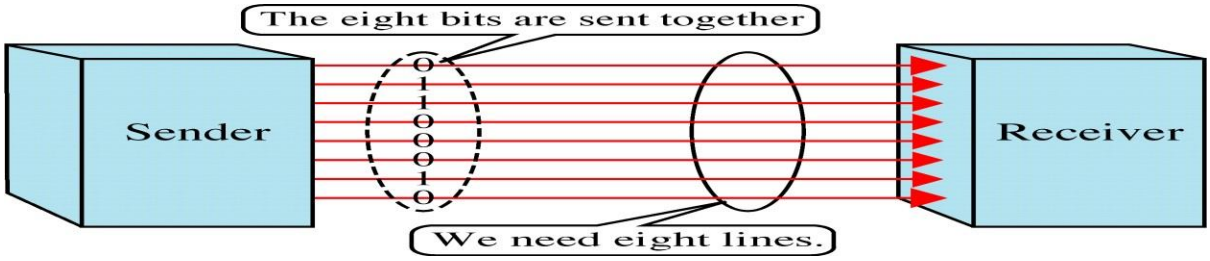
Information generated by a source need to be encoded into a suitable format for transmission. To transmit the encoded signals generated by the Information-processing equipment over a communication link, assistance is needed.

TRANSMISSION TYPES:

The transmission of binary data across a link can be accomplished in either parallelor serial mode.

Parallel Transmission:

- Binary data, consisting of 1s and 0s, may be organised into groups of n bits each. By grouping, we can send data n bits at a time instead of one. This is called parallel transmission.
- We use n wires to send n bits at one time. That way each bit has its own wire, andall n bits of one group can be transmitted with each clock pulse from one device to another.
- The Figure below shows how parallel transmission works for n = 8. Typically, the eight wires are bundled in a cable with a connector at each end.



Advantage

- The advantage of parallel transmission is speed.
- All else being equal, parallel transmission can increase the transfer speed by a factorof n over serial transmission.

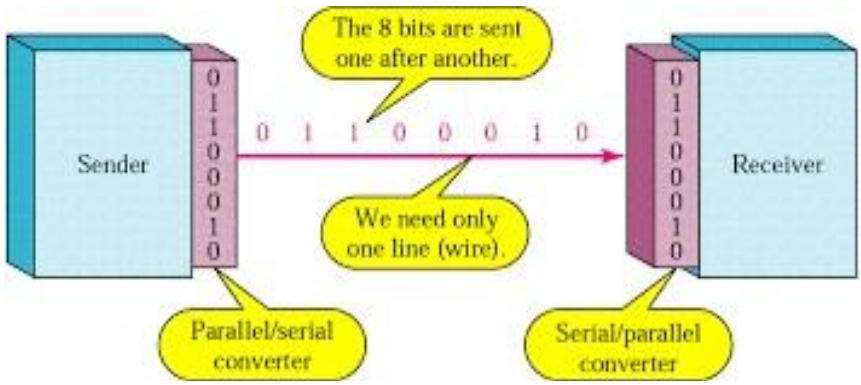
Disadvantage

- A significant disadvantage of parallel transmission is cost.
- Parallel transmission requires n communication lines (wires in the example) just totransmit the data stream.

- As this is expensive, parallel transmission is usually limited to short distances.

Serial transmission

- In serial transmission one bit follows another, so we need only one communicationchannel rather than n to transmit data between two communicating devices.
- The advantage of serial over parallel transmission is that with only one communication channel, serial transmission reduces the cost of transmission overparallel by roughly a factor of n.



Serial transmission occurred in two ways

TRANSMISSION MEDIA:

1`.A transmission medium can be broadly defined as anything that can carry informationfrom a source to a destination.

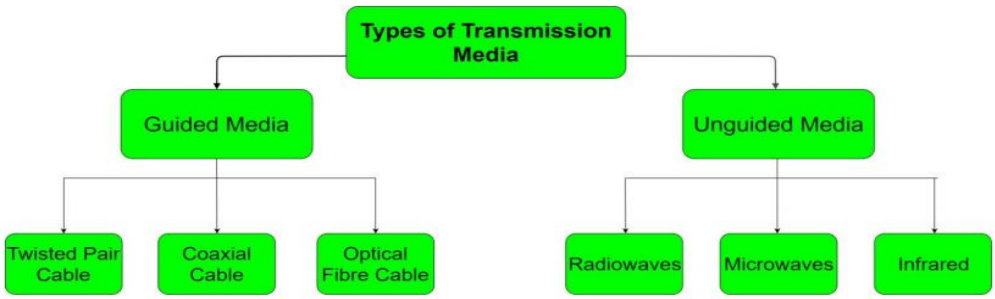
2 .The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversionof data from another form.

CATEGORIES:

In telecommunications, transmission media can be divided into two broad categories:

1.guided

1. unguided.



1. GUIDED MEDIA:

Guided media, which are those that provide a conduit from one device to another,.

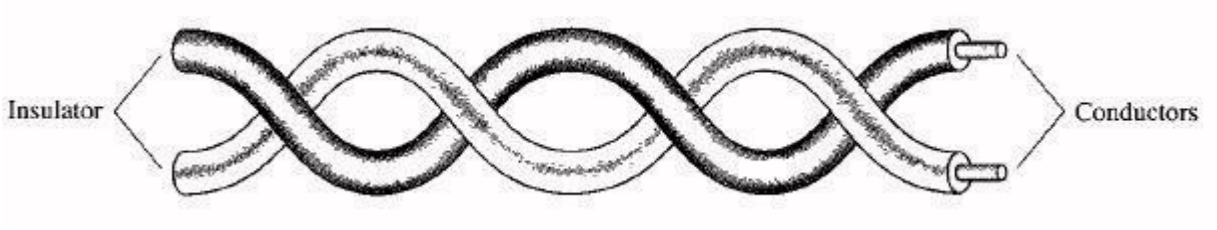
A signal traveling along any of these media is directed and contained by the physicallimits of the medium.

Features:

- High Speed
- Secure
- Used for comparatively shorter distances

Ex: twisted-pair cable, coaxial cable, and fiber-optic cable

i) **Twisted-Pair Cable:**

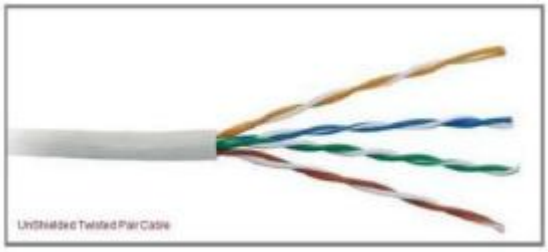


1. A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.
2. One of the wires is used to carry signals to the receiver, and the other is used only asa ground reference. The receiver uses the difference between the two.

CATEGORIES/TYPES/KINDS:

1. Unshielded twisted Pair Cable (UTP)
2. Shielded Twisted-Pair Cable (STP)

1.Unshielded twisted Pair Cable (UTP):



1. The most common twisted-pair cable used in communications is referred to asUnshielded twisted-pair (UTP).
2. It consists of two conductors usually copper which is covered by plastic insulator.
3. Two wires are twisted one over the other at regular interval to decrease the noise anddisturbances. So that at the receiving end the receiver will get the desired information.

Advantages:

1. It is easy to use and flexible.
2. It is cheap.
3. It is easy to install.

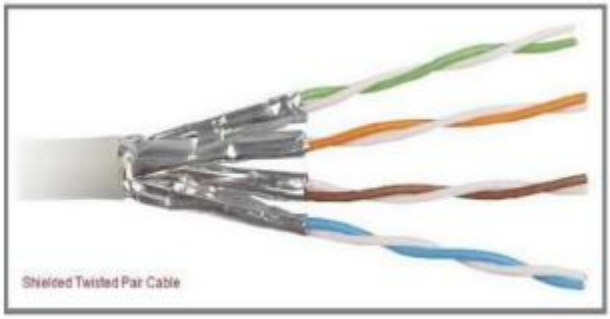
Disadvantages:

1. Susceptible to external interference
2. Lower capacity and performance in comparison to STP
3. Short distance transmission due to attenuation

Applications:

1. Is used in telephone lines to provide voice and data channels.
2. The most commonly used connecter is RJ 45 (Register jack).

2.Shielded Twisted-Pair Cable (STP):



1. STP cable has a metal foil or braided mesh covering that encases each pair ofinsulated conductors.
2. It eliminates crosstalk.
3. Here the metal foil is connected to the ground and other connection are same as UTP.

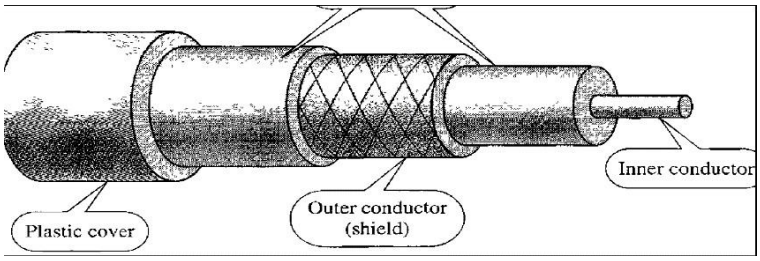
Advantages:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparitively faster

Disadvantages:

- Comparitively difficult to install and manufacture
- More expensive
- Bulky

ii) Coaxial Cable:



1. Coaxial cable (or coax) carries signals of higher frequency ranges than those in twistedpair cable, in part because the two media are constructed quite differently.
2. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in anouter conductor of metal foil, braid, or a combination of the two.
3. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.
4. This outer conductor is also enclosed in an insulating sheath, and the whole cable isProtected by a plastic cover.
5. Coax carries signals of higher frequency ranges (i.e. 100 KHz – 500MHz) than thosein twisted pair cable, in part because the two media are constructed quite differently.
6. Coaxial cables categorized by their radio government (RG) ratings.

APPLICATION:

1. Coaxial cable was widely used in analog telephone networks where a single coaxialnetwork could carry 10,000 voice signals.
   Cable TV networks also use coaxial cables.
2. Another common application of coaxial cable is in traditional Ethernet LANs.
3. Connectors used: Barrel connector, T-connector, Terminator
   Advantages:

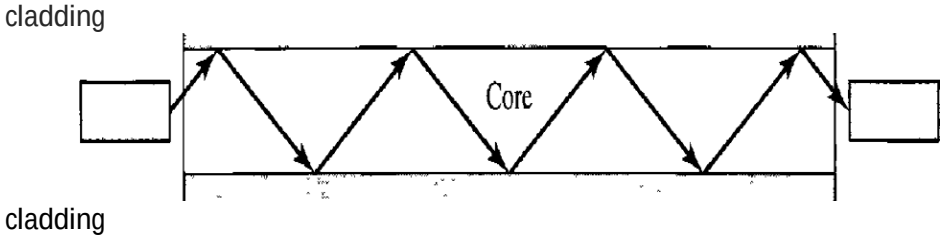
- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantages:

- Single cable failure can disrupt the entire network

iii) Optical Fiber Cable:

1. A fiber-optic cable is made of glass or plastic and transmits signals in the formof light.
2. Optical fibers use reflection to guide light through a channel.
3. A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
4. The difference in density of the two materials must be such that a beam of lightmoving through the core is reflected off the cladding instead of being refractedinto it.



Applications:

1. Fiber-optic cable is often found in backbone networks because its wide bandwidth isCost-effective.
2. Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-Xalso use fiber-optic cable.

Advantages : Fiber-optic cable has several advantages over metallic cable (twisted pairor coaxial).

1. Higher bandwidth.
2. Less signal attenuation.
3. Noise resistance
4. Light weight.

Disadvantages: There are some disadvantages in the use of optical fiber.

1. Installation and maintenance. Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
2. Unidirectional light propagation. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
3. Cost. The cable and the interfaces are relatively more expensive than those of otherguided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.
4. Fragility: Glass fiber is more easily broken than wire which makes it less useful, where hardware portability is required.

2.UNGUIDED MEDIA:

- Unguided transmission involves the mode of communication by means of electro-magnetic waves without using physical conductor.
- Signals are normally broadcast through free space and the receiver are allowed tocapture the signals by using an antenna.

Features:

- Signal is broadcasted through air
- Less Secure
- Used for larger distances

Types of wireless transmission:-

1. Radio wave

2. Micro wave
3. Infra red

Radio waves:-

- The radio waves are omni-directional.
- When the antenna transmits radio waves they are propagated in all direction.
- The frequencies it transmits can penetrate the wall.
- It transmits in two ways i.e Amplitude modulation (AM) and frequencymodulation(FM).
- The bandwidth of the radio waves is 3KHz to 3000GHz.
- Radio waves are used for multi-cast communication such as radio, television and livestreaming.

Radio Frequency Spectrum

The radio spectrum is divided into bands based on frequency.

Three important bands for communication are: HF, VHF, UHF.HF: High frequency (HF) is the ITU designation[1][2] for the band of radio aves with frequency between 3 and 30 megahertz (MHz). These frequencies can be used for long-distance communication across intercontinental distances and for mountainous terrains which prevent line-of-sight communications.

Advantages

- Long-range communication with low power
- No need for line-of-sight
- Covers oceans and remote areas

Disadvantages

- Signal fading and noise
- Large antenna required (¼ wave = 10–25 m)
- Limited bandwidth → mainly voice & Morse code

Applications

- *Amateur Radio (Ham Radio)*
- *International Shortwave Broadcasting (BBC, Voice of America)*
- *Maritime & Aviation communication*
- *Military long-range communication*
- *Emergency & Disaster communication (e.g., during cyclones)*

VHF Band (30–300 MHz)

Propagation Characteristics

- *Line-of-Sight (LOS): Signals travel in straight line → limited by Earth's curvature.*
- *Range: Typically 50–150 km (can extend with height/repeaters).*
- *Tropospheric Scattering/Ducting: Occasional long-range during weather inversion.*
- *Minimal Ionospheric Reflection.*

Advantages

- *Clear audio quality (FM)*
- *Moderate antenna size (¼ wave = 0.5–2.5 m)*
- *Less interference than HF*
- *Good for mobile communication*

Disadvantages

- *Limited range (needs repeaters for wide coverage)*
- *Blocked by hills, buildings*

Applications

- *FM Radio Broadcasting (88–108 MHz)*
- *Television Channels (VHF Low: 54–88 MHz, VHF High: 174–216 MHz)*
- *Two-Way Radio (Police, Fire, Taxi)*
- *Marine VHF Radio (156–162 MHz – Channel 16 emergency)*
- *Aircraft Communication (118–137 MHz)*
- *Amateur Radio (2-meter band: 144–148 MHz)*

Example: Your car FM radio uses VHF band.

UHF Band (300–3000 MHz)

Propagation Characteristics

- *Strict Line-of-Sight: Very limited range (30–100 km).*
- *Penetrates buildings better than higher bands.*
- *Absorbed by rain, foliage.*
- *High bandwidth → supports video & data.*

Advantages

- *Small antenna size (¼ wave = 5–25 cm)*
- *High data rate*
- *Less interference*
- *Ideal for dense urban areas*

Disadvantages

- *Very short range*
- *Easily blocked by obstacles*
- *Higher power consumption*

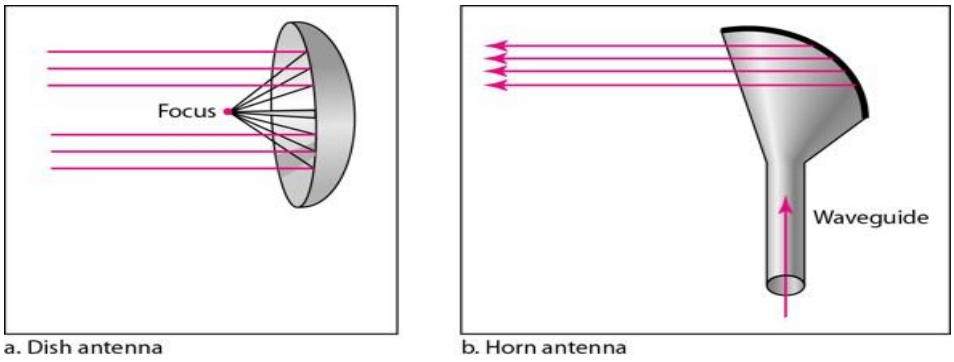
Applications

- *Television Broadcasting (UHF Channels: 470–694 MHz in many countries)*
- *Mobile Phones (GSM, 4G, 5G in lower UHF)*

- *Wi-Fi (2.4 GHz is technically SHF, but often grouped near UHF)*
- *Cordless Phones, Walkie-Talkies*
- *GPS (L1: 1575 MHz, L2: 1227 MHz)*
- *Microwave Ovens (2.45 GHz – ISM band)*
- *Bluetooth, RFID, Satellite TV (Ku band starts at 12 GHz, but UHF used in some downlinks)*
  Example: DTH satellite dish receives UHF signals from set-top box to TV.

Micro waves:-

- The electromagnetic waves having frequencies 1-30GHz are known asmicrowaves.
- These waves are unidirectional.
- When an antenna transmits microwaves they can be narrowly focused.
- This means that sending and receiving antenna need to be aligned.
- Microwaves propagation follows line-of-sight propagation mode.
- It transmits very high frequency range.
- The bandwidth of this propagation is relatively wide. So, sub-bands can beassigned in between them.
  Two types of antenna are used:- a-parabolic dish antenna b-horn antenna.a:-parabolic dish antenna



a. Dish antenna b. Horn antenna

- These are used in cellular network and satellite network and also incase of wireless LAN.

Ku Band:

In computer networks, the Ku-band (12-18 GHz) is a microwave frequency range crucial for satellite communications, enabling applications like direct-to-home TV, VSATs for remote internet/data, and backhaul, offering a good balance of capacity and coverage with smaller dishes, though it's more prone to rain fade than C-band but less than Ka-band.

Key Characteristics

- **Frequency:** 12 to 18 GHz.
- **Wavelength:** 1.67 to 2.5 cm.
- **Origin:** "K-under" (German for "K-below"), as it sits below the K-band.

Applications in Networking

Ku band is one of the most widely used bands for commercial satellite services:

- **Direct-to-Home (DTH) Satellite Television:** The dominant band for broadcasting hundreds of TV channels (e.g., Dish TV, DirecTV). It delivers high-quality video and audio to small home dishes (typically 60–90 cm).

- **VSAT (Very Small Aperture Terminal) Networks:** Two-way data communication for broadband internet, enterprise networking, remote monitoring, and point-of-sale systems. Common in rural areas, ships, and aircraft.
- **Satellite News Gathering (SNG):** Live broadcasts from remote locations.
- **Backhaul**: Linking remote cell towers or studios to main networks.
- **Maritime and Aeronautical Connectivity:** On ships and planes for internet and voice.
- **Other:** Space communications (e.g., NASA TDRS for ISS), police speed radar (in some regions).

Examples: Starlink uses Ku-band for user terminals; many GEO satellites (e.g., SES, Intelsat) have Ku-band transponders.

Advantages

- **Smaller Antennas:** High power allows for smaller, more affordable dishes.
- **Coverage:** Offers wide geographic coverage.
- **Cost-Effective:** Generally more economical for users compared to Ka-band.
  Higher Bandwidth/Data Rates: Supports HD/4K video and faster internet compared to lower bands.

Disadvantages:

- **Rain Fade:** More affected by heavy rain than C-band, but less than Ka-band.
- **Weather Impact:** High frequencies can suffer signal attenuation (rain fade).

  Narrower Beam: Requires precise pointing; slight misalignment causes signal loss.

Infra-red:-

- Infra-red frequency ranges from (300 GHz-400THz).
- It is used for short range communication.
- These frequencies cannot penetrate any type of obstacles.
- It also works in the mode of line-of-sight propagation.
  For example:- the communication between remote to a device.

Data link Layer:

The data link layer transforms the physical layer, a raw transmission facility, to a link responsible for node-to-node (hop-to-hop) communication. Specific responsibilities of the data link layer include framing, addressing, flow control, error control, and media access control. The data link layer divides the stream of bits received from the network layer into manageable data units called frames. The data link layer adds a header to the frame to define the addresses of the sender and receiver of the frame.

Functions of the Data Link Layer

Function	Description
Framing	Divides the stream of bits into manageable units called *frames*.
Physical Addressing	Adds hardware (MAC) addresses of the sender and receiver to each frame.
Error Detection and Correction	Detects and sometimes corrects errors caused by noise or signal loss.
Flow Control	Prevents the sender from overwhelming the receiver with too much data.
Access Control (MAC)	Determines which device has control over the communication channel at a given time.
Reliability	Ensures reliable frame delivery using acknowledgment and retransmission techniques.

Design Issues of Data Link Layer

The key design issues involve how data is packaged, transmitted, and managed across a shared link.

a) Framing

- Process of dividing data into frames for easier transmission and error checking.
- Methods:
  - Character count
  - Byte stuffing
  - Bit stuffing
  - Physical layer coding violations

b) Flow Control

- Ensures sender does not send frames faster than the receiver can process.
- Techniques:
  - Stop-and-Wait protocol
  - Sliding Window protocol

c) Error Control

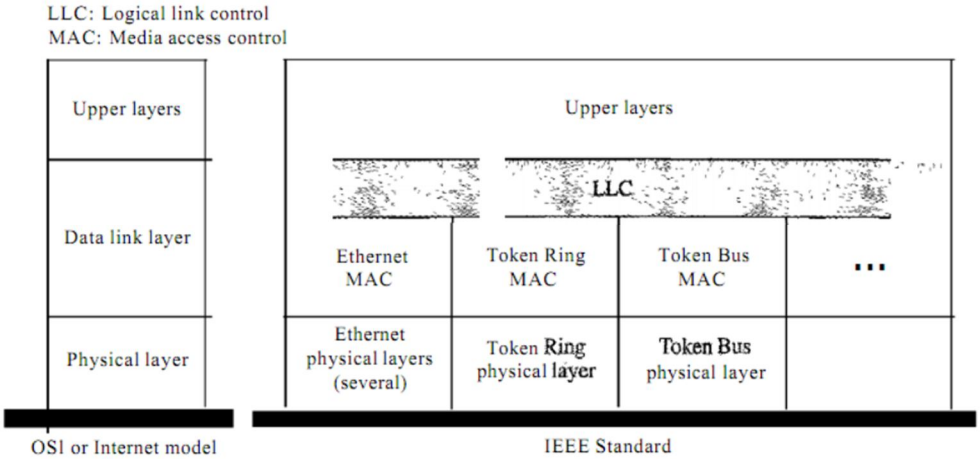
- Deals with detection and retransmission of lost or corrupted frames.
- Techniques:
  - Parity check, Checksum, CRC (Cyclic Redundancy Check)
  - ARQ (Automatic Repeat reQuest) methods:
    - Stop-and-Wait ARQ
    - Go-Back-N ARQ
    - Selective Repeat ARQ

d) Access Control (MAC - Medium Access Control)

- Controls how multiple devices share a common channel.
- Two main approaches:
  - Controlled Access: Polling, Token Passing
  - Random Access: ALOHA, CSMA/CD, CSMA/CA

IEEE STANDARDS

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers.



Protocols at Data Link Layer

(A) Ethernet (IEEE 802.3)

The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC). Since then, it has gone through four generations: Standard Ethernet (Iot Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (I Gbps), and Ten-Gigabit Ethernet (I0 Gbps),

It is the most widely used wired LAN protocol.

It uses CSMA/CD (Carrier Sense Multiple Access with Collision Detection) for channel access.

Types of Ethernet

1. Fast Ethernet

- **Speed:** 100 Mbps
- **Media:** Twisted pair (CAT5) and fiber optic cables

- **Variants:** 100BASE - TX, 100BASE - FX, 100BASE - T4

2. Gigabit Ethernet

- **Speed:** 1 Gbps (1000 Mbps)
- **Media:** CAT5e, CAT6, and fiber optic cables
- Common in modern office and home networks

3. 10 - Gigabit Ethernet

- **Speed:** 10 Gbps
- **Media:** CAT6a, CAT7, and fiber optic cables
- Supports long distances (up to 10 km with fiber)
- Widely used in data centers and enterprise backbones

4. Switch Ethernet

- Uses network switches for dedicated connections
- Each device gets a separate collision domain
- Supports speeds from 10 Mbps to 10 Gbps

MAC Address: 48-bit unique hardware address (e.g., 00-1A-2B-3C-4D-5E)

Frame Format:

Field	Description
Preamble	Synchronization bits
Destination MAC	Receiver's address
Source MAC	Sender's address
Type/Length	Indicates protocol type (e.g., IPv4)
Data	Actual payload
CRC	Error detection field

Operation:

1. Station listens to the medium before sending (Carrier Sense).
2. If channel is idle → transmits frame.
3. If collision occurs → stops, waits for random backoff time, and retries.

(B) Wireless LAN (IEEE 802.11 / Wi-Fi)

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).

The BSS without anAP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture. In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an infrastructure network.

An extended service set (ESS) is made up of two or more BSSs with APs. the BSSs are connected through a distribution system, which is usually a wired LAN. the extended service set uses two types of stations: mobile and stationary.

The extended service set uses two types of stations: mobile and stationary.

Features:

- Provides wireless connectivity using radio waves.
- Operates in 2.4 GHz or 5 GHz frequency bands.
- Follows CSMA/CA (Collision Avoidance) mechanism because collision detection is hard in wireless.

Architecture:

1. Basic Service Set (BSS) – Single access point with associated stations.
2. Extended Service Set (ESS) – Multiple access points interconnected.
3. Ad-hoc Mode – Direct device-to-device communication without AP.

Key Components:

- Access Point (AP): Connects wireless stations to wired network.

- Station (STA): Wireless device like laptop, phone, etc.

Frame Types:

- Management frames: Establish and maintain connections.
- Control frames: Control access to the medium.
- Data frames: Carry actual user data.

Features:

- Mobility and flexibility
- Encryption support (WEP, WPA, WPA2, WPA3)
- Data rates: 11 Mbps (802.11b) → several Gbps (802.11ax – Wi-Fi 6)

(C) Bluetooth (IEEE 802.15.1)

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on.

A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet.

The latest version of Bluetooth is Bluetooth 5.4 with 2Mbps speed.

- It is a short-range wireless communication technology for connecting devices (PAN – Personal Area Network).
- It operates in the 2.4 GHz ISM band.
- Uses frequency hopping spread spectrum (FHSS) to reduce interference.

Architecture:

- It forms piconet where there is one master and up to seven active slave devices.
- There is also possibility of interconnection of multiple piconets known as scatternet.

Features:

- Range: ~10 meters (can extend up to 100 m for Class 1 devices)
- Data rate: Up to 3 Mbps (Bluetooth 2.0) and higher for newer versions.
- Low power consumption (ideal for IoT, wearables, etc.)

  It is low cost.

  It supports voice and data.

Applications:

- Wireless headsets and earphones
- File transfer between phones/laptops
- Smart devices and IoT communication

SWITCHING:

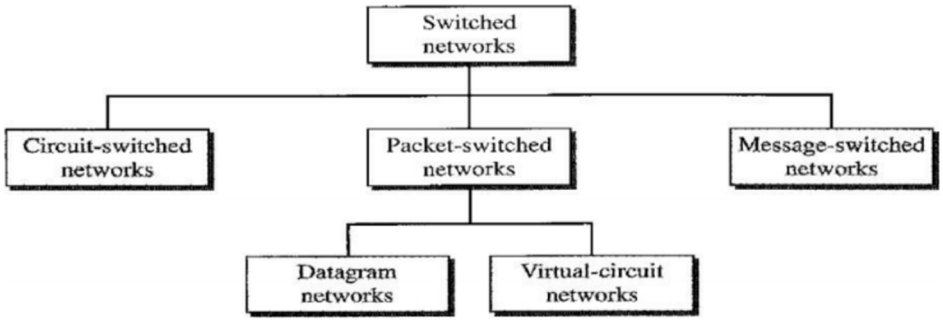
• A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch.

• The process by which data are transmitted from one node to the other via a switched network is called switching.

The end systems (communicating devices) are labeled A, B, C, D, and so on, and the switches are labeled I, II, III, IV, and V. Each switch is connected to multiple links.

TYPES:

1. Circuit switching
2.Packet switching
3.Message switching.



CIRCUIT-SWITCHED NETWORKS

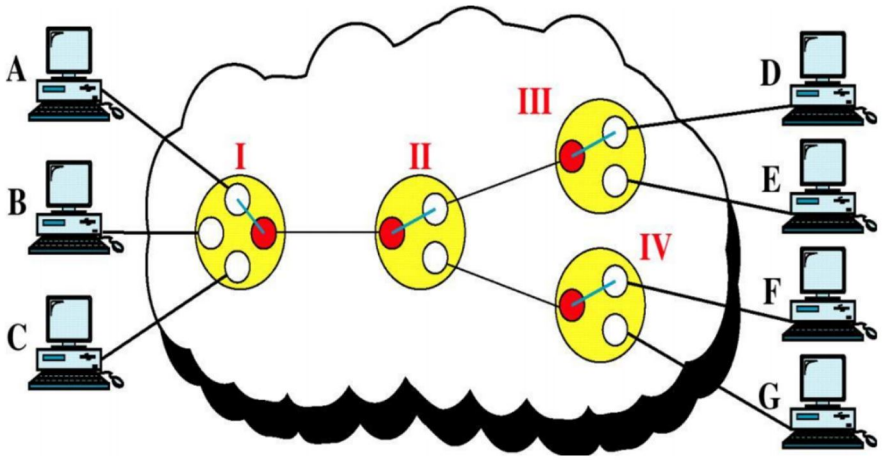
- A circuit-switched network consists of a set of switches connected by physical links.
- A connection between two stations is a dedicated path made of one or more links.

However, each connection uses only one dedicated channel on each link. Each link is normally divided into n channels by using FDM or TDM.

Circuit switching takes place at the physical layer.

Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and receive by the destination station, although there may be periods of silence.

There is no addressing involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM). Of course, there is end-to- end addressing used .



Three Phases

The actual communication in a circuit-switched network requires three phases: connection setup, data transfer, connection teardown.

Setup Phase

Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches.

Data Transfer Phase

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase

When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

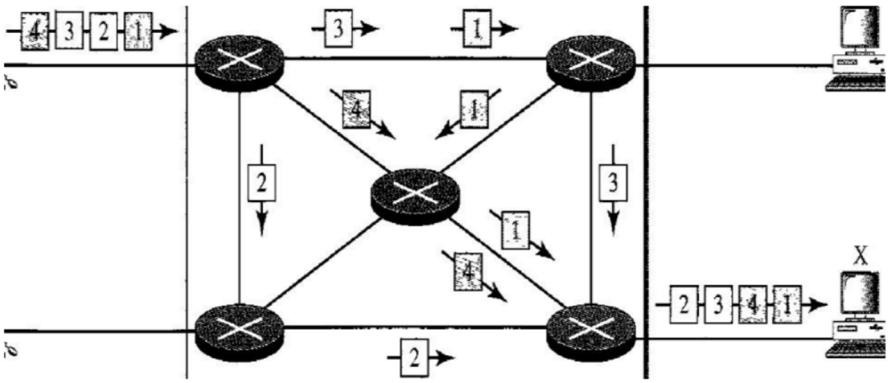
PACKET SWITCHED NETWORK

- In this switching network data are transmitted in discrete units called as packets.
- The problems associated with circuit switching like non voice and data transmission problem was successfully overcome in packet switching.
- In packet switching there is no resource allocation for the packets. The allocation is done on first come first serve basis.
- There are two popular approaches for packet switching.

- Datagram approach
- Virtual circuit approach

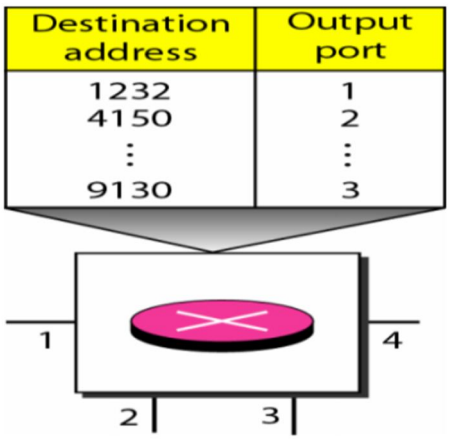
DATAGRAM NETWORKS

- In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multipacket transmission, the network treats it as though it existed alone. Packets in this approach are referred to as data grams.
- Datagram switching is normally done at the network layer.
- The switches in a datagram network are traditionally referred to as routers.
- The datagram networks are sometimes referred to as connectionless networks. The term connectionless here means that the switch (packet switch) does not keep information about the connection state. There are no setup or teardown phases. Each packet is treated the same by a switch regardless of its source or destination.



Routing Table

- Each packet switch has a routing table which is based on the destination address.
- The routing tables are dynamic and are updated periodically.
- The destination addresses and the corresponding forwarding output ports are recorded in the tables.
- The destination address in the header of a packet in a datagram network remains the same during the entire journey of the packet.
- When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded.



Efficiency

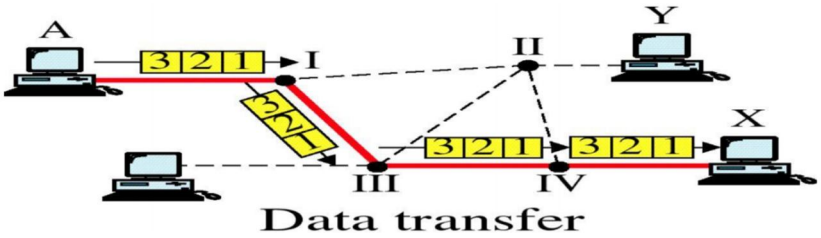
- Better than that of a circuit-switched network.
- Resources are allocated only when there are packets to be transferred. If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be reallocated during these minutes for other packets from other sources.
- Switching in the Internet is done by using the datagram approach to packet switching at the network layer

VIRTUAL-CIRCUIT NETWORKS

- A virtual-circuit network is a cross between a circuit-switched network and a datagram

network. It has some characteristics of both.

- As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.
- Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
- As in a circuit-switched network, all packets follow the same path established during the connection.
- A virtual-circuit network is normally implemented in the data link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer. But this may change in the future.



Data transfer

Addressing In a virtual-circuit network,
It has two types of addressing are involved: global and local (virtual-circuit identifier).
Global Addressing:
A source or a destination needs to have a global address, an address that can be unique in the scope of the network or internationally if the network is part of an international network.
Virtual-Circuit Identifier:
The identifier that is actually used for data transfer is called the virtual-circuit identifier (VCI). A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves it has a different VCI.
Three Phases
As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown.
Setup phase
In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection.
Data Transfer Phase and teardown phase

- To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit.
- The table, in its simplest form, has four columns. This means that the switch holds four pieces of information for each virtual circuit that is already set up.
- The data transfer phase is active until the source sends all its frames to the destination. The process creates a virtual circuit, not a real circuit, between the source and destination.
- After sending all frames, a special frame is send to end the connection
- Destination B responds with a teardown confirmation frame

Differences between Circuit switching and Packet switching

CIRCUIT SWITCHING	***PACKET SWITCHING***
1. In circuit switching a message path or data communication path or channel or circuit is dedicated to an entire message .	1. In this switching network data are transmitted indiscrete units called as packets.
2. Circuit-switching is more reliable than packet-switching	2. Packet-switching is less reliable than circuit-switching
3.circuit switching statically reserves the requiredbandwidth	3.packet switching acquires & releases it as it isneeded

4. In circuit switching, path is dedicated for thetransmission.	4. In packet switching, route can be shared fordifferent transmission.
5. With circuit switching any unused bandwidth ona allocated circuit is just wasted.	5. with packet switching any unused bandwidthmay be utilized by other packets
6. Circuit switching is old and expensive.	6. Packet switching is more modern.

UNIT - 3

NETWORK LAYER AND ROUTING PROTOCOL

Design issues:

The design of the network layer involves several critical issues to ensure efficient, reliable, and scalable communication across networks.

1. Store-and-Forward Packet Switching

- The network layer uses **packet switching** to send data in small, independent packets.
- Each router **receives**, **stores**, and then **forwards** the packet to the next hop.
- Design concern: minimizing **delay** and **congestion** while maintaining reliability.

2. Services Provided to the Transport Layer

Two main types of services can be offered:

Service Type	Description	Example
Connection-Oriented Service	A logical path is established before data transfer.	Virtual Circuit (used in ATM, MPLS)
Connectionless Service	Each packet is treated independently, without setup.	Datagram (used in IP)

Design Issue: Deciding whether to use a *connection-oriented* or *connectionless* model affects reliability, overhead, and speed.

3. Routing Algorithms

Routing is the **process of selecting paths** for data to travel across networks.

Key Design Goals:

- **Efficiency:** Choose the shortest or least-cost path.
- **Adaptivity:** Adjust routes when network conditions change.
- **Scalability:** Handle large and complex networks.
- **Fairness:** Distribute network load evenly.

Types of Routing:

Type	Description
Static Routing	Manually configured routes that do not change.
Dynamic Routing	Routes change automatically based on network conditions (e.g., OSPF, RIP).
Hierarchical Routing	Large networks divided into regions for manageability.
Broadcast / Multicast Routing	One-to-many or many-to-many communication.

4. Congestion Control

- Occurs when **too many packets** are in the network, causing **delays and packet loss**.
- The network layer must control traffic to keep performance optimal.

Methods:

- **Buffer management:** Limit packet queues.
- **Traffic shaping:** Regulate data flow.
- **Load shedding:** Drop packets when overloaded.
- **Feedback signals:** Inform sender to slow down.

5. Internetworking

- Refers to connecting **different types of networks** (e.g., LANs, WANs) together.
- The network layer must handle **heterogeneity**, including:

- Different addressing schemes
- Different packet sizes (MTU)
- Different protocols (Ethernet, Wi-Fi, etc.)

Solution:

- Use of **IP (Internet Protocol)** to provide a **universal addressing and routing scheme**.

6. Fragmentation and Reassembly

- Different networks may have different **Maximum Transmission Units (MTUs)**.
- The network layer must **fragment** large packets and **reassemble** them at the destination.

Example:

If Ethernet supports 1500 bytes and the IP packet is 4000 bytes →
IP divides it into smaller fragments.

Design Issue: Maintaining fragment order and efficiency during reassembly.

8. Addressing

- Each device on the network must have a **unique logical address** (e.g., IP address).
- Network layer handles:
  - **Address assignment**
  - **Address mapping** (e.g., ARP)
  - **Subnetting and supernetting**

Design Issue: Creating a scalable and hierarchical addressing system.

The Network Layer is the third layer in the OSI (Open Systems Interconnection) model.
It lies above the Data Link Layer and below the Transport Layer.

Routing: Determines the best path for packet transmission from source to destination.

Logical Addressing: Assigns unique IP addresses to identify devices on the network.

Packet Forwarding: Moves packets through routers based on routing tables.

Fragmentation and Reassembly: Splits large packets into smaller ones suitable for the data link layer, then reassembles them.

Error Handling and Diagnostics: Manages routing errors and provides error reporting (e.g., ICMP).

Logical Addressing:

A logical address is a network layer address (usually an IP address) used to identify a device on a network independently of the physical hardware.

- It is assigned by software (not burned into hardware like MAC address).
- Used for communication between different networks.

Physical vs. Logical Address

Feature	Physical Address (MAC)	Logical Address (IP)
Layer	Data Link Layer	Network Layer
Nature	Hardware-based (fixed)	Software-based (assigned)
Format	48-bit hexadecimal (e.g., 00:1A:C2:9B:00:68)	32-bit (IPv4) or 128-bit (IPv6)
Purpose	Identifies device on local network (LAN)	Identifies device globally across networks
Assigned By	Manufacturer (in NIC)	Network administrator or ISP
Example	00:0A:E6:3E:FD:E1	192.168.1.10

The Internet addresses are 32 bits in length; this gives us a maximum of 232 addresses. These addresses are referred to as IPv4 (IP version 4) addresses or simply IP addresses if there is no confusion.
For addressing more number of devices new addressing format is used i.e IPv6 which is of 128bit length.

IPv4 ADDRESSES

IPv4 addresses are unique. They are unique in the sense that each address defines one, and only one, connection to the Internet. Two devices on the Internet can never have the same address at the same time.
An IPv4 address is 32 bits long.

Address Space

A protocol such as IPv4 that defines addresses has an address space. An address space is the total number of addresses used by the protocol. If a protocol uses N bits to define an address, the address space is 2N because each bit can have two different values (0 or 1) and N bits can have 2N values.
IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4 billion). This means that, theoretically, if there were no restrictions, more than 4 billion devices could be connected to the Internet.

Notations

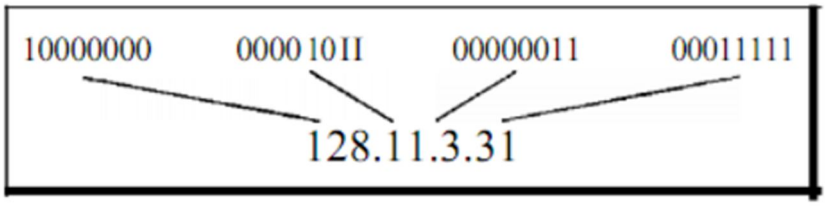
There are two prevalent notations to show an IPv4 address: binary notation and dotted-decimal notation.

Binary Notation

In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address. The following is an example of an IPv4 address in binary notation:
01110101 10010101 00011101 00000010

Dotted-Decimal Notation

To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. The following is the dotted~decimal notation of the above address:
117.149.29.2
each number in dotted-decimal notation is
a value ranging from 0 to 255.



Example 19.1

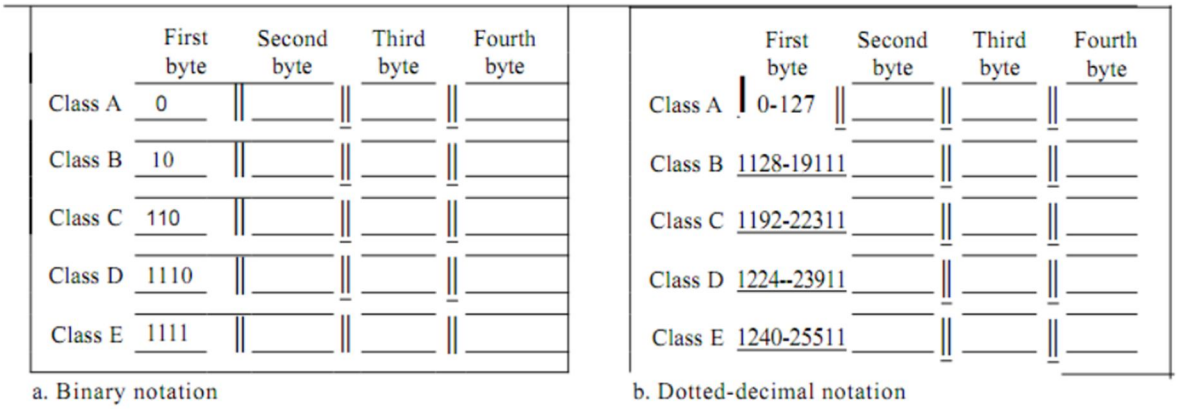
Change the following IPv4 addresses from binary notation to dotted-decimal notation.
a. 10000001 00001011 00001011 11101111
b. 11000001 10000011 00011011 11111111
Solution
a. 129.11.11.239
b. 193.131.27.255

Example 19.2

Change the following IPv4 addresses from dotted-decimal notation to binary notation.
a. 111.56.45.78
b. 221.34.7.82
Solution
We replace each decimal number with its binary equivalent (see Appendix B).
a.• 01101111 00111000 00101101 01001110
b. 11011101 00100010 00000111 01010010

Classful Addressing:

In classful addressing, the address space is divided into five classes:
A, B, C, D, and E.
We can find the class of an address when given the address in binary notation or dotted-decimal notation. If the address is given in binary notation, the first few bits can immediately tell us the class of the address. If the address is given in decimal-dotted notation, the first byte defines the class. Both methods are shown in Figure 19.2.



Example 19.4
Find the class of each address.
a. 00000001 00001011 00001011 11101111
b. 11000001 10000011 00011011 11111111
c. 14.23.120.8
d. 252.5.15.111
Solution
a. The first bit is O. This is a class A address.
b. The first 2 bits are 1; the third bit is O. This is a class C address.
c. The first byte is 14 (between 0 and 127); the class is A.
d. The first byte is 252 (between 240 and 255); the class is E.
Classes and Blocks
One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size as shown in Table 19.1.

Class	*Number ofBlocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

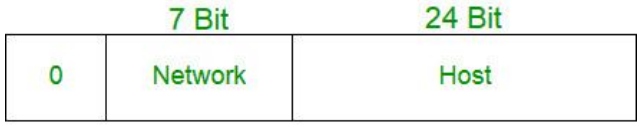
In c1assfnl addressing, a large part of the available addresses were wasted.

Class A

- Class A IP addresses are assigned to networks that require a very large number of hosts.
- The network ID in Class A is 8 bits long, while the host ID is 24 bits long.
- The most significant bit (MSB) of the first octet is always 0, and the remaining 7 bits are used to identify the network.
- The 24-bit host ID uniquely identifies hosts within the same network.
- The default subnet mask for Class A is 255.0.0.0.
- The total number of usable host addresses per network is 224 – 2 = 16,777,214 (excluding network and

broadcast addresses).

- The IP address range for Class A is 0.0.0.0 to 127.255.255.255.



Class A

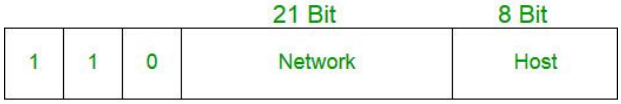
Class B

- Class B IP addresses are assigned to medium to large-sized networks.
- The network ID is 16 bits long, and the host ID is also 16 bits long.
- The first two bits of the first octet are always 10, which identifies a Class B address.
- The remaining 14 bits are used to determine the network ID.
- The 16-bit host ID uniquely identifies hosts within the same network.
- The default subnet mask for Class B is 255.255.0.0.
- The total number of Class B networks is 214 = 16,384 networks.
- The total number of usable host addresses per network is 216 – 2 = 65,534 hosts.
- The IP address range for Class B is 128.0.0.0 to 191.255.255.255.

Class B

Class C

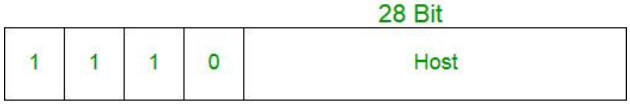
- Class C IP addresses are assigned to small-sized networks.
- The network ID is 24 bits long, while the host ID is 8 bits long.
- The first three bits of the first octet are always 110, which identifies a Class C address.
- The remaining 21 bits are used to determine the network ID.
- The 8-bit host ID uniquely identifies hosts within the same network.
- The default subnet mask for Class C is 255.255.255.0.
- The total number of Class C networks is 2^{21} = 2,097,152 networks.
- The total number of usable host addresses per network is 2^8 – 2 = 254 hosts.
- The IP address range for Class C is 192.0.0.0 to 223.255.255.255.



Class C

Class D

- Class D IP addresses are reserved for multicast communication.
- The first four bits of the first octet are always 1110, which identifies a Class D address.
- The remaining 28 bits are used to represent the multicast group address that interested hosts can join.
- Class D addresses do not have a network ID or host ID division.
- No subnet mask is defined for Class D addressing.
- The IP address range for Class D is 224.0.0.0 to 239.255.255.255.



Class D

Class E

- Class E IP addresses are reserved for experimental and research purposes.
- The first four bits of the first octet are always 1111, which identifies a Class E address.
- Class E addresses do not have network ID and host ID divisions.
- No subnet mask is defined for Class E addressing.
- The IP address range for Class E is 240.0.0.0 to 255.255.255.255.

Class E

Range of Special IP Addresses

- **169.254.0.0 – 169.254.255.255**
  Used as **link-local addresses** when a device cannot obtain an IP address from a DHCP server.
- **127.0.0.0 – 127.255.255.255**
  Reserved for **loopback addresses**, used to test network functionality on the local machine.
- **0.0.0.0 – 0.255.255.255 (0.0.0.0/8)**
  Represents the **current network** and is used during initialization before a device is assigned a valid IP address.

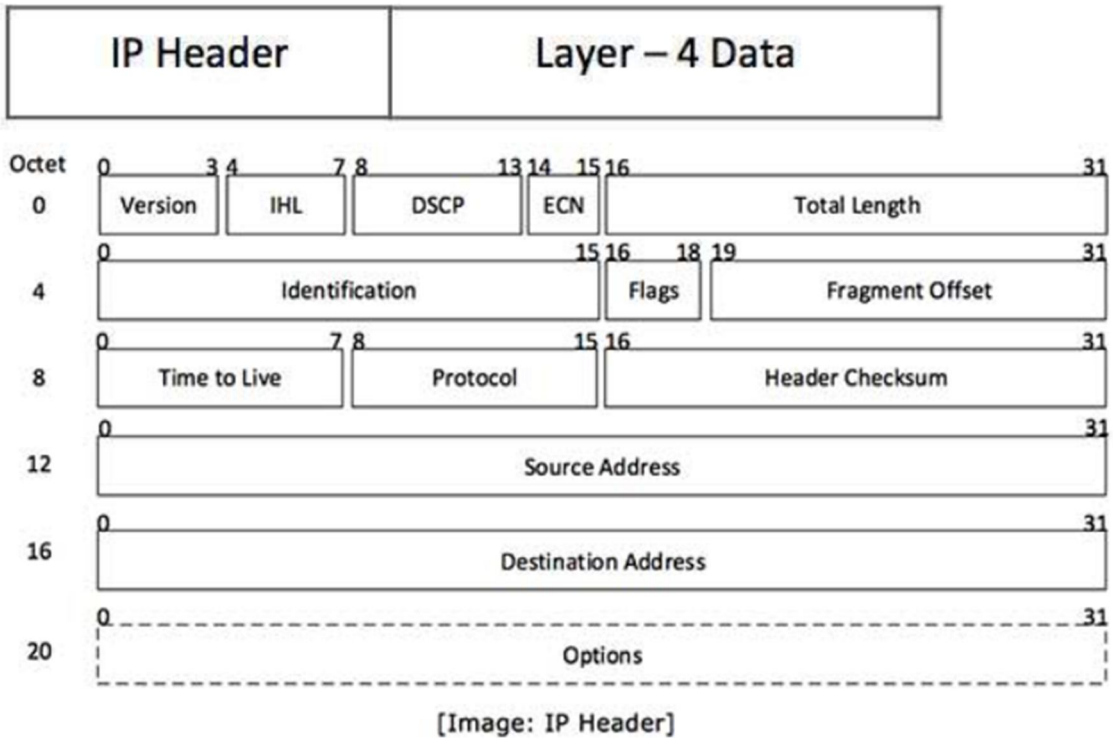
Limitations of Classful Addressing

1. **Wastage of IP Addresses:**
   - Organizations often received more IPs than needed.
   - Example: A company needing 1000 IPs had to take a whole Class B network (65,534 IPs).
2. **Inflexibility in Network Design:**
   - Fixed class boundaries (A, B, C) made efficient subnetting difficult.
3. **IP Address Exhaustion:**
   - Rapid growth of the internet quickly consumed available addresses.

Classful addressing was replaced by **Classless Inter-Domain Routing (CIDR)** — which allows **variable-length subnet masking (VLSM)** for better IP utilization.

Internet Protocol Version 4 (IPv4)

Internet Protocol is one of the major protocols in the TCP/IP protocols suite. This protocol works at the network layer of the OSI model and at the Internet layer of the TCP/IP model. Thus this protocol has the responsibility of identifying hosts based upon their logical addresses and to route data among them over the underlying network.
IPv4 is an unreliable and connectionless datagram protocol-a best-effort delivery
service. The term best-effort means that IPv4 provides no error control or flow control
If reliability is important, IPv4 must be paired with a reliable protocol such as TCP.
Packets in the IPv4 layer are called datagrams.
A datagram is a variable-length packet consisting of two parts: header and data.
The header is 20 to 60 bytes in length and contains information essential to routing and delivery.



[Image: IP Header]

- **Version** – Version no. of Internet Protocol used (e.g. IPv4).
- **IHL** – Internet Header Length; Length of entire IP header.
- **DSCP** – Differentiated Services Code Point; this is Type of Service.
- **ECN** – Explicit Congestion Notification; It carries information about the congestion seen in the route.
- **Total Length** – Length of entire IP Packet (including IP header and IP Payload).
- **Identification** – If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.
- **Flags** – As required by the network resources, if IP Packet is too large to handle, these flags tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to 0.
- **Fragment Offset** – This offset tells the exact position of the fragment in the original IP Packet.
- **Time to Live** – To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- **Protocol** – Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- **Header Checksum** – This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- **Source Address** – 32-bit address of the Sender (or source) of the packet.
- **Destination Address** – 32-bit address of the Receiver (or destination) of the packet.
- **Options** – This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.