UNIT 1
INTRODUCTION

Introduction to Computer Networks

- A set of devices often mentioned as nodes connected by media link is called a Network.
- A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called Communication channels.
- Computer network is a telecommunication channel using which we can share data with other computers or devices, connected to the same network. It is also called Data Network. The best example of computer network is Internet.
- Computer network does not mean a system with one Control Unit connected to multiple other systems as its slave. That is Distributed system, not Computer Network.
- A network must be able to meet certain criterias, these are mentioned below:
  - Performance
  - Reliability
  - Security

Performance

It can be measured in the following ways:

- **Transit time :** It is the time taken to travel a message from one device to another.
- **Response time :** It is defined as the time elapsed between enquiry and response.

Other ways to measure performance are :

- Efficiency of software
- Number of users
- Capability of connected hardware

Reliability

It decides the frequency at which network failure take place. More the failures are, less is the network's reliability.

Security

It refers to the protection of data from any unauthorised user or access. While travelling through network, data passes many layers of network, and data can be traced if attempted. Hence security is also a very important characteristic for Networks.

Properties of a Good Network

1. **Interpersonal Communication:** We can communicate with each other efficiently and easily. Example: emails, chat rooms, video conferencing etc, all of these are possible because of computer networks.
2. **Resources can be shared:** We can share physical resources by making them available on a network such as printers, scanners etc.
3. **Sharing files, data:** Authorised users are allowed to share the files on the network.

Basic Communication Model
A Communication model is used to exchange data between two parties. For example: communication between a computer, server and telephone (through modem).

Source
Data to be transmitted is generated by this device, example: telephones, personal computers etc.

Transmitter
The data generated by the source system is not directly transmitted in the form its generated. The transmitter transforms and encodes the data in such a form to produce electromagnetic waves or signals.

Transmission System
A transmission system can be a single transmission line or a complex network connecting source and destination.

Receiver
Receiver accepts the signal from the transmission system and converts it into a form which is easily managed by the destination device.

Destination
Destination receives the incoming data from the receiver.

Data Communication
- The exchange of data between two devices through a transmission medium is called Data Communication.
- The data is exchanged in the form of 0's and 1's. The transmission medium used is wire cable.
- For data communication to occur, the communication device must be a part of a communication system.
- Data Communication has two types - Local and Remote which are discussed below:

Local
Local communication takes place when the communicating devices are in the same geographical area, same building, or face-to-face etc.

Remote
Remote communication takes place over a distance i.e. the devices are farther. The effectiveness of a data communication can be measured through the following features :
- **Delivery:** Delivery should be done to the correct destination.
- **Timeliness:** Delivery should be on time.
- **Accuracy:** Data delivered should be accurate.

Components of Data Communication

1. **Message:** It is the information to be delivered.
2. **Sender:** Sender is the person who is sending the message.
3. **Receiver:** Receiver is the person to whom the message is being sent to.
4. **Medium:** It is the medium through which the message is sent. For example: A Modem.
5. **Protocol:** These are some set of rules which govern data communication.

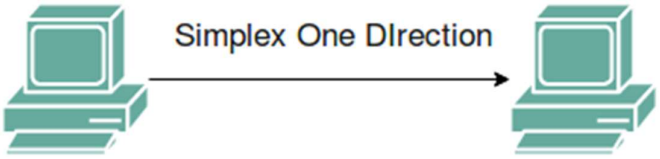
Data Flow

Transmission Modes in Computer Networks (Simplex, Half-Duplex and Full-Duplex)

- Transmission mode means transferring of data between two devices. It is also known as communication mode.
- Buses and networks are designed to allow communication to occur between individual devices that are interconnected.
- There are three types of transmission mode:-
    1. Simplex Mode
    2. Half-Duplex Mode
    3. Full-Duplex Mode

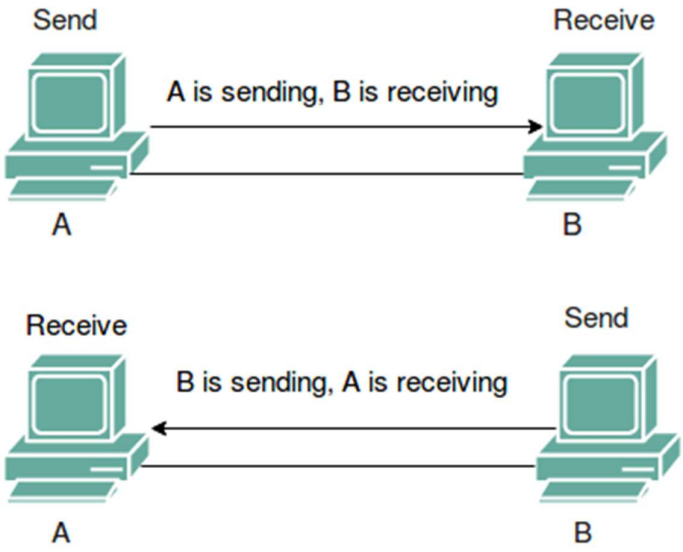
Simplex Mode

- 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 one direction.
- Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.



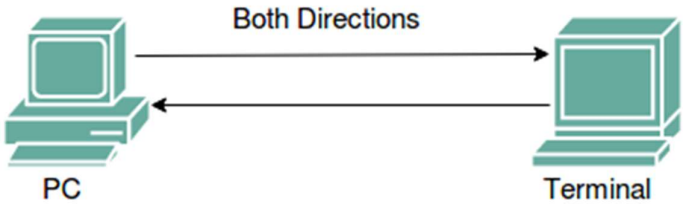
Half-Duplex Mode

- 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.
- The half-duplex mode is used in cases where there is no need for communication in both direction at the same time.
- The entire capacity of the channel can be utilized for each direction.
- Example: Walkie- talkie in which message is sent one at a time and messages are sent in both the directions.



Full-Duplex Mode

- In full-duplex mode, both stations can transmit and receive simultaneously.
- In full_duplex mode, signals going in one direction share the capacity of the link with signals going in other direction, this sharing can occur in two ways:
    1. Either the link must contain two physically separate transmission paths, one for sending and other for receiving.
    2. Or the capacity is divided between signals travelling in both directions.
- Full-duplex mode is used when communication in both direction is required all the time. The capacity of the channel, however must be divided between the two directions.
- Example: Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.



Goals of Computer Networks

The following are some important goals of computer networks:

1. **Resource Sharing –** Many organizations has 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, 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.

Types 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.
- There are some similarities and dissimilarities between them. 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.
- There are other types of Computer Networks also, like :
  - PAN (Personal Area Network)
  - SAN (Storage Area Network)
  - EPN (Enterprise Private Network)
  - VPN (Virtual Private Network)

1. **Local Area Network (LAN) –**
   - LAN or Local Area Network connects network devices in such a way that personal computer and workstations can share data, tools and programs.
   - The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol.
   - Routers are found at the boundary of a LAN, connecting them to the larger WAN.
   - Data transmits at a very fast rate as the number of computers linked are limited.
   - LANs cover smaller geographical area (Size is limited to a few kilometers) and are privately owned.
   - One can use it for an office building, home, hospital, schools, etc.
   - LAN is easy to design and maintain. A Communication medium used for LAN has twisted pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.
   - Early LAN's had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps.
   - The fault tolerance of a LAN is more and there is less congestion in this network.

2. **Metropolitan Area Network (MAN) –**
   - MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN.
   - It connects two or more computers that are apart but resides in the same or different cities.
   - It covers a large geographical area and may serve as an ISP (Internet Service Provider).

- MAN is designed for customers who need a high-speed connectivity. Speeds of MAN ranges in terms of Mbps.
- It's hard to design and maintain a Metropolitan Area Network.
- The fault tolerance of a MAN is less and also there is more congestion in the network.
- It is costly and may or may not be owned by a single organization.
- Devices used for transmission of data through MAN are: Modem and Wire/Cable.
- Examples of a MAN are the part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

3. **Wide Area Network (WAN) –**
    - WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country.
    - A WAN could be a connection of LAN connecting to other LAN's via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public.
    - The technology is high speed and relatively expensive.
    - There are two types of WAN: **Switched WAN** and **Point-to-Point WAN**.
    - WAN is difficult to design and maintain.
    - Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network.
    - A Communication medium used for WAN is PSTN or Satellite Link.
    - Due to long distance transmission, the noise and error tend to be more in WAN.
    - WAN's data rate is slow about a 10th LAN's speed, since it involves increased distance and increased number of servers and terminals etc. Speeds of WAN ranges from few kilobits per second (Kbps) to megabits per second (Mbps).
    - Devices used for transmission of data through WAN are: Optic wires, Microwaves and Satellites.
    - Example of a Switched WAN is the asynchronous transfer mode (ATM) network and Point-to-Point WAN is dial-up line that connects a home computer to the Internet.

Conclusion –

There are many advantages of LAN over MAN and WAN, such as LAN's provide excellent reliability, high data transmission rate, they can easily be managed, and shares peripheral devices too. Local Area Network cannot cover cities or towns and for that Metropolitan Area Network is needed, which can connect city or a group of cities together. Further, for connecting Country or a group of Countries one requires Wide Area Network.

Differences between LAN, WAN and MAN

LAN	MAN	WAN
LAN stands for Local Area Network.	MAN stands for Metropolitan Area Network.	WAN stands for Wide area network.
LAN's ownership is private.	MAN's ownership can be private or public.	While WAN also might not be owned by one organization.
The transmission speed of LAN is high.	While the transmission speed of MAN is average.	Whereas the transmission speed of WAN is low.
The propagation delay is short in LAN.	There is moderate propagation delay in MAN.	Whereas there is long propagation delay.
There is less congestion in LAN.	While there is more congestion in MAN.	Whereas there is more congestion than MAN in WAN.
LAN's design and maintenance is easy.	While MAN's design and maintenance is difficult than LAN.	Whereas WAN's design and maintenance is also difficult than LAN as well MAN.
There is more fault tolerance in LAN.	While there is less fault tolerance.	In WAN, there is also less fault tolerance.

Wireless and Wired Network

- **Wired Network**

As we know "wired" is the term refers to any physical medium consisting of cables. The cables can be copper wire, twisted pair or fiber optic. Wired network is used to carry different forms of electrical signals from one end to the other. Mostly in wired network one internet connection is being taken using T1 line, cable modem or using any other means. This connection is shared among multiple devices using wired network concept.

Examples of wired network: LAN (Local Area Network): This network consists of ethernet cards housed in PCs or laptops. These cards are connected using ethernet cables. The data flows between these cards. For small wired network router is used to connect few number of desktop or laptop computers. In order to increase the network coverage for more number of systems multiple switches and routers are used.

- **Wireless Network**

As we know "Wireless" is the term refers to medium made of electromagnetic waves (i.e. EM Waves) or infrared waves. All the wireless devices will have antenna or sensors. Typical wireless devices include cellular mobile, wireless sensors, TV remote, satellite disc receiver, laptops with WLAN card etc. Wireless network does not use wires for data or voice communication; it uses radio frequency waves as mentioned above. The other examples are fiber optic communication link and broadband ADSL etc.

Examples of wireless network:
1. Outdoor cellular technologies such as GSM, CDMA, WiMAX, LTE, Satellite etc.
2. Indoor wireless technologies such as Wireless LAN(or WiFi), Bluetooth, IrDA, Zigbee, Zwave etc.

Difference between Wired and Wireless Network

Specifications	Wired network	Wireless network
Speed of operation	Higher	lower compare to wired networks, But advanced wireless technologies such as LTE, LTE-A and WLAN-11ad will make it possible to achieve speed par equivalent to wired network
System Bandwidth	High	Low, as Frequency Spectrum is very scarse resource
Cost	Less as cables are not expensive	More as wireless subscriber stations, wireless routers, wireless access points and adapters are expensive
Installation	Wired network installation is cumbersome and it requires more time	Wireless network installation is easy and it requires less time
Mobility	Limited, as it operates in the area covered by connected systems with the wired network	Not limited, as it operates in the entire wireless network coverage
Transmission medium	copper wires, optical fiber cables, ethernet	EM waves or radiowaves or infrared

Types of Network transmission
Between the network hardware (LAN, MAN and WAN), network transmission exists.
There are of 2 types:

1. **Broadcast Network Link –**
   - The communication channel is shared by all the machines on the network.
   - Packets sent by any machine are received by all the others.
   - A special code (those registered with the channel, will gain the information) in address field will be added.
   - In multicasting, 1 bit indicates the multicast and the rest n-1 bit can hold the group no. Each machine can subscribe to any group.
2. **Point to Point Network Link –**
   - Point-to-point links connect individual pairs of machines (involves 2 nodes).
   - To go from the source to the destination on a network made up of point-to-point links, short mess- sages, called packets in certain contexts, may have to first visit one or more inter- mediate machines.
   - Often multiple routes, of different lengths, are possible, so finding good ones is important in point-to-point networks.
   - Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called unicasting.

Types of Network Topology
The arrangement of a network which comprises of nodes and connecting lines via sender and receiver is referred as network topology. The various network topologies are :

a) Mesh Topology:
In mesh topology, every device is connected to another device via particular channel.

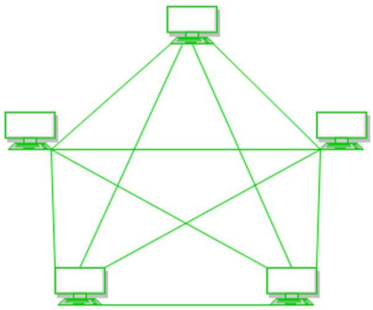


Figure 1: Every device is connected with another via dedicated channels. These channels are known as links.

Advantages of this topology :

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

Problems with this topology :

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

b) 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 others nodes are connected to the central node. The hub can be passive in nature i.e. not intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as active hubs. Active hubs have repeaters in them.

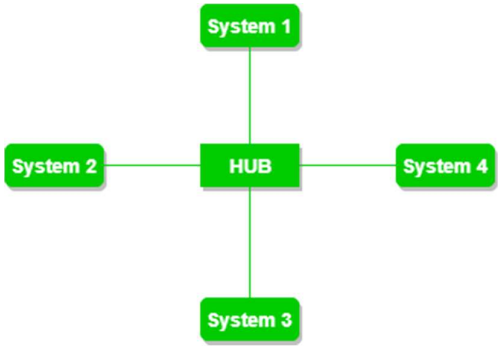


Figure 2: A star topology having four systems connected to single point of connection i.e. hub.

Advantages of this topology :

- If N devices are connected to each other in star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device require only 1 port i.e. to connect to the hub.

Problems with this topology :

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

c) Bus Topology:

Bus topology is a network type in which every computer and network device is connected to single cable. It transmits the data from one end to another in single direction. No bi-directional feature is in bus topology.

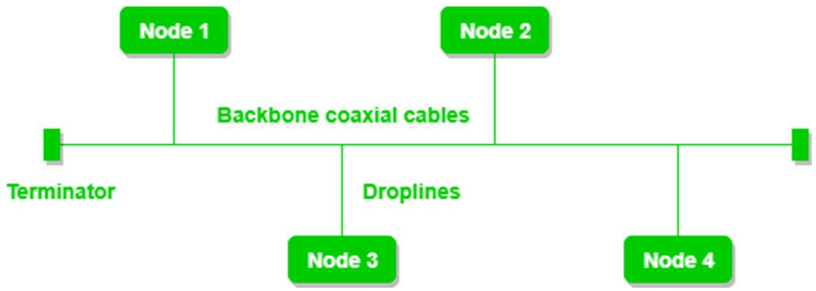


Figure 3: A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

Advantages of this topology :

- If N devices are connected to each other in bus topology, then the number of cables required to connect them is 1 which is known as backbone cable and N drop lines are required.
- Cost of the cable is less as compared to other topology, but it is used to built small networks.

Problems with this topology :

- 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 MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD etc.

d) Ring Topology:

In this topology, it forms a ring connecting a devices with its exactly two neighbouring devices.

The following operations takes place in ring topology are :

1. One station is known as monitor station which takes all the responsibility to perform the operations.

2. To transmit the data, station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
3. When no station is transmitting the data, then the token will circulate in the ring.
4. There are two types of token release techniques : Early token release releases the token just after the transmitting the data and Delay token release releases the token after the acknowledgement is received from the receiver.

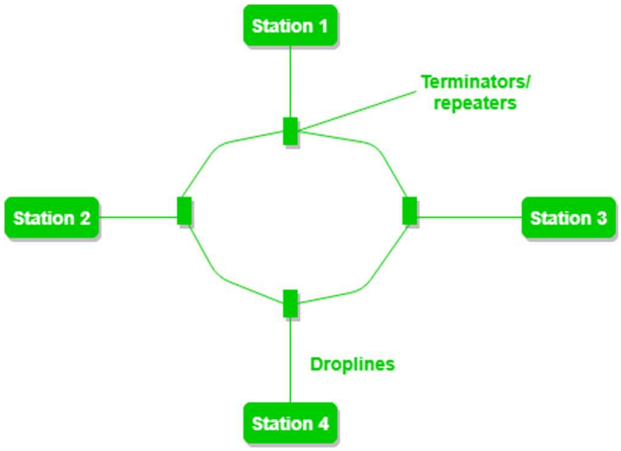


Figure 4: A ring topology comprises of 4 stations connected with each forming a ring..

Advantages of this topology :

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

Problems with this topology :

- Troubleshooting is difficult in this topology.
- Addition of stations in between or removal of stations can disturb the whole topology.

e) Hybrid Topology:

This topology is a collection of two or more topologies which are described above. This is a scalable topology which can be expanded easily. It is reliable one but at the same it is a costly topology.

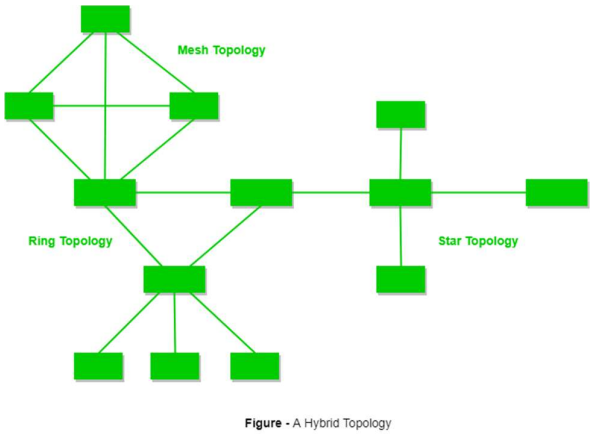


Figure - A Hybrid Topology

Figure 5: A hybrid topology which is a combination of ring and star topology.

Network Protocols

Network Protocols are a set of rules governing exchange of information in an easy, reliable and secure way.

There are various types of protocols that support a major and compassionate role in communicating with different devices across the network. These are:

1. Transmission Control Protocol (TCP)
2. Internet Protocol (IP)
3. User Datagram Protocol (UDP)
4. Post office Protocol (POP)
5. Simple mail transport Protocol (SMTP)
6. File Transfer Protocol (FTP)
7. Hyper Text Transfer Protocol (HTTP)
8. Hyper Text Transfer Protocol Secure (HTTPS)
9. Telnet
10. Gopher

- **Transmission Control Protocol (TCP):** TCP is a popular communication protocol which is used for communicating over a network. It divides any message into series of packets that are sent from source to destination and there it gets reassembled at the destination.
- **Internet Protocol (IP):** IP is designed explicitly as addressing protocol. It is mostly used with TCP. The IP addresses in packets help in routing them through different nodes in a network until it reaches the destination system. TCP/IP is the most popular protocol connecting the networks.
- **User Datagram Protocol (UDP):** UDP is a substitute communication protocol to Transmission Control Protocol implemented primarily for creating loss-tolerating and low-latency linking between different applications.
- **Post office Protocol (POP):** POP3 is designed for receiving incoming E-mails.
- **Simple mail transport Protocol (SMTP):** SMTP is designed to send and distribute outgoing E-Mail.
- **File Transfer Protocol (FTP):** FTP allows users to transfer files from one machine to another. Types of files may include program files, multimedia files, text files, and documents, etc.
- **Hyper Text Transfer Protocol (HTTP):** HTTP is designed for transferring a hypertext among two or more systems. HTML tags are used for creating links. These links may be in any form like text or images. HTTP is designed on Client-server principles which allow a client system for establishing a connection with the server machine for making a request. The server acknowledges the request initiated by the client and responds accordingly.
- **Hyper Text Transfer Protocol Secure (HTTPS):** HTTPS is abbreviated as Hyper Text Transfer Protocol Secure is a standard protocol to secure the communication among two computers one using the browser and other fetching data from web server. HTTP is used for transferring data between the client browser (request) and the web server (response) in the hypertext format, same in case of HTTPS except that the

transferring of data is done in an encrypted format. So it can be said that https thwart hackers from interpretation or modification of data throughout the transfer of packets.

- **Telnet:** Telnet is a set of rules designed for connecting one system with another. The connecting process here is termed as remote login. The system which requests for connection is the local computer, and the system which accepts the connection is the remote computer.
- **Gopher:** Gopher is a collection of rules implemented for searching, retrieving as well as displaying documents from isolated sites. Gopher also works on the client/server principle.

Network Interface

- In computing, a network interface is a software or hardware interface between two pieces of equipment or protocol layers in a computer network.
- A network interface will usually have some form of network address. This may consist of a node identifier and a port number or may be a unique node ID in its own right.
- Network interfaces provide standardized functions such as passing messages, connecting and disconnecting, etc.

Examples

- Computer port (hardware), an interface to other computers or peripherals
- Network interface controller, the device a computer uses to connect to a computer network
- Network interface device, a demarcation point for a telephone network
- Network socket, a software interface to the network
- Port (computer networking), a protocol interface to the network

Network Services

- In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.
- Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client components running on other devices. However, the client and server components can both be run on the same machine.
- Clients and servers will often have a user interface, and sometimes other hardware associated with it.
- Examples are the Domain Name System (DNS) which translates domain names to Internet protocol (IP) addresses and the Dynamic Host Configuration Protocol (DHCP) to assign networking configuration information to network hosts.

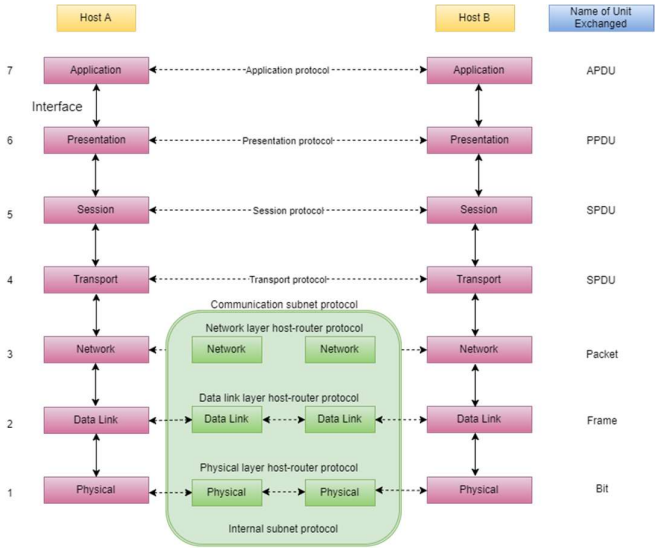
ISO-OSI reference model

There are n numbers of users who use computer network and are located over the world. So to ensure, national and worldwide data communication, systems must be developed which are compatible to communicate with each other ISO has developed a standard. ISO stands for

International organization of Standardization. This is called a model for Open System Interconnection (OSI) and is commonly known as OSI model.
The ISO-OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system. They are:

1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Datalink Layer
7. Physical Layer

Below we have the complete representation of the OSI model, showcasing all the layers and how they communicate with each other.



In the table below, we have specified the protocols used and the data unit exchanged by each layer of the OSI Model.

Layer	Name of Protocol	Name of Unit exchanged
Application	Application Protocol	APDU - Application Protocol Data Unit
Presentation	Presentation Protocol	PPDU - Presentation Protocol Data Unit
Session	Session Protocol	SPDU - Session Protocol Data Unit
Transport	Transport Protocol	TPDU - Transport Protocol Data Unit
Network	Network layer host-router Protocol	Packet
Data Link	Data link layer host-router Protocol	Frame
Physical	Physical layer host-router Protocol	Bit

Feature of OSI Model

- Big picture of communication over network is understandable through this OSI model.
- We see how hardware and software work together.
- We can understand new technologies as they are developed.

- Troubleshooting is easier by separate networks.
- Can be used to compare basic functional relationships on different networks.

Principles of OSI Reference Model

The OSI reference model has 7 layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

- A layer should be created where a different abstraction is needed.
- Each layer should perform a well-defined function.
- The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
- The layer boundaries should be chosen to minimize the information flow across the interfaces.
- The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that architecture does not become unwieldly.

Functions of Different Layers

Following are the functions performed by each layer of the OSI model. This is just an introduction, we will cover each layer in details in the coming tutorials.

The Physical Layer

- Physical Layer is the lowest layer of the OSI Model.
- It activates, maintains and deactivates the physical connection.
- It is responsible for transmission and reception of the unstructured raw data over network.
- Voltages and data rates needed for transmission is defined in the physical layer.
- It converts the digital/analog bits into electrical signal or optical signals.
- Data encoding is also done in this layer.

Data Link Layer

- Data link layer synchronizes the information which is to be transmitted over the physical layer.
- The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
- Transmitting and receiving data frames sequentially is managed by this layer.
- This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
- This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

The Network Layer

- Network Layer routes the signal through different channels from one node to other.

- It acts as a network controller. It manages the Subnet traffic.
- It decides by which route data should take.
- It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

Transport Layer

- Transport Layer decides if data transmission should be on parallel path or single path.
- Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
- It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.
- Transport layer can be very complex, depending upon the network requirements.

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

The Session Layer

- Session Layer manages and synchronize the conversation between two different applications.
- Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

The Presentation Layer

- Presentation Layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
- While receiving the data, presentation layer transforms the data to be ready for the application layer.
- Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
- It perfroms Data compression, Data encryption, Data conversion etc.

Application Layer

- Application Layer is the topmost layer.
- Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.
- This layer mainly holds application programs to act upon the received and to be sent data.

Merits of OSI reference model

- OSI model distinguishes well between the services, interfaces and protocols.
- Protocols of OSI model are very well hidden.
- Protocols can be replaced by new protocols as technology changes.

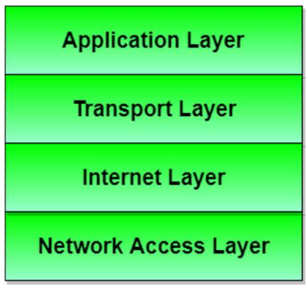
- Supports connection oriented services as well as connectionless service.

Demerits of OSI reference model

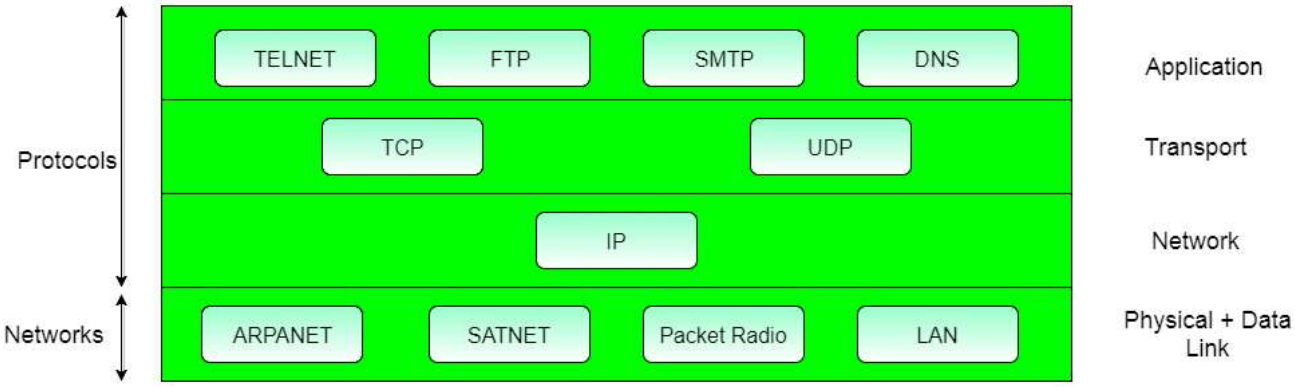
- Model was devised before the invention of protocols.
- Fitting of protocols is tedious task.
- It is just used as a reference model.

TCP/IP architecture

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. They also offer simple naming and addressing schemes.



Protocols and networks in the TCP/IP model:



Overview of TCP/IP reference model

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defence's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact untill the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

Below we have discussed the 4 layers that form the TCP/IP reference model:

Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
   - Delivering IP packets
   - Performing routing
   - Avoiding congestion

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. **FTP(File Transfer Protocol)** is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. **SMTP(Simple Mail Transport Protocol)** is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. **DNS(Domain Name Server)** resolves an IP address into a textual address for Hosts connected over a network.
5. It allows peer entities to carry conversation.
6. It defines two end-to-end protocols: TCP and UDP

- **TCP(Transmission Control Protocol):** It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.
- **UDP(User-Datagram Protocol):** It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service.

Merits of TCP/IP model

- It operated independently.
- It is scalable.
- Client/server architecture.
- Supports a number of routing protocols.
- Can be used to establish a connection between two computers.

Demerits of TCP/IP

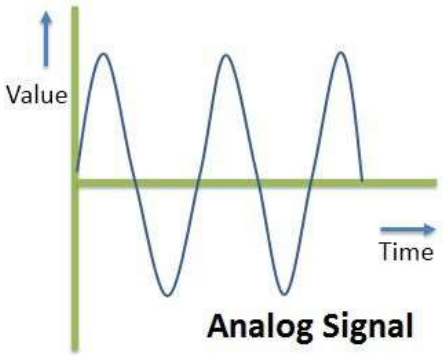
- In this, the transport layer does not guarantee delivery of packets.
- The model cannot be used in any other application.
- Replacing protocol is not easy.
- It has not clearly separated its services, interfaces and protocols.

PHYSICAL LAYER

Analog Signal and Digital Signal

Analog signal –

- It is a kind of continuous wave form that changes over time.
- An anlaog signal is further classified into simple and composite signals.
- A simple analog signal is a sine wave that cannot be decomposed further. On the other hand, a composite analog signal can be further decomposed into multiple sine waves.
- An analog signal is described using amplitude, period or frequency and phase.
- Amplitude marks the maximum height of the signal. Frequency marks the rate at which signal is changing. Phase marks the position of the wave with respect to time zero.

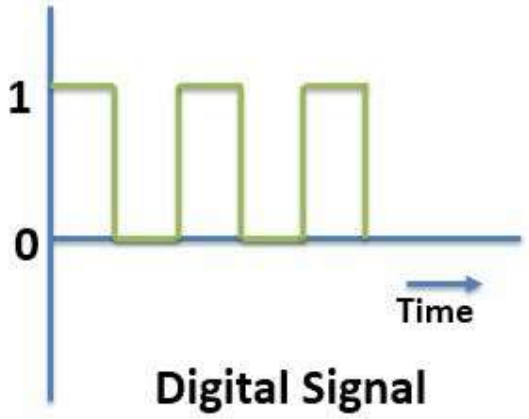


- An analog signal is not immune to noise hence, it faces distortion and decrease the quality of transmission. The range of value in an analog signal is not fixed.

Digital Signal -

- Digital signals also carry information like analog signals but is somewhat is different from analog signals.

- Digital signal is non-continuous, discrete time signal.
- Digital signal carries information or data in the binary form i.e. a digital signal represent information in the form of bits.
- Digital signal can be further decomposed into simple sine waves that are called harmonics.
- Each simple wave has different amplitude, frequency and phase.
- Digital signal is described with bit rate and bit interval.
- Bit interval describes the time require for sending a single bit. On the other hand, bit rate describes the frequency of bit interval.



- A digital signal is more immune to the noise; hence, it hardly faces any distortion.
- Digital signals are easier to transmit and are more reliable when compared to analog signals. Digital signal has a finite range of values. The digital signal consists 0s and 1s.

Basis for Comparison	Analog Signal	Digital Signal
Basic	An analog signal is a continuous wave that changes over a time period.	A digital signal is a discrete wave that carries information in binary form.
Representation	An analog signal is represented by a sine wave.	A digital signal is represented by square waves.
Description	An analog signal is described by the amplitude, period or frequency, and phase.	A digital signal is described by bit rate and bit intervals.
Range	Analog signal has no fixed range.	Digital signal has a finite numbers i.e. 0 and 1.
Distortion	An analog signal is more prone to distortion.	A digital signal is less prone to distortion.
Transmit	An analog signal transmit data in the form of a wave.	A digital signal carries data in the binary form i.e. 0 nad 1.
Example	The human voice is the best example of an analog signal.	Signals used for transmission in a computer are the digital signal.

Bandwidth

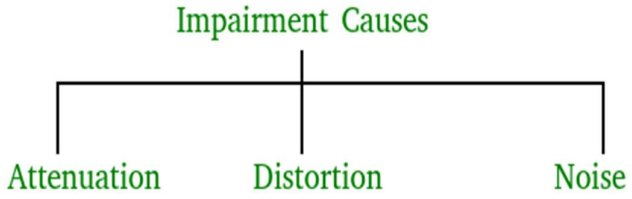
- Bandwidth is the difference between the upper and lower frequencies in a continuous band of frequencies.
- It is typically measured in hertz, and depending on context, may specifically refer to passband bandwidth or baseband bandwidth.

- Passband bandwidth is the difference between the upper and lower cutoff frequencies of, for example, a band-pass filter, a communication channel, or a signal spectrum.
- Baseband bandwidth applies to a low-pass filter or baseband signal; the bandwidth is equal to its upper cutoff frequency.
- A key characteristic of bandwidth is that any band of a given width can carry the same amount of information, regardless of where that band is located in the frequency spectrum. For example, a 3 kHz band can carry a telephone conversation whether that band is at baseband (as in a POTS telephone line) or modulated to some higher frequency.

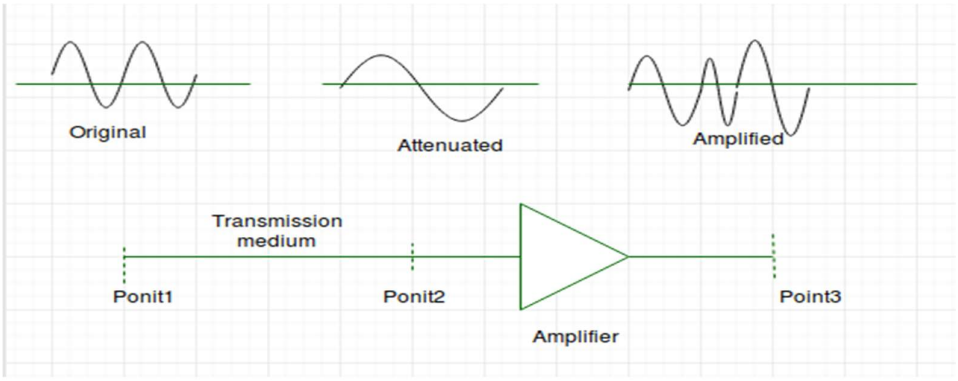
Transmission Impairment

In communication system, analog signals travel through transmission media, which tends to deteriorate the quality of analog signal. This imperfection causes signal impairment. This means that received signal is not same as the signal that was send.

Causes of impairment –



- **Attenuation –** It means loss of energy. The strength of signal decreases with increasing distance which causes loss of energy in overcoming resistance of medium. This is also known as attenuated signal. Amplifiers are used to amplify the attenuated signal which gives the original signal back.



Attenuation is measured in decibels(dB). It measures the relative strengths of two signals or one signal at two different point.

$$\text{Attenuation(dB)} = 10\log10(P2/P1)$$

P1 is power at sending end and P2 is power at receiving end.

- **Distortion –** It means change in the shape of signal. This is generally seen in composite signals with different frequencies. Each frequency component has its own propagation speed travelling through a medium. Every component arrives at different time which

leads to delay distortion. Therefore, they have different phases at receiver end from what they had at sender's end.

- **Noise –** The random or unwanted signal that mixes up with the original signal is called noise. There are several types of noise such as induced noise, crosstalk noise, thermal noise and impulse noise which may corrupt the signal.

  Induced noise comes from sources such as motors and appliances. These devices act as sending antenna and transmission medium act as receiving antenna. Thermal noise is movement of electrons in wire which creates an extra signal. Crosstalk noise is when one wire affects the other wire. Impulse noise is a signal with high energy that comes from lightning or power lines

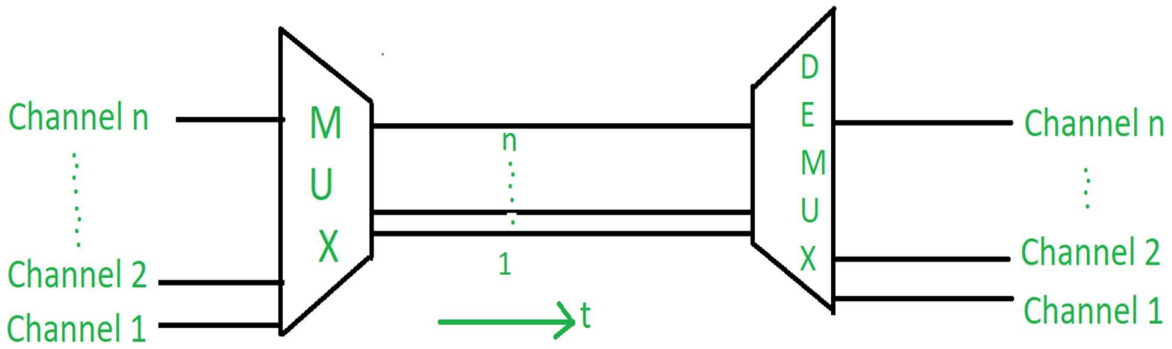
SNR = AVG SIGNAL POWER / AVG NOISE POWER

Multiplexing

Multiplexing is used in the cases where the signals of lower bandwidth and the transmitting media is having higher bandwidth. In this case, the possibility of sending a number of signals is more. In this the signals are combined into one and are sent over a link which has greater bandwidth of media than the communicating nodes.

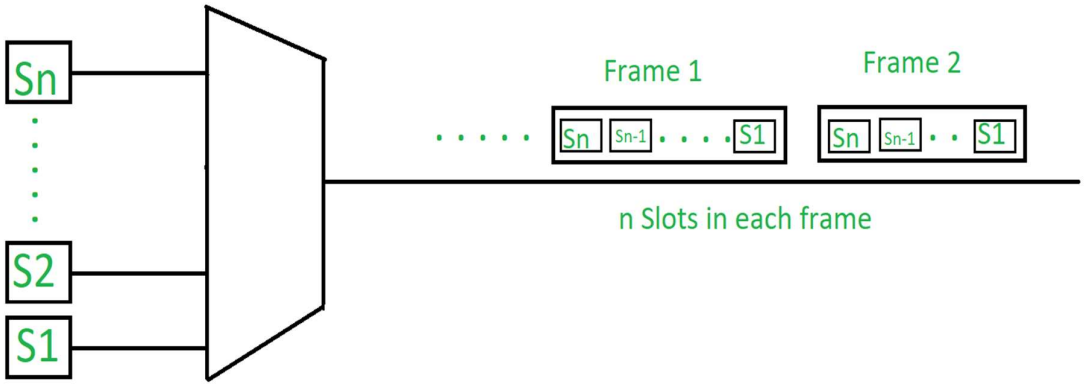
1. Frequency Division Multiplexing (FDM) –

In this a number of signals are transmitted at the same time, and each source transfers its signals in the allotted frequency range. There is a suitable frequency gap between the 2 adjacent signals to avoid over-lapping. Since the signals are transmitted in allotted time so this decreases the probability of collision. The frequency spectrum is divided into several logical channels, in which every user feels that they posses a particular bandwidth. A number of signals are sent simultaneously on the same time allocating separate frequency band or channel to each signal. It is used in radio and TV transmission. Therefore to avoid interference between two successive channels Guard bands are used.



2. Time Division Multiplexing (TDM) –

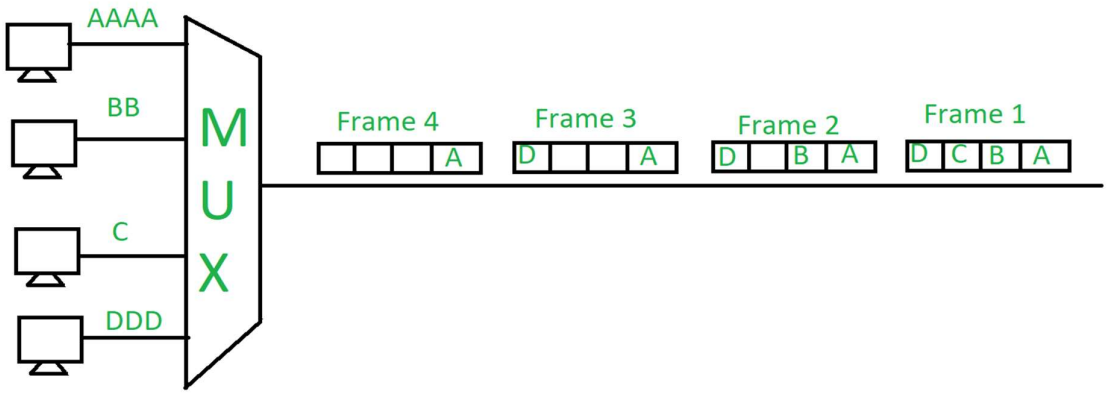
This happens when data transmission rate of media is greater than that of the source, and each signal is allotted a definite amount of time. These slots are so small that all transmissions appear to be parallel. In frequency division multiplexing all the signals operate at the same time with different frequencies, but in time division multiplexing all the signals operate with same frequency at different times.



It is of following types:

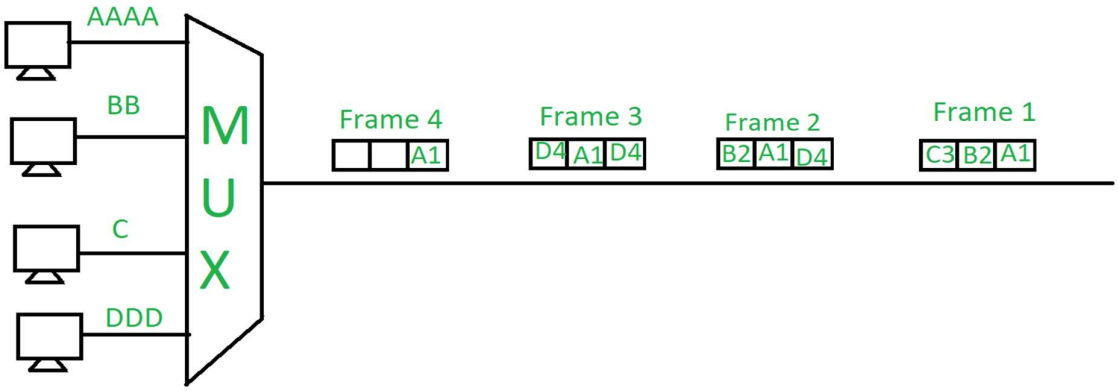
- **Synchronous TDM –**

The time slots are pre-assigned and fixed. This slot is even given if the source is not ready with data at this time. In this case the slot is transmitted empty. It is used for multiplexing digitized voice stream.



- **Asynchronous (or statistical) TDM –**

The slots are allocated dynamically depending on the speed of source or their ready state. It dynamically allocates the time slots according to different input channel's needs, thus saving the channel capacity.



3. Wavelength Division Multiplexing

Wavelength division multiplexing (WDM) is a technique of multiplexing multiple optical carrier signals through a single optical fiber channel by varying the wavelengths of laser lights. WDM allows communication in both the directions in the fiber cable.

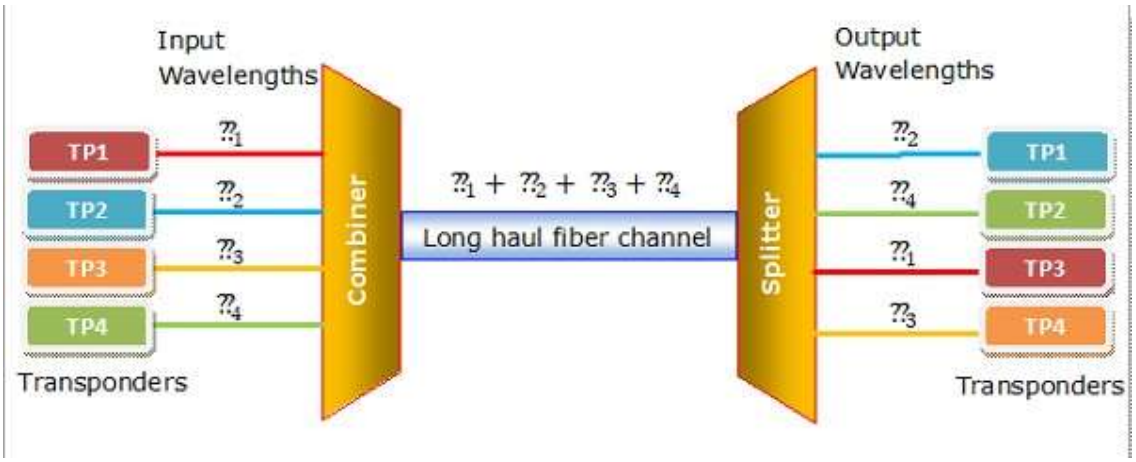
Concept and Process

In WDM, the optical signals from different sources or (transponders) are combined by a multiplexer, which is essentially an optical combiner. They are combined so that their wavelengths are different.

The combined signal is transmitted via a single optical fiber strand. At the receiving end, a demultiplexer splits the incoming beam into its components and each of the beams is send to the corresponding receivers.

Example

The following diagram conceptually represents multiplexing using WDM. It has 4 optical signals having 4 different wavelengths. Each of the four senders generates data streams of a particular wavelength. The optical combiner multiplexes the signals and transmits them over a single long-haul fiber channel. At the receiving end, the splitter demultiplexes the signal into the original 4 data streams.



Categories of WDM

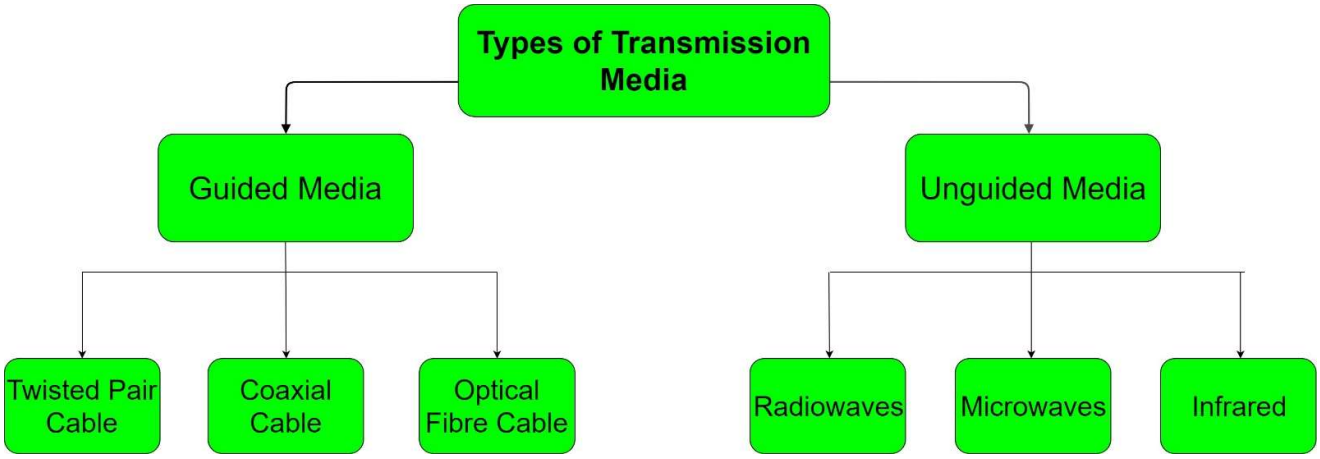
Based upon the wavelength, WDM can be divided into two categories −

Course WDM (CWDM): CWDM generally operates with 8 channels where the spacing between the channels is 20 nm (nanometers) apart. It consumes less energy than DWDM and is less expensive. However, the capacity of the links, as well as the distance supported, is lesser.

Dense WDM (DWDM): In DWDM, the number of multiplexed channels much larger than CWDM. It is either 40 at 100GHz spacing or 80 with 50GHz spacing. Due to this, they can transmit the huge quantity of data through a single fiber link. DWDM is generally applied in core networks of telecommunications and cable networks. It is also used in cloud data centers for their IaaS services.

Transmission Media

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:



1. Guided Media:

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

(i) Twisted Pair Cable –

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

(a) Unshielded Twisted Pair (UTP):

This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

Advantages:

- Least expensive
- Easy to install
- High speed capacity

Disadvantages:

- Susceptible to external interference
- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation

(b) Shielded Twisted Pair (STP):

This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

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 –

It has an outer plastic covering containing 2 parallel conductors each having a separate insulated protection cover. Coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

Advantages:

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

Disadvantages:

- Single cable failure can disrupt the entire network

(iii) Optical Fibre Cable –

It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for transmission of large volumes of data.

Advantages:

- Increased capacity and bandwidth
- Light weight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile

- unidirectional, ie, will need another fibre, if we need bidirectional communication

2. Unguided Media:
It is also referred to as Wireless or Unbounded transmission media.No physical medium is required for the transmission of electromagnetic signals.

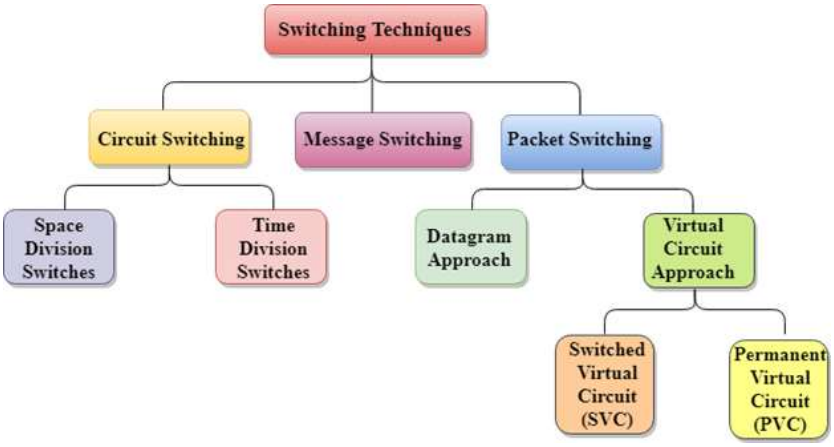
Features:
- Signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 major types of Unguided Media:
(i) Radiowaves –
These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radiowaves for transmission.
Further Categorized as (i) Terrestrial and (ii) Satellite.

(ii) Microwaves –
It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

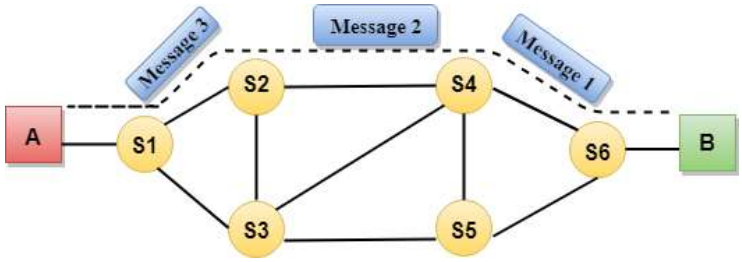
(iii) Infrared –
Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

Switching Techniques



Circuit Switching
- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.

- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.



Advantages:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

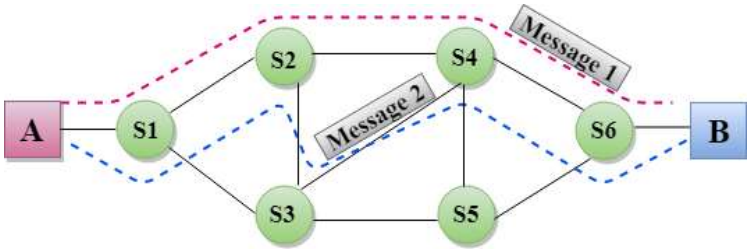
Disadvantages:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.

- Each and every node stores the entire message and then forward it to the next node. This type of network is known as store and forward network.
- Message switching treats each message as an independent entity.



Advantages:

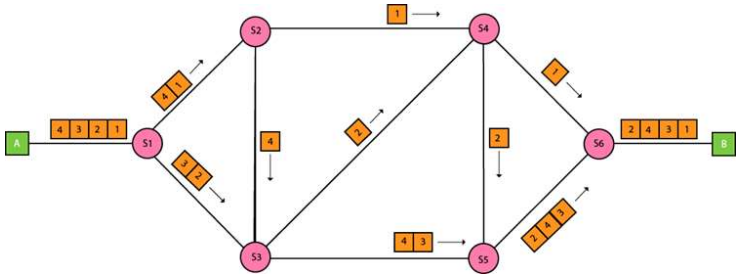
- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages:

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



Advantages:

- Cost-effective: In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- Reliable: If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- Efficient: Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages:

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

Comparison of circuit Switching, Packet switching & Message Switching

Parameter	Message switching	Circuit switching	Packet switching
Application	Telegraph network for transmission of telegrams	Telephone network for bi-directional, real time transfer of voice signals	Internet for datagram and reliable stream service between computers
End terminal	Telegraph, teletype	Telephone, modem	Computer
Information type	Morse, Baudot, ASCII	Analog voice or PCM digital voice	Binary information
Transmission system	Digital data over different transmission media	Analog and digital data over different transmission media	Digital data over different transmission media

ISDN

The Integrated Services of Digital Networking, in short ISDN is a telephone network based infrastructure that allows the transmission of voice and data simultaneously at a high speed with greater efficiency. This is a circuit switched telephone network system, which also provides access to Packet switched networks. Several kinds of access interfaces are:

- Narrowband ISDN
- Broadband ISDN

Narrowband ISDN

- The Narrowband Integrated Services Digital Network is called the N-ISDN.
- This can be understood as a telecommunication that carries voice information in a narrow band of frequencies.
- This is actually an attempt to digitize the analog voice information. This uses 64kbps circuit switching.
- The narrowband ISDN is implemented to carry voice data, which uses lesser bandwidth, on a limited number of frequencies.

Broadband ISDN

- The Broadband Integrated Services Digital Network is called the B-ISDN.
- This integrates the digital networking services and provides digital transmission over ordinary telephone wires, as well as over other media.
- The broadband ISDN speed is around 2 MBPS to 1 GBPS and the transmission is related to ATM, i.e., Asynchronous Transfer Mode.
- The broadband ISDN communication is usually made using the fiber optic cables.
- As the speed is greater than 1.544 Mbps, the communications based on this are called Broadband Communications.

ATM (Asynchronous Transfer Mode)

- ATM stands for Asynchronous Transfer Mode. It is a switching technique that uses time division multiplexing (TDM) for data communications.
- ATM networks are connection oriented networks for cell relay that supports voice, video and data communications.
- It encodes data into small fixed - size cells so that they are suitable for TDM and transmits them over a physical medium.
- The size of an ATM cell is 53 bytes: 5 byte header and 48 byte payload.
- There are two different cell formats - user-network interface (UNI) and network-network interface (NNI). The below image represents the Functional Reference Model of the Asynchronous Transfer Mode.

Benefits of ATM Networks are

- It provides the dynamic bandwidth that is particularly suited for bursty traffic.
- Since all data are encoded into identical cells, data transmission is simple, uniform and predictable.
- Uniform packet size ensures that mixed traffic is handled efficiently.
- Small sized header reduces packet overload, thus ensuring effective bandwidth usage.
- ATM networks are scalable both in size and speed.

ATM reference model comprises of three layers

1. **Physical Layer:** This layer corresponds to physical layer of OSI model. At this layer, the cells are converted into bit streams and transmitted over the physical medium. This layer has two sub layers: PMD sub layer (Physical Medium Dependent) and TC (Transmission Convergence) sub layer.

2. **ATM Layer:** This layer is comparable to data link layer of OSI model. It accepts the 48 byte segments from the upper layer, adds a 5 byte header to each segment and converts into 53 byte cells. This layer is responsible for routing of each cell, traffic management, multiplexing and switching.
3. **ATM Adaptation Layer (AAL):** This layer corresponds to network layer of OSI model. It provides facilities to the existing packet switched networks to connect to ATM network and use its services. It accepts the data and converts them into fixed sized segments. The transmissions can be of fixed or variable data rate. This layer has two sub layers: Convergence sub layer and Segmentation and Reassembly sub layer.
4. **ATM endpoints:** It contains ATM network interface adaptor. Examples of endpoints are workstations, routers, CODECs, LAN switches, etc.
5. **ATM switch:** It transmits cells through the ATM networks. It accepts the incoming cells from ATM endpoints (UNI) or another switch (NNI), updates cell header and retransmits cell towards destination.

UNIT 2
DATA LINK LAYER

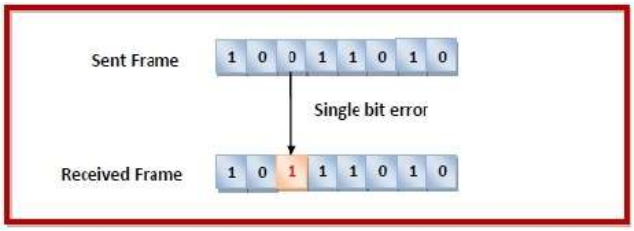
Errors

- When bits are transmitted over the computer network, they are subject to get corrupted due to interference and network problems. The corrupted bits leads to spurious data being received by the destination and are called errors.
- Error control in data link layer is the process of detecting and correcting data frames that have been corrupted or lost during transmission.
- In case of lost or corrupted frames, the receiver does not receive the correct data-frame and sender is ignorant about the loss.
- Data link layer follows a technique to detect transit errors and take necessary actions, which is retransmission of frames whenever error is detected or frame is lost. The process is called Automatic Repeat Request (ARQ).

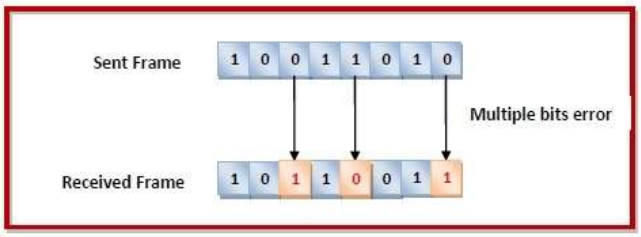
Types of Errors

Errors can be of three types, namely single bit errors, multiple bit errors, and burst errors.

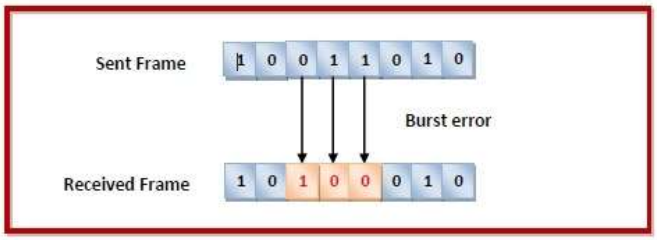
- **Single bit error** − In the received frame, only one bit has been corrupted, i.e. either changed from 0 to 1 or from 1 to 0.



- **Multiple bits error** − In the received frame, more than one bits are corrupted.



- **Burst error** − In the received frame, more than one consecutive bits are corrupted.



Error control can be done in two ways

- **Error detection** − Error detection involves checking whether any error has occurred or not. The number of error bits and the type of error does not matter.
- **Error correction** − Error correction involves ascertaining the exact number of bits that has been corrupted and the location of the corrupted bits.

For both error detection and error correction, the sender needs to send some additional bits along with the data bits. The receiver performs necessary checks based upon the additional redundant bits. If it finds that the data is free from errors, it removes the redundant bits before passing the message to the upper layers.

Bit Stuffing and Byte Stuffing

- **Byte stuffing** is a mechanism to convert a message formed of a sequence of bytes that may contain reserved values such as frame delimiter, into another byte sequence that does not contain the reserved values.
- **Bit stuffing** is the mechanism of inserting one or more non-information bits into a message to be transmitted, to break up the message sequence, for synchronization purpose.

Purposes of byte stuffing and bit stuffing

- In Data Link layer, the stream of bits from physical layer are divided into data frames.
- The data frames can be of fixed length or variable length.
- In variable - length framing, the size of each frame to be transmitted may be different. So, a pattern of bits is used as a delimiter to mark the end of one frame and the beginning of the next frame.
- However, if the pattern occurs in the message, then mechanisms needs to be incorporated so that this situation is avoided.

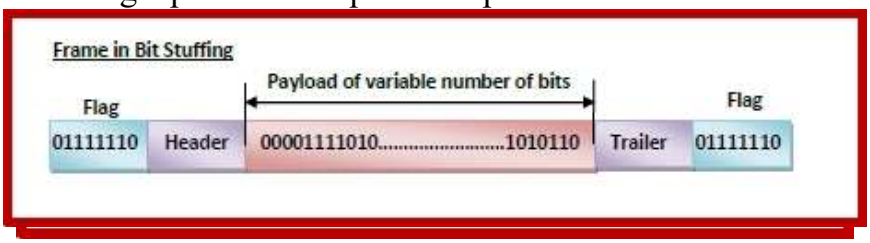
The two common approaches are −

Byte - Stuffing − A byte is stuffed in the message to differentiate from the delimiter. This is also called character-oriented framing.

Bit - Stuffing − A pattern of bits of arbitrary length is stuffed in the message to differentiate from the delimiter. This is also called bit - oriented framing.

Data link layer frames in byte stuffing and bit stuffing
A data link frame has the following parts −

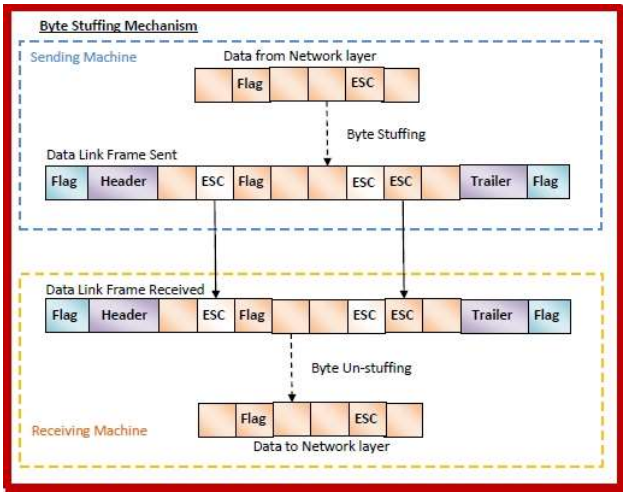
- **Frame Header** − It contains the source and the destination addresses of the frame.
- **Payload field** − It contains the message to be delivered. In bit stuffing it is a variable sequence of bits, while in byte stuffing it is a variable sequence of data bytes.
- **Trailer** − It contains the error detection and error correction bits.
- **Flags** − Flags are the frame delimiters signalling the start and end of the frame. In bit stuffing, flag comprises of a bit pattern that defines the beginning and end bits. It is generally of 8-bits and comprises of six or more consecutive 1s. In byte stuffing, flag is of 1- byte denoting a protocol - dependent special character.



Mechanisms of byte stuffing versus bit stuffing

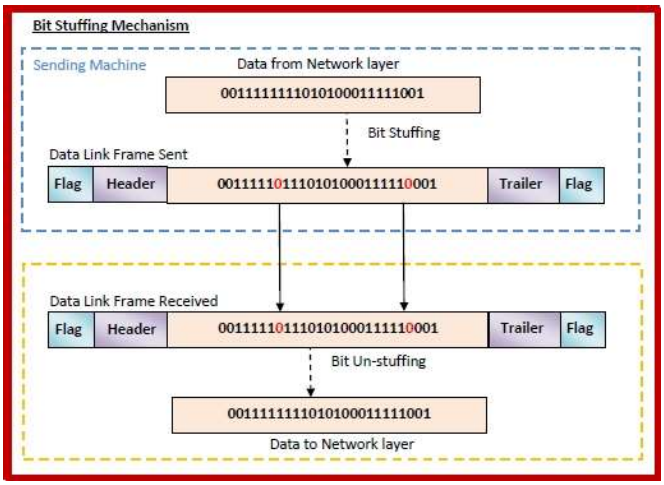
Byte Stuffing Mechanism

If the pattern of the flag byte is present in the message byte sequence, there should be a strategy so that the receiver does not consider the pattern as the end of the frame. Here, a special byte called the escape character (ESC) is stuffed before every byte in the message with the same pattern as the flag byte. If the ESC sequence is found in the message byte, then another ESC byte is stuffed before it.



Bit Stuffing Mechanism

Here, the delimiting flag sequence generally contains six or more consecutive 1s. Most protocols use the 8-bit pattern 01111110 as flag. In order to differentiate the message from the flag in case of same sequence, a single bit is stuffed in the message. Whenever a 0 bit is followed by five consecutive 1bits in the message, an extra 0 bit is stuffed at the end of the five 1s. When the receiver receives the message, it removes the stuffed 0s after each sequence of five 1s. The un-stuffed message is then sent to the upper layers.



Error Detection Techniques

There are three main techniques for detecting errors in frames: Parity Check, Checksum and Cyclic Redundancy Check (CRC).

Parity Check

- The parity check is done by adding an extra bit, called parity bit to the data to make a number of 1s either even in case of even parity or odd in case of odd parity.
- While creating a frame, the sender counts the number of 1s in it and adds the parity bit in the following way
  - In case of even parity: If a number of 1s is even then parity bit value is 0. If the number of 1s is odd then parity bit value is 1.
  - In case of odd parity: If a number of 1s is odd then parity bit value is 0. If a number of 1s is even then parity bit value is 1.
  - On receiving a frame, the receiver counts the number of 1s in it. In case of even parity check, if the count of 1s is even, the frame is accepted, otherwise, it is rejected. A similar rule is adopted for odd parity check.
  - The parity check is suitable for single bit error detection only.

Checksum

In this error detection scheme, the following procedure is applied

- Data is divided into fixed sized frames or segments.
- The sender adds the segments using 1's complement arithmetic to get the sum. It then complements the sum to get the checksum and sends it along with the data frames.
- The receiver adds the incoming segments along with the checksum using 1's complement arithmetic to get the sum and then complements it.

- If the result is zero, the received frames are accepted; otherwise, they are discarded.

Cyclic Redundancy Check (CRC)

Cyclic Redundancy Check (CRC) involves binary division of the data bits being sent by a predetermined divisor agreed upon by the communicating system. The divisor is generated using polynomials.

- Here, the sender performs binary division of the data segment by the divisor. It then appends the remainder called CRC bits to the end of the data segment. This makes the resulting data unit exactly divisible by the divisor.
- The receiver divides the incoming data unit by the divisor. If there is no remainder, the data unit is assumed to be correct and is accepted. Otherwise, it is understood that the data is corrupted and is therefore rejected.

Error Correction Techniques

Error correction techniques find out the exact number of bits that have been corrupted and as well as their locations. There are two principle ways

- **Backward Error Correction (Retransmission)** − If the receiver detects an error in the incoming frame, it requests the sender to retransmit the frame. It is a relatively simple technique. But it can be efficiently used only where retransmitting is not expensive as in fiber optics and the time for retransmission is low relative to the requirements of the application.
- **Forward Error Correction** − If the receiver detects some error in the incoming frame, it executes error-correcting code that generates the actual frame. This saves bandwidth

required for retransmission. It is inevitable in real-time systems. However, if there are too many errors, the frames need to be retransmitted.

The four main error correction codes are

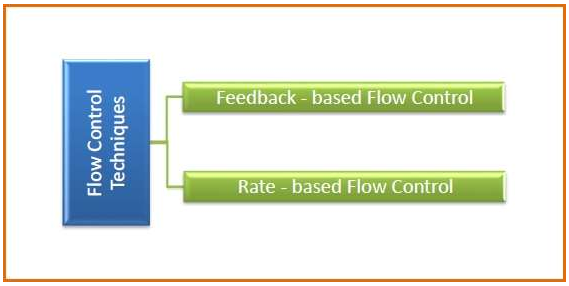
- Hamming Codes
- Binary Convolution Code
- Reed – Solomon Code
- Low-Density Parity-Check Code

Flow Control

Flow control is a technique that allows two stations working at different speeds to communicate with each other. It is a set of measures taken to regulate the amount of data that a sender sends so that a fast sender does not overwhelm a slow receiver. In data link layer, flow control restricts the number of frames the sender can send before it waits for an acknowledgment from the receiver.

Approaches of Flow Control

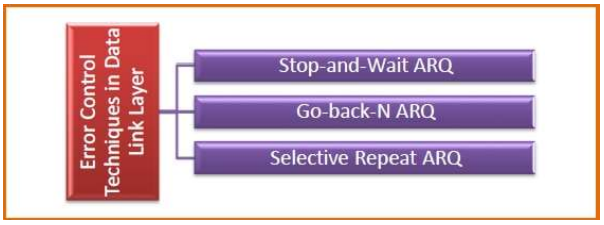
Flow control can be broadly classified into two categories −



- **Feedback based Flow Control -** In these protocols, the sender sends frames after it has received acknowledgments from the user. This is used in the data link layer.
- **Rate based Flow Control -** These protocols have built in mechanisms to restrict the rate of transmission of data without requiring acknowledgment from the receiver. This is used in the network layer and the transport layer.

Flow Control Techniques in Data Link Layer

Data link layer uses feedback based flow control mechanisms. There are two main techniques –



Stop and Wait ARQ

This protocol involves the following transitions:

- A timeout counter is maintained by the sender, which is started when a frame is sent.

- If the sender receives acknowledgment of the sent frame within time, the sender is confirmed about successful delivery of the frame. It then transmits the next frame in queue.
- If the sender does not receive the acknowledgment within time, the sender assumes that either the frame or its acknowledgment is lost in transit. It then retransmits the frame.
- If the sender receives a negative acknowledgment, the sender retransmits the frame.

Go-Back-N ARQ

The working principle of this protocol is:

- The sender has buffers called sending window.
- The sender sends multiple frames based upon the sending-window size, without receiving the acknowledgment of the previous ones.
- The receiver receives frames one by one. It keeps track of incoming frame's sequence number and sends the corresponding acknowledgment frames.
- After the sender has sent all the frames in window, it checks up to what sequence number it has received positive acknowledgment.
- If the sender has received positive acknowledgment for all the frames, it sends next set of frames.
- If sender receives NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

Selective Repeat ARQ

- Both the sender and the receiver have buffers called sending window and receiving window respectively.
- The sender sends multiple frames based upon the sending-window size, without receiving the acknowledgment of the previous ones.
- The receiver also receives multiple frames within the receiving window size.
- The receiver keeps track of incoming frame's sequence numbers, buffers the frames in memory.
- It sends ACK for all successfully received frames and sends NACK for only frames which are missing or damaged.
- The sender in this case, sends only packet for which NACK is received.

Sliding Window

This protocol improves the efficiency of stop and wait protocol by allowing multiple frames to be transmitted before receiving an acknowledgment.

The working principle of this protocol can be described as follows −

- Both the sender and the receiver has finite sized buffers called windows. The sender and the receiver agrees upon the number of frames to be sent based upon the buffer size.
- The sender sends multiple frames in a sequence, without waiting for acknowledgment. When its sending window is filled, it waits for acknowledgment. On receiving acknowledgment, it advances the window and transmits the next frames, according to the number of acknowledgments received.

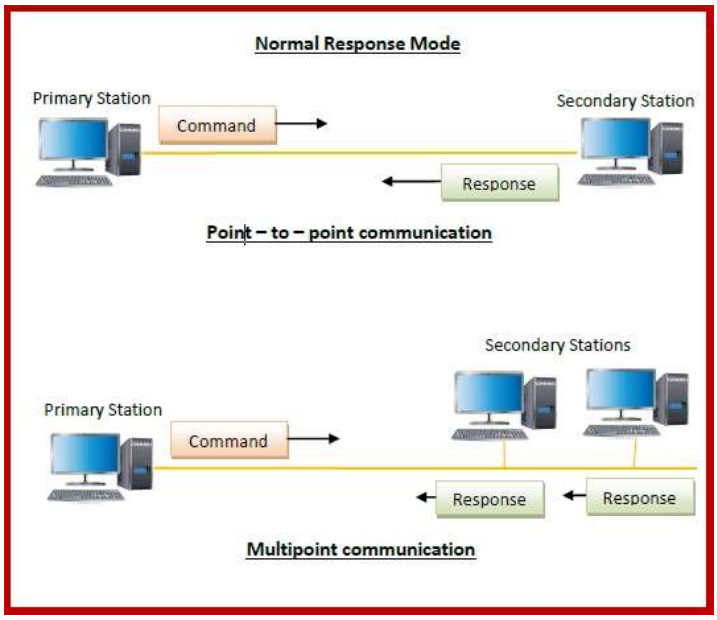
HDLC

- High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes.
- Since it is a data link protocol, data is organized into frames.
- A frame is transmitted via the network to the destination that verifies its successful arrival.
- It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.

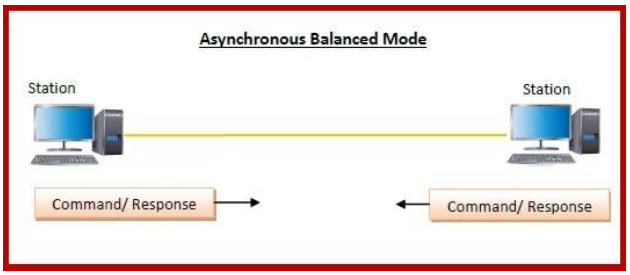
Transfer Modes

HDLC supports two types of transfer modes, normal response mode and asynchronous balanced mode.

- **Normal Response Mode (NRM)** − Here, two types of stations are there, a primary station that send commands and secondary station that can respond to received commands. It is used for both point - to - point and multipoint communications.



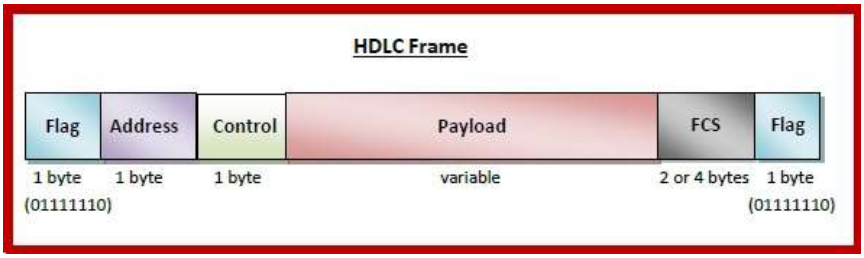
- **Asynchronous Balanced Mode (ABM)** − Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.



HDLC Frame

HDLC is a bit - oriented protocol where each frame contains up to six fields. The structure varies according to the type of frame. The fields of a HDLC frame are −

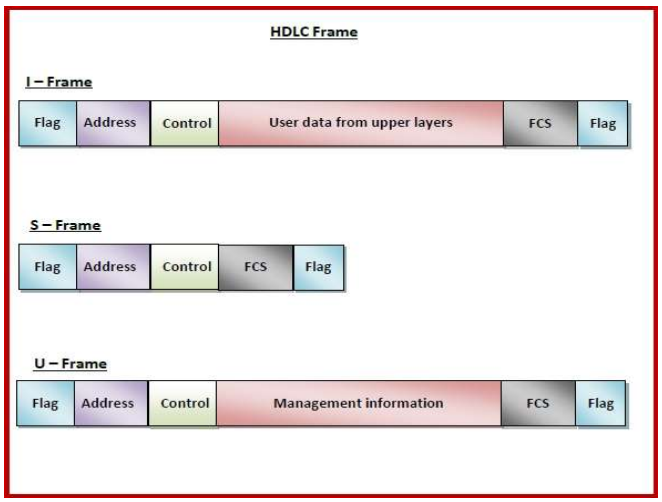
- **Flag** − It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
- **Control** − It is 1 or 2 bytes containing flow and error control information.
- **Payload** − This carries the data from the network layer. Its length may vary from one network to another.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



Types of HDLC Frames

There are three types of HDLC frames. The type of frame is determined by the control field of the frame −

- **I-frame** − I-frames or Information frames carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of control field of I-frame is 0.
- **S-frame** − S-frames or Supervisory frames do not contain information field. They are used for flow and error control when piggybacking is not required. The first two bits of control field of S-frame is 10.
- **U-frame** − U-frames or Un-numbered frames are used for myriad miscellaneous functions, like link management. It may contain an information field, if required. The first two bits of control field of U-frame is 11.



MEDIUM ACCESS SUB LAYER

Point to Point Protocol

- Point - to - Point Protocol (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 byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds.
- Since it is a data link layer protocol, data is transmitted in frames. It is also known as RFC 1661.

Services Provided by PPP

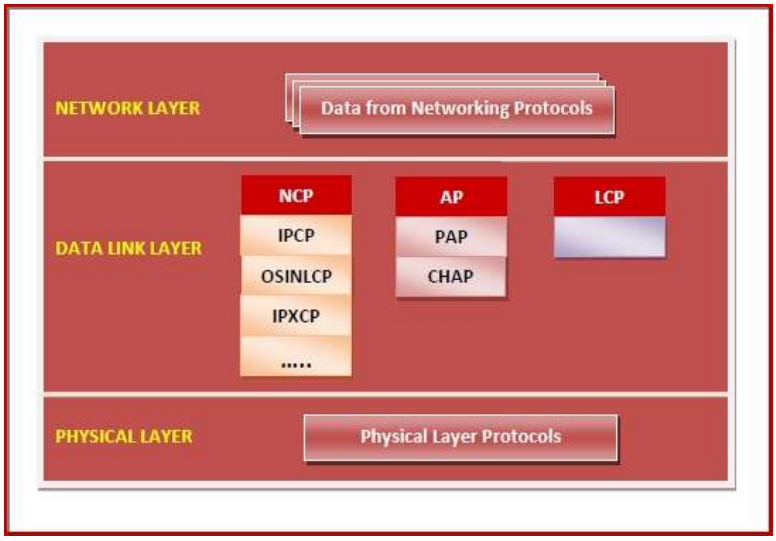
The main services provided by Point - to - Point Protocol are −

- Defining the frame format of the data to be transmitted.
- Defining the procedure of establishing link between two points and exchange of data.
- Stating the method of encapsulation of network layer data in the frame.
- Stating authentication rules of the communicating devices.
- Providing address for network communication.
- Providing connections over multiple links.
- Supporting a variety of network layer protocols by providing a range os services.

Components of PPP

Point - to - Point Protocol is a layered protocol having three components −

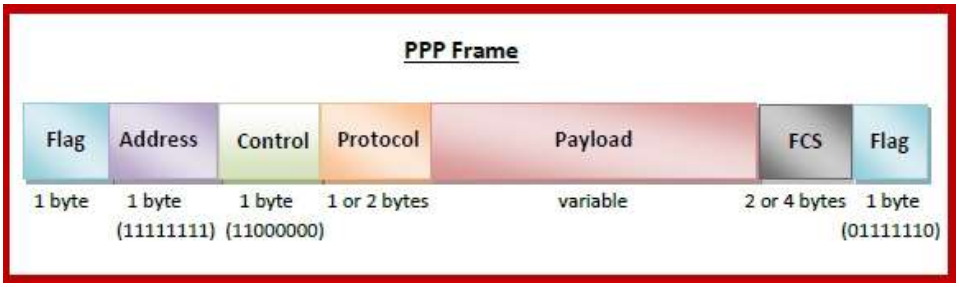
- **Encapsulation Component** − It encapsulates the datagram so that it can be transmitted over the specified physical layer.
- **Link Control Protocol (LCP)** − It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links.
- **Authentication Protocols (AP)** − These protocols authenticate endpoints for use of services. The two authentication protocols of PPP are:
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
- **Network Control Protocols (NCPs)** − These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there. Some of the NCPs of PPP are:
  - Internet Protocol Control Protocol (IPCP)
  - OSI Network Layer Control Protocol (OSINLCP)
  - Internetwork Packet Exchange Control Protocol (IPXCP)
  - DECnet Phase IV Control Protocol (DNCP)
  - NetBIOS Frames Control Protocol (NBFCP)
  - IPv6 Control Protocol (IPV6CP)



PPP Frame

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

- **Flag** − 1 byte that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − 1 byte which is set to 11111111 in case of broadcast.
- **Control** − 1 byte set to a constant value of 11000000.
- **Protocol** − 1 or 2 bytes that define the type of data contained in the payload field.
- **Payload** − This carries the data from the network layer. The maximum length of the payload field is 1500 bytes. However, this may be negotiated between the endpoints of communication.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



FDDI

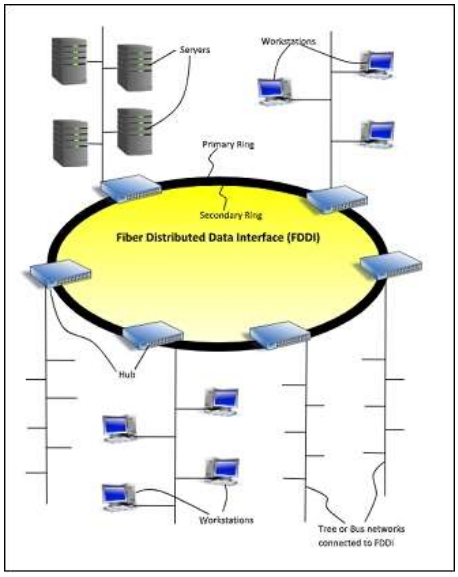
Fiber Distributed Data Interface (FDDI) is a set of ANSI and ISO standards for transmission of data in local area network (LAN) over fiber optic cables. It is applicable in large LANs that can extend up to 200 kilometers in diameter.

Features

- FDDI uses optical fiber as its physical medium.
- It operates in the physical and medium access control (MAC layer) of the Open Systems Interconnection (OSI) network model.
- It provides high data rate of 100 Mbps and can support thousands of users.

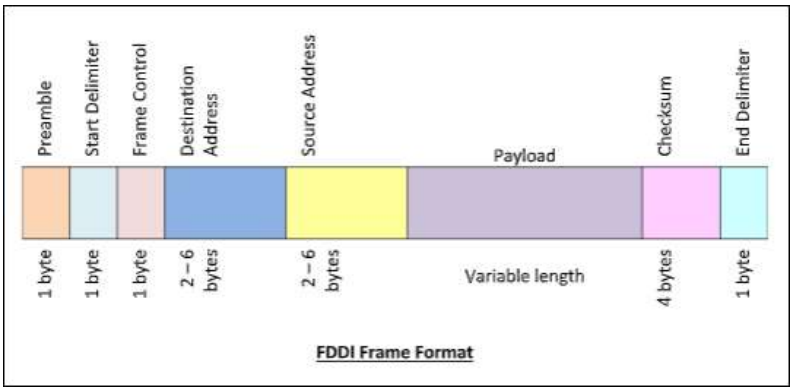
- It is used in LANs up to 200 kilometers for long distance voice and multimedia communication.
- It uses ring based token passing mechanism and is derived from IEEE 802.4 token bus standard.
- It contains two token rings, a primary ring for data and token transmission and a secondary ring that provides backup if the primary ring fails.
- FDDI technology can also be used as a backbone for a wide area network (WAN).

The following diagram shows FDDI –



Frame Format

The frame format of FDDI is similar to that of token bus as shown in the following diagram-



The fields of an FDDI frame are −

- **Preamble:** 1 byte for synchronization.
- **Start Delimiter:** 1 byte that marks the beginning of the frame.
- **Frame Control:** 1 byte that specifies whether this is a data frame or control frame.
- **Destination Address:** 2-6 bytes that specifies address of destination station.
- **Source Address:** 2-6 bytes that specifies address of source station.
- **Payload:** A variable length field that carries the data from the network layer.
- **Checksum:** 4 bytes frame check sequence for error detection.

- **End Delimiter:** 1 byte that marks the end of the frame.

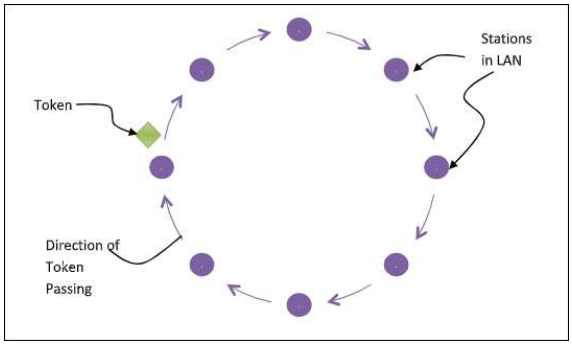
Token Bus and Token Ring

Token Ring

- Token ring (IEEE 802.5) is a communication protocol in a local area network (LAN) where all stations are connected in a ring topology and pass one or more tokens for channel acquisition.
- A token is a special frame of 3 bytes that circulates along the ring of stations. A station can send data frames only if it holds a token. The tokens are released on successful receipt of the data frame.

Token Passing Mechanism in Token Ring

If a station has a frame to transmit when it receives a token, it sends the frame and then passes the token to the next station; otherwise it simply passes the token to the next station. Passing the token means receiving the token from the preceding station and transmitting to the successor station. The data flow is unidirectional in the direction of the token passing. In order that tokens are not circulated infinitely, they are removed from the network once their purpose is completed. This is shown in the following diagram –

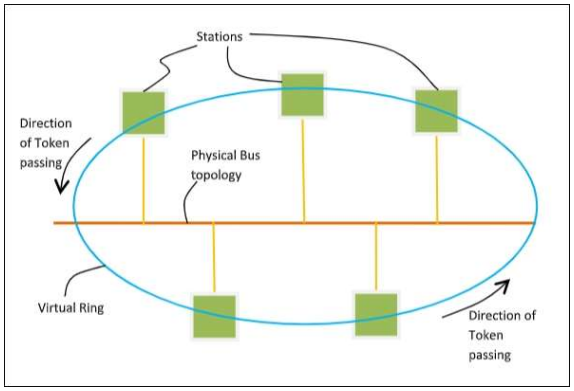


Token Bus

- Token Bus (IEEE 802.4) is a standard for implementing token ring over virtual ring in LANs.
- The physical media has a bus or a tree topology and uses coaxial cables.
- A virtual ring is created with the nodes/stations and the token is passed from one node to the next in a sequence along this virtual ring.
- Each node knows the address of its preceding station and its succeeding station.
- A station can only transmit data when it has the token.
- The working principle of token bus is similar to Token Ring.

Token Passing Mechanism in Token Bus

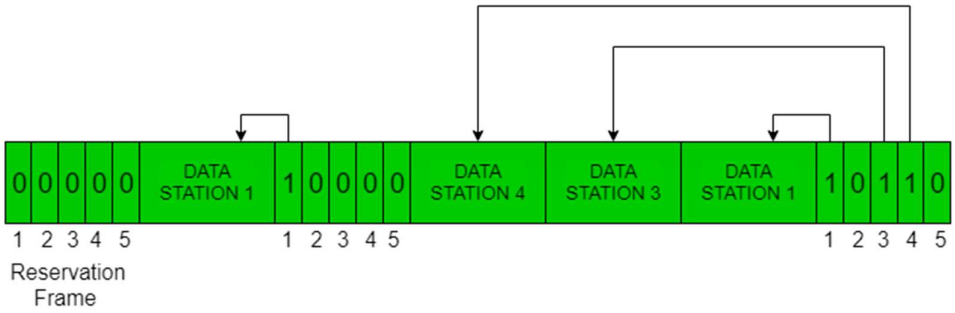
A token is a small message that circulates among the stations of a computer network providing permission to the stations for transmission. If a station has data to transmit when it receives a token, it sends the data and then passes the token to the next station; otherwise, it simply passes the token to the next station. This is depicted in the following diagram -



Reservation

- In the reservation method, a station needs to make a reservation before sending data.
- The time line has two kinds of periods:
  1. Reservation interval of fixed time length
  2. Data transmission period of variable frames.
- If there are M stations, the reservation interval is divided into M slots, and each station has one slot.
- Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.
- In general, i th station may announce that it has a frame to send by inserting a 1 bit into i th slot. After all N slots have been checked, each station knows which stations wish to transmit.
- The stations which have reserved their slots transfer their frames in that order.
- After data transmission period, next reservation interval begins.
- Since everyone agrees on who goes next, there will never be any collisions.

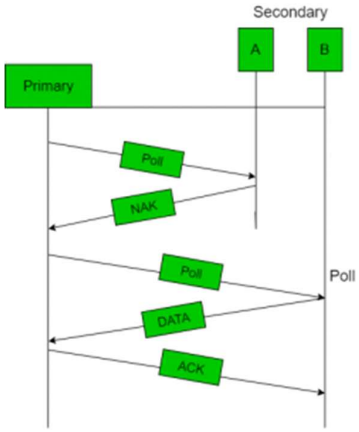
The following figure shows a situation with five stations and a five slot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.

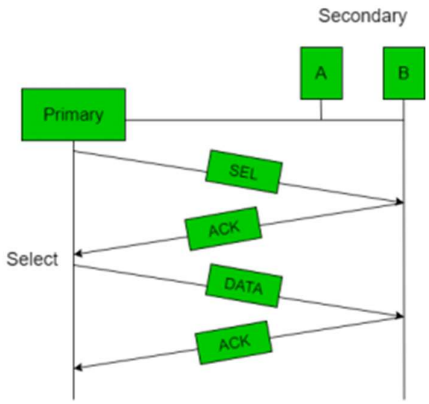


Polling

- Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn.
- In this, one acts as a primary station(controller) and the others are secondary stations. All data exchanges must be made through the controller.
- The message sent by the controller contains the address of the node being selected for granting access.

- Although all nodes receive the message but the addressed one responds to it and sends data, if any. If there is no data, usually a "poll reject"(NAK) message is sent back.
- Problems include high overhead of the polling messages and high dependence on the reliability of the controller.



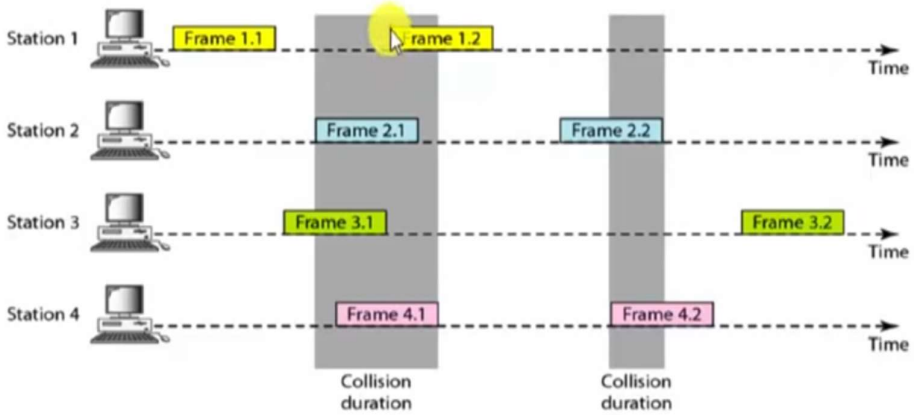


Pure Aloha

- It allows user to transmit whenever they have data to be sent.
- Senders wait to see if a collision occurred (after the whole message has been sent).
- If collision occurs, each station involved waits a random amount of time then tries again.
- System in which multiple users share a common channel in a way can lead to conflicts are widely known as contention system.
- Whenever 2 frames try to copy the channel at the same time, there will be a collision and both will be garbled.
- If the 1st bit of the new frame overlaps with hust the last bit of a frame almost finished, both frames will be totally destroyed and both frames will have to be retransmitted later.
- Frames are transmitted at completely arbitrary times.
- The throughput of the Pure Aloha is maximized when the frames are of uniform length.
- Formula to calculate the throughput of Pure Aloha is,

$$S = G * e^{2G}$$

- The throughput is maximum when G=1/2 which is 18% of the total transmitted data frames.

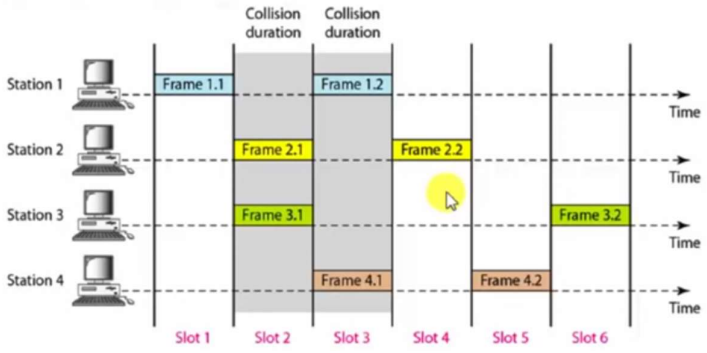


Slotted Aloha

- It was invented to improve the efficiency of Pure Aloha as chances of collision in Pure Aloha are very high.
- The time of the shared channel is divided into discrete intervals called slots.
- The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.
- If any station is not able to place the frame onto the channel at the beginning of the slot then the station has to wait until the beginning of the next time slot.
- The formula to calculate the throughput of the Slotted Aloha is

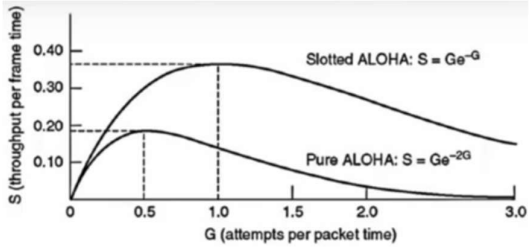
S = G * e^G

- The throughput is maximum when G=1 which is 37% of the total transmitted data frames.
- 37% of the time slot is empty, 37% successes and 26% collision.



Difference between Pure Aloha and Slotted Aloha

S.NO	Pure Aloha	Slotted Aloha
1.	In this aloha, any station can transmit the data at any time.	In this, any station can transmit the data at the beginning of any time slot.
2.	In this, The time is continuous and not globally synchronized.	In this, The time is discrete and globally synchronized.
3.	Vulnerable time for pure aloha = 2 x Tt	Vulnerable time for Slotted aloha = Tt
4.	In Pure Aloha, Probability of successful transmission of data packet $= G \times e^{-2G}$	In Slotted Aloha, Probability of successful transmission of data packet $= G \times e^{-G}$
5.	In pure aloha, Maximum efficiency = 18.4%	In slotted aloha, Maximum efficiency = 36.8%
6.	Pure aloha doesn't reduces the number of collisions to half.	Slotted aloha reduces the number of collisions to half and doubles the efficiency of pure aloha.

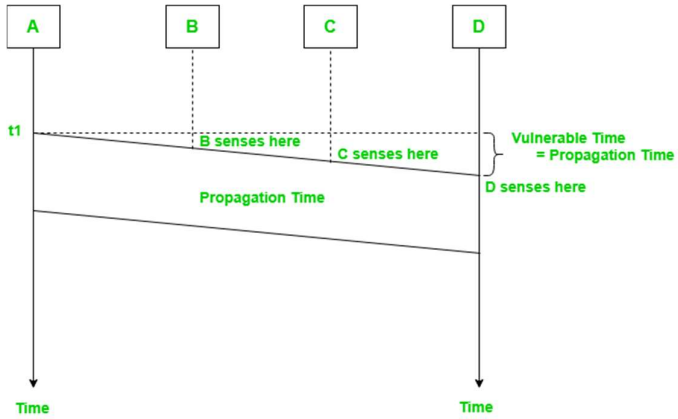


Carrier Sense Multiple Access (CSMA)

- This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the datalink layer.
- Carrier Sense multiple access requires that each station first check the state of the medium before sending.

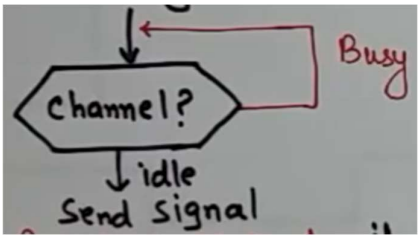
Vulnerable Time – It is the Propagation Time (Tp). This is the time needed for a signal to propagate from one end of the medium to the other end.

Vulnerable time = Propagation time (Tp)

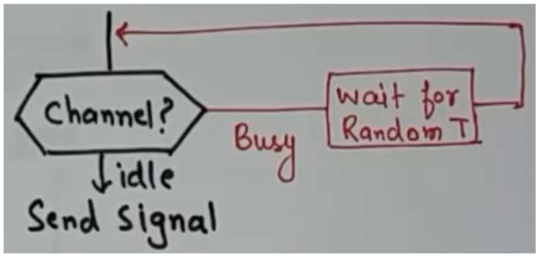


Persistence Methods in CSMA

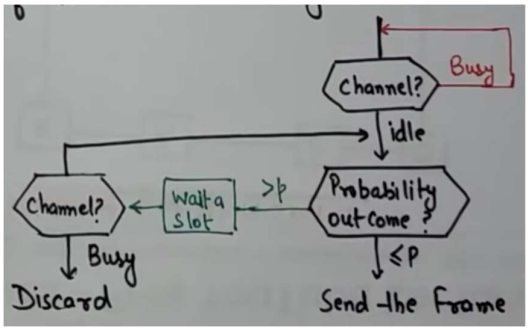
- **1 – persistent method:** If the station finds the line idle, it sends frame immediately (with probability 1).



- **Non – persistent method:** If the line is idle, station sends the frame immediately. If the line is not idle, it waits for a random amount of time and then senses the line again.

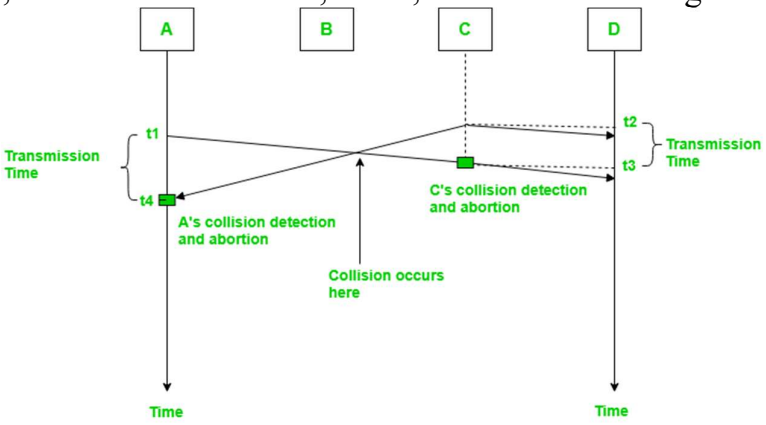


- **p – persistent method:** It combines the advantages of the other 2 strategies.



Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

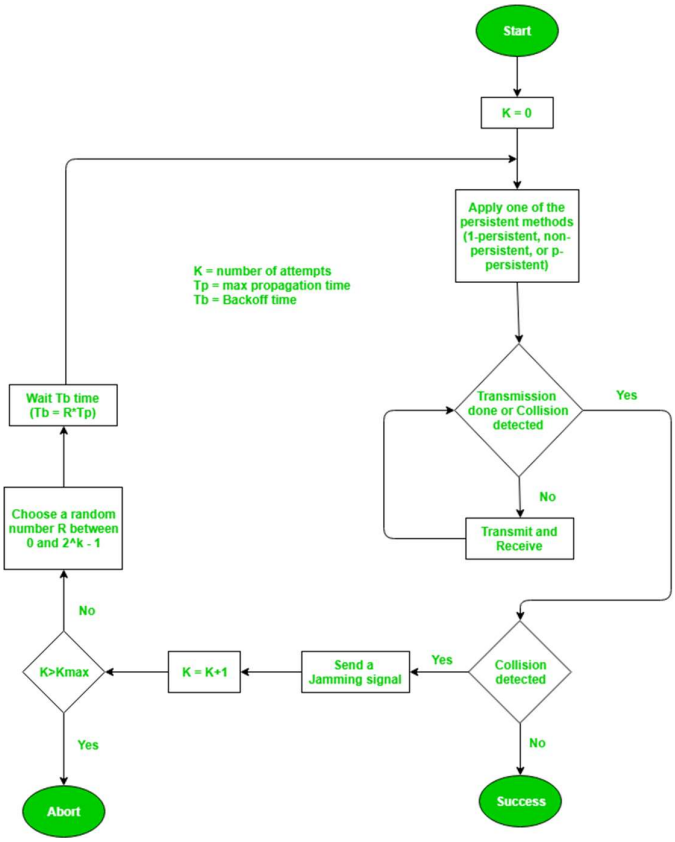
- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful.
- If successful, the station is finished, if not, the frame is sent again.



In the diagram, A starts send the first bit of its frame at t1 and since C sees the channel idle at t2, starts sending its frame at t2. C detects A's frame at t3 and aborts transmission. A detects C's frame at t4 and aborts its transmission. Transmission time for C's frame is therefore t3-t2 and for A's frame is t4-t1.

So, the frame transmission time (Tfr) should be at least twice the maximum propagation time (Tp). This can be deduced when the two stations involved in collision are maximum distance apart.

Process –



The entire process of collision detection can be explained as follows:

Throughput and Efficiency – The throughput of CSMA/CD is much greater than pure or slotted ALOHA.

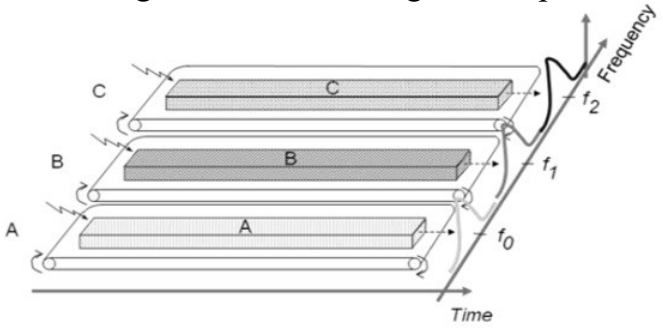
- For 1-persistent method throughput is 50% when G=1.
- For non-persistent method throughput can go upto 90%.

FDMA

- Frequency Division Multiple Access (FDMA) is one of the most common analogue multiple access methods.
- The frequency band is divided into channels of equal bandwidth so that each conversation is carried on a different frequency (as shown in the figure below).

Overview

- In FDMA method, guard bands are used between the adjacent signal spectra to minimize crosstalk between the channels.
- A specific frequency band is given to one person, and it will be received by identifying each of the frequency on the receiving end.
- It is often used in the first generation of analog mobile phone.



Advantages of FDMA

As FDMA systems use low bit rates (large symbol time) compared to average delay spread, it offers the following advantages −

- Reduces the bit rate information and the use of efficient numerical codes increases the capacity.
- It reduces the cost and lowers the inter symbol interference (ISI)
- Equalization is not necessary.
- An FDMA system can be easily implemented. A system can be configured so that the improvements in terms of speech encoder and bit rate reduction may be easily incorporated.
- Since the transmission is continuous, less number of bits are required for synchronization and framing.

Disadvantages of FDMA

Although FDMA offers several advantages, it has a few drawbacks as well, which are listed below −

- It does not differ significantly from analog systems; improving the capacity depends on the signal-to-interference reduction, or a signal-to-noise ratio (SNR).
- The maximum flow rate per channel is fixed and small.
- Guard bands lead to a waste of capacity.
- Hardware implies narrowband filters, which cannot be realized in VLSI and therefore increases the cost.

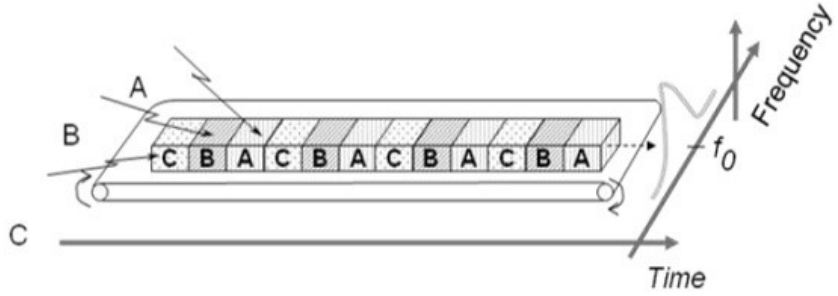
TDMA

- Time Division Multiple Access (TDMA) is a digital cellular telephone communication technology.
- It facilitates many users to share the same frequency without interference.
- Its technology divides a signal into different timeslots, and increases the data carrying capacity.

Overview

- Time Division Multiple Access (TDMA) is a complex technology, because it requires an accurate synchronization between the transmitter and the receiver.
- TDMA is used in digital mobile radio systems. The individual mobile stations cyclically assign a frequency for the exclusive use of a time interval.
- In most of the cases, the entire system bandwidth for an interval of time is not assigned to a station.
- However, the frequency of the system is divided into sub-bands, and TDMA is used for the multiple access in each sub-band. Sub-bands are known as carrier frequencies.
- The mobile system that uses this technique is referred as the multi-carrier systems.

In the following example, the frequency band has been shared by three users. Each user is assigned definite timeslots to send and receive data. In this example, user 'B' sends after user 'A,' and user 'C' sends thereafter. In this way, the peak power becomes a problem and larger by the burst communication.



Advantages of TDMA

Here is a list of few notable advantages of TDMA −

- Permits flexible rates (i.e. several slots can be assigned to a user, for example, each time interval translates 32Kbps, a user is assigned two 64 Kbps slots per frame).
- Can withstand gusty or variable bit rate traffic. Number of slots allocated to a user can be changed frame by frame (for example, two slots in the frame 1, three slots in the frame 2, one slot in the frame 3, frame 0 of the notches 4, etc.).
- No guard band required for the wideband system.

- No narrowband filter required for the wideband system.

Disadvantages of TDMA

The disadvantages of TDMA are as follow −

- High data rates of broadband systems require complex equalization.
- Due to the burst mode, a large number of additional bits are required for synchronization and supervision.
- Call time is needed in each slot to accommodate time to inaccuracies (due to clock instability).
- Electronics operating at high bit rates increase energy consumption.
- Complex signal processing is required to synchronize within short slots.

CDMA

- Code Division Multiple Access (CDMA) is a sort of multiplexing that facilitates various signals to occupy a single transmission channel.
- It optimizes the use of available bandwidth. The technology is commonly used in ultra-high-frequency (UHF) cellular telephone systems.

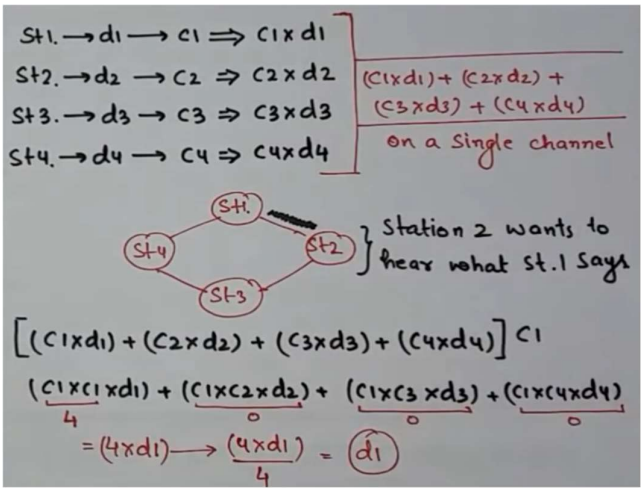
Overview

- Code Division Multiple Access system is very different from time and frequency multiplexing.
- In this system, a user has access to the whole bandwidth for the entire duration.
- The basic principle is that different CDMA codes are used to distinguish among the different users.

How communication with code takes place?

i. If codes are multiplied with each other, then the answer is 0.
ii. If codes are multiplied with itself, then we get 4 [no. of stations].

For ex.
Let there be 4 stations.
Let code for Station 1, 2, 3 and 4 be c1, c2, c3 and c4 respectively.
Let data for Station 1, 2, 3 and 4 be d1, d2, d3 and d4 respectively.
Therefore, **c1 * c2 = 0 and c2 * c2 = 4**



The factors deciding the CDMA capacity are −

- Processing Gain
- Signal to Noise Ratio
- Voice Activity Factor
- Frequency Reuse Efficiency

Advantages of CDMA

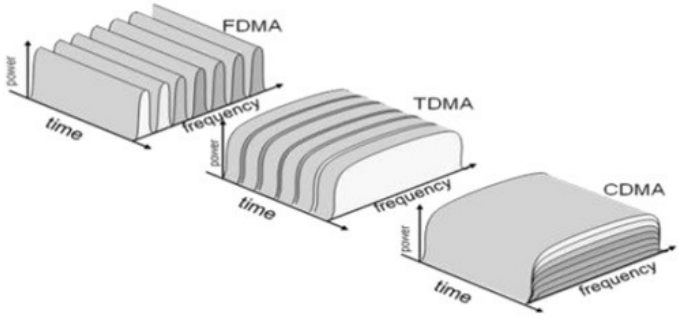
CDMA has a soft capacity. The greater the number of codes, the more the number of users. It has the following advantages −

- CDMA requires a tight power control, as it suffers from near-far effect. In other words, a user near the base station transmitting with the same power will drown the signal latter. All signals must have more or less equal power at the receiver
- Rake receivers can be used to improve signal reception. Delayed versions of time (a chip or later) of the signal (multipath signals) can be collected and used to make decisions at the bit level.
- Flexible transfer may be used. Mobile base stations can switch without changing operator. Two base stations receive mobile signal and the mobile receives signals from the two base stations.
- Transmission Burst − reduces interference.

Disadvantages of CDMA

The disadvantages of using CDMA are as follows −

- The code length must be carefully selected. A large code length can induce delay or may cause interference.
- Time synchronization is required.
- Gradual transfer increases the use of radio resources and may reduce capacity.
- As the sum of the power received and transmitted from a base station needs constant tight power control. This can result in several handovers.

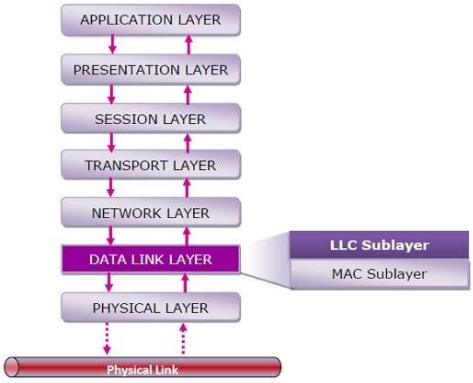


LLC

- The logical link control (LLC) is the upper sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission.
- It acts act an interface between the network layer and the medium access control (MAC) sublayer of the data link layer.
- The LLC sublayer is mainly used for its multiplexing property.
- It allows several network protocols to operate simultaneously within a multipoint network over the same network medium.

- The Open System Interconnections (OSI) model is a 7 – layered networking framework that conceptualizes how communications should be done between heterogeneous systems.
- The data link layer is the second lowest layer. It is divided into two sublayers −
  - The logical link control (LLC) sublayer
  - The medium access control (MAC) sublayer

The following diagram depicts the position of the LLC sublayer -



Functions

- The primary function of LLC is to multiplex protocols over the MAC layer while transmitting and likewise to de-multiplex the protocols while receiving.
- LLC provides hop-to-hop flow and error control.
- It allows multipoint communication over computer network.
- Frame Sequence Numbers are assigned by LLC.
- In case of acknowledged services, it tracks acknowledgements

Ethernet

- Ethernet is most widely used LAN Technology, which is defined under IEEE standards 802.3.
- The reason behind its wide usability is Ethernet is easy to understand, implement, maintain and allows low-cost network implementation.
- Also, Ethernet offers flexibility in terms of topologies which are allowed.
- Ethernet operates in two layers of the OSI model, Physical Layer, and Data Link Layer.
- For Ethernet, the protocol data unit is Frame since we mainly deal with DLL. In order to handle collision, the Access control mechanism used in Ethernet is CSMA/CD.

Traditional Ethernet and Fast Ethernet

- Traditional Ethernet supports data transfers at a rate of 10 megabits per second (Mbps). As the performance needs of networks increased over time, the industry created additional Ethernet specifications for Fast Ethernet and Gigabit Ethernet. The most common form of traditional Ethernet, however, is 10Base-T. It offers better electrical properties than Thicknet or Thinnet because 10Base-T cables use unshielded twisted pair (UTP) wiring rather than coaxial. 10Base-T is also more cost-effective than alternatives such as fiber optic cabling.

- Fast Ethernet extends traditional Ethernet performance up to 100 Mbps, and Gigabit Ethernet, up to 1,000 Mbps. Although they aren't available to the average consumer, 10 Gigabit Ethernet (10,000 Mbps) now powers the networks of some businesses, data centers, and Internet2 entities. Generally, however, the expense limits its widespread adoption. Fast Ethernet comes in two major varieties:
  i. 100Base-T (using unshielded twisted pair cable)
  ii. 100Base-FX (using fiber optic cable)

Network Devices

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub** - These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.
- **Passive Hub** - These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Types of Bridges

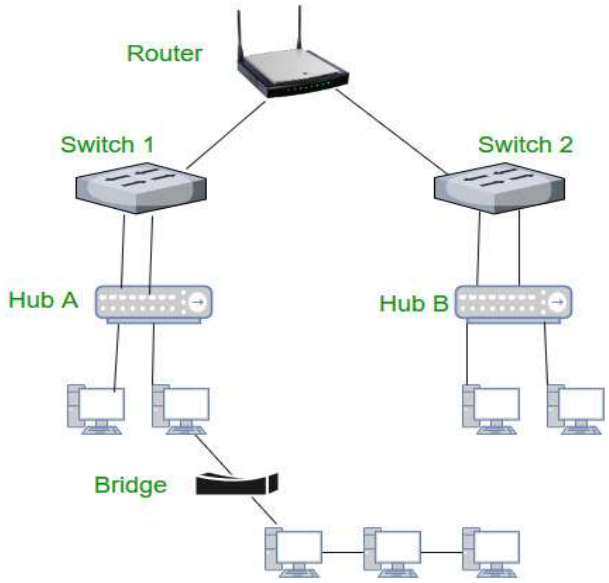
- **Transparent Bridges** - These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges** - In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

4. Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

7. Brouter – It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.

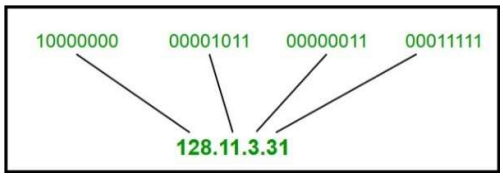


UNIT 3
NETWORK LAYER

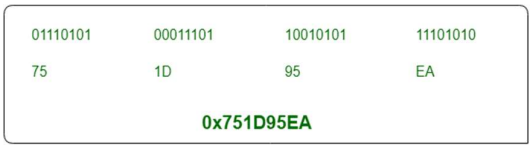
Internet Address

- IP address 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 232.
- Generally, there are two notations in which IP address is written, dotted decimal notation and hexadecimal notation.

Dotted Decimal Notation:



Hexadecimal Notation:



Some points to be noted about dotted decimal notation:

- The value of any segment (byte) is between 0 and 255 (both included).
- There are no zeroes 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:

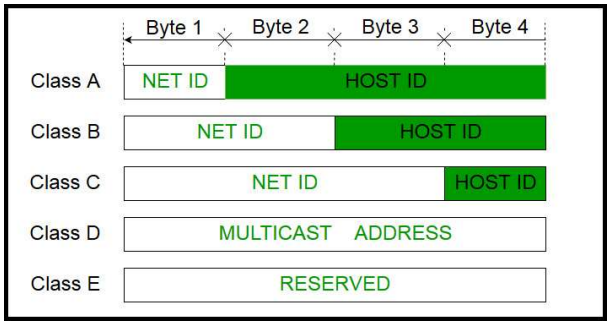
- Class A
- Class B
- Class C
- Class D
- Class E

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

IPv4 address is divided into two parts:

- Network ID
- Host ID

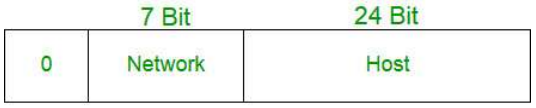
The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns IP address to each device that is connected to its network.



Note: IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).

Class A:
IP address belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.



Class A

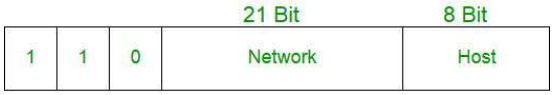
Class B:
IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.

- The network ID is 16 bits long.
- The host ID is 16 bits long.

Class B

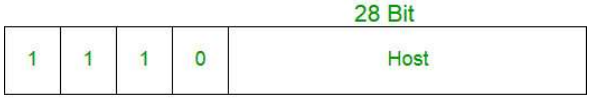
Class C:
IP address belonging to class C are assigned to small-sized networks.

- The network ID is 24 bits long.
- The host ID is 8 bits long.



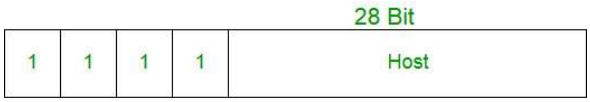
Class C

Class D:
IP address belonging to class D are reserved for multi-casting. The higher order 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

Class E:
IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254. 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

Problems with Classful Addressing:

- The problem with this classful addressing method is that millions of class A address are wasted, many of the class B address are wasted, whereas,
- number of addresses available in class C is so small that it cannot cater the needs of organizations.
- Class D addresses are used for multicast routing and are therefore available as a single block only.
- Class E addresses are reserved.

Since there are these problems, Classful networking was replaced by Classless Inter-Domain Routing (CIDR) in 1993. We will be discussing Classless addressing in next post.

Subnetting

- It is an idea of splitting a block to smaller blocks.
- In this, a network is divided into several smaller subnets with each subnetwork having its separate subnetwork address.
- A subnetwork has Subnet ID and Host ID.
- Subnetting increases the length of the net ID and decreases the length of the Host ID.

Subnet Address – When a network is subnetted, the first address in the subnet is identifier of the subnet and used by the router to route the packets destined for that subnetwork.

Types of Routing
Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.

There are 3 types of routing:
1. Static routing –
Static routing is a process in which we have to manually add routes in routing table. Static Routing is also known as non-adaptive routing which doesn't change routing table unless the network administrator changes or modify them manually. Static routing does not use complex routing algorithms and It provides high or more security than dynamic routing.

Advantages –

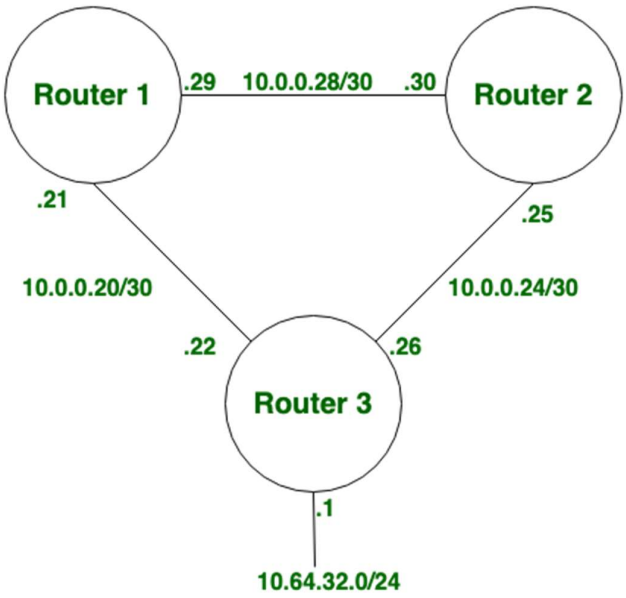
- No routing overhead for router CPU which means a cheaper router can be used to do routing.
- It adds security because only administrator can allow routing to particular networks only.

- No bandwidth usage between routers.

Disadvantage –

- For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.
- The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology.

Configuration –



2. Dynamic Routing –

Dynamic routing makes automatic adjustment of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach it. RIP and OSPF are the best examples of dynamic routing protocol. Automatic adjustment will be made to reach the network destination if one route goes down.

A dynamic protocol have following features:

- The routers should have the same dynamic protocol running in order to exchange routes.
- When a router finds a change in the topology then router advertises it to all other routers.

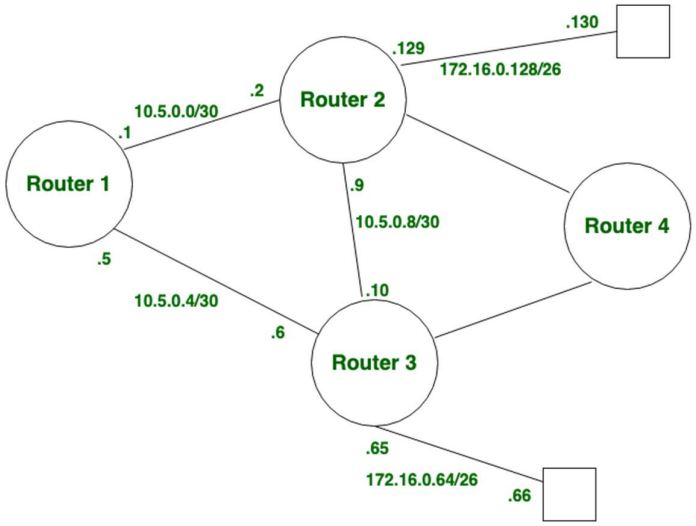
Advantages –

- Easy to configure.
- More effective at selecting the best route to a destination remote network and also for discovering remote network.

Disadvantage –

- Consumes more bandwidth for communicating with other neighbors.
- Less secure than static routing.

Configuration –



Difference between Static and Dynamic Routing:

S.NO	Static Routing	Dynamic Routing
1.	In static routing routes are user defined.	In dynamic routing, routes are updated according to topology.
2.	Static routing does not use complex routing algorithms.	Dynamic routing uses complex routing algorithms.
3.	Static routing provides high or more security.	Dynamic routing provides less security.
4.	Static routing is manual.	Dynamic routing is automated.
5.	Static routing is implemented in small networks.	Dynamic routing is implemented in large networks.
6.	In static routing, additional resources are not required.	In dynamic routing, additional resources are required.

Routing Table

A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables. See below a Routing Table:

Destination	Subnet mask	Interface
128.75.43.0	255.255.255.0	Eth0
128.75.43.0	255.255.255.128	Eth1
192.12.17.5	255.255.255.255	Eth3
default		Eth2

The entry corresponding to the default gateway configuration is a network destination of 0.0.0.0 with a network mask (netmask) of 0.0.0.0. The Subnet Mask of default route is always 255.255.255.255 .

Entries of an IP Routing Table:
A routing table contains the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination. Routing Table provides the device with instructions for sending the packet to the next hop on its route across the network.

Each entry in the routing table consists of the following entries:

- **Network ID:** The network ID or destination corresponding to the route.
- **Subnet Mask:** The mask that is used to match a destination IP address to the network ID.
- **Next Hop:** The IP address to which the packet is forwarded
- **Outgoing Interface:** Outgoing interface the packet should go out to reach the destination network.
- **Metric:** A common use of the metric is to indicate the minimum number of hops (routers crossed) to the network ID.

Routing table entries can be used to store the following types of routes:

- Directly Attached Network IDs
- Remote Network IDs
- Host Routes
- Default Route
- Destination

When a router receives a packet, it examines the destination IP address, and looks up into its Routing Table to figure out which interface packet will be sent out.

There are ways to maintain Routing Table:

- Directly connected networks are added automatically.
- Using Static Routing.
- Using Dynamic Routing.

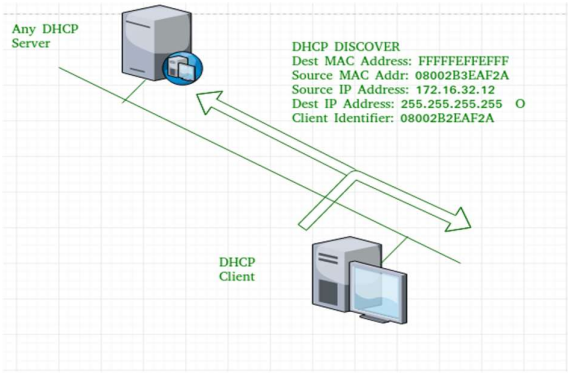
DHCP
Dynamic Host Configuration Protocol(DHCP) is an application layer protocol which is used to provide:

- Subnet Mask (Option 1 – e.g., 255.255.255.0)
- Router Address (Option 3 – e.g., 192.168.1.1)
- DNS Address (Option 6 – e.g., 8.8.8.8)
- Vendor Class Identifier (Option 43 – e.g., ‘unifi’ = 192.168.1.9 ##where unifi = controller)

1. DHCP is based on a client-server model and based on discovery, offer, request, and ACK.
2. DHCP port number for server is 67 and for the client is 68. It is a Client server protocol which uses UDP services. IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called DORA process, but there are 8 DHCP messages in the process.

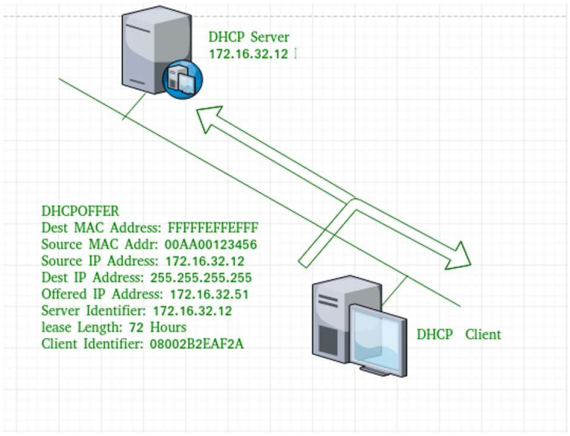
DHCP discover message –

This is a first message generated in the communication process between server and client. This message is generated by Client host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long.



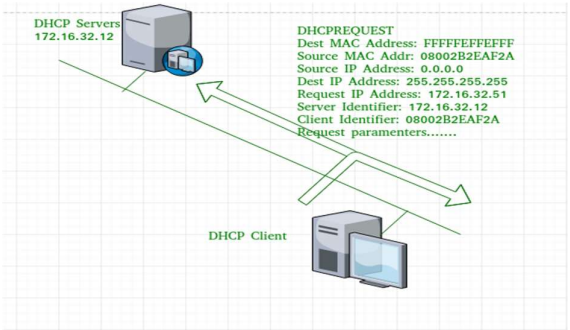
DHCP offer message –

The server will respond to host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by server. Size of message is 342 bytes. If there are more than one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives. Also a server ID is specified in the packet in order to identify the server.

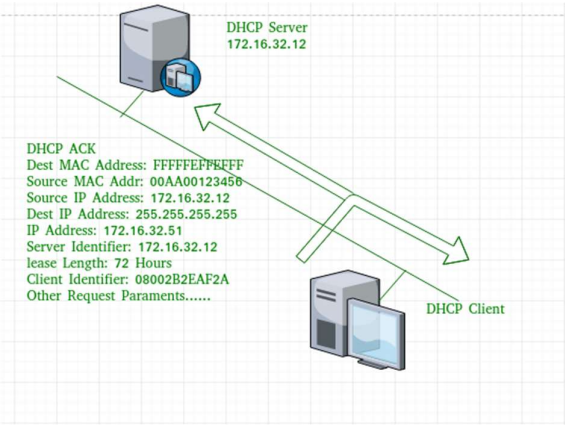


DHCP request message –

When a client receives a offer message, it responds by broadcasting a DHCP request message. The client will produce a gratitutous ARP in order to find if there is any other host present in the network with same IP address. If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP address. A Client ID is also added in this message.



DHCP acknowledgement message –
In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.



DHCP negative acknowledgement message –
Whenever a DHCP server receives a request for IP address that is invalid according to the scopes that is configured with, it send DHCP Nak message to client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to client.

DHCP decline –
If DHCP client determines the offered configuration parameters are different or invalid, it sends DHCP decline message to the server .When there is a reply to the gratuitous ARP by any host to the client, the client sends DHCP decline message to the server showing the offered IP address is already in use.

DHCP release –
A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.

DHCP inform –
If a client address has obtained IP address manually then the client uses a DHCP inform to obtain other local configuration parameters, such as domain name. In reply to the dhcp inform message, DHCP server generates DHCP ack message with local configuration suitable for the client without allocating a new IP address. This DHCP ack message is unicast to the client.

Advantages:
- centralized management of IP addresses
- ease of adding new clients to a network
- reuse of IP addresses reducing the total number of IP addresses that are required
- simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client

The DHCP protocol gives the network administrator a method to configure the network from a centralised area.
With the help of DHCP, easy handling of new users and reuse of IP address can be achieved.

Disadvantages:

- IP conflict can occur

IEEE 802 Wireless Standards

- The IEEE 802 Standard comprises a family of networking standards that cover the physical layer specifications of technologies from Ethernet to wireless.
- IEEE 802 is subdivided into 22 parts that cover the physical and data-link aspects of networking.
- The better known specifications (bold in table below) include 802.3 Ethernet, 802.11 Wi-Fi, 802.15 Bluetooth/ZigBee, and 802.16

802	**Overview**	**Basics of physical and logical networking concepts.**
802.1	Bridging	LAN/MAN bridging and management. Covers management and the lower sub-layers of OSI Layer 2, including MAC-based bridging (Media Access Control), virtual LANs and port-based access control.
802.2	Logical Link	Commonly referred to as the LLC or Logical Link Control specification. The LLC is the top sub-layer in the data-link layer, OSI Layer 2. Interfaces with the network Layer 3.
802.3	Ethernet	"Grandaddy" of the 802 specifications. Provides asynchronous networking using "carrier sense, multiple access with collision detect" (CSMA/CD) over coax, twisted-pair copper, and fiber media. Current speeds range from 10 Mbps to 10 Gbps. Click for a list of the "hot" 802.3 technologies.
802.4	Token Bus	Disbanded
802.5	Token Ring	The original token-passing standard for twisted-pair, shielded copper cables. Supports copper and fiber cabling from 4 Mbps to 100 Mbps. Often called "IBM Token-Ring."
802.6	Distributed queue dual bus (DQDB)	"Superseded **Revision of 802.1D-1990 edition (ISO/IEC 10038). 802.1D incorporates P802.1p and P802.12e. It also incorporates and supersedes published standards 802.1j and 802.6k. Superseded by 802.1D-2004." (See IEEE status page.)
802.7	Broadband LAN Practices	Withdrawn Standard. Withdrawn Date: Feb 07, 2003. No longer endorsed by the IEEE. (See IEEE status page.)

802.8	Fiber Optic Practices	Withdrawn PAR. Standards project no longer endorsed by the IEEE. (See IEEE status page.)
802.9	Integrated Services LAN	Withdrawn PAR. Standards project no longer endorsed by the IEEE. (See IEEE status page.)
802.10	Interoperable LAN security	Superseded **Contains: IEEE Std 802.10b-1992. (See IEEE status page.)
802.11	Wi-Fi	Wireless LAN Media Access Control and Physical Layer specification. 802.11a,b,g,etc. are amendments to the original 802.11 standard. Products that implement 802.11 standards must pass tests and are referred to as "Wi-Fi certified."
802.11a		• Specifies a PHY that operates in the 5 GHz U-NII band in the US - initially 5.15-5.35 AND 5.725-5.85 - since expanded to additional frequencies • Uses Orthogonal Frequency-Division Multiplexing • Enhanced data speed to 54 Mbps • Ratified after 802.11b
802.11b		• Enhancement to 802.11 that added higher data rate modes to the DSSS (Direct Sequence Spread Spectrum) already defined in the original 802.11 standard • Boosted data speed to 11 Mbps • 22 MHz Bandwidth yields 3 non-overlaping channels in the frequency range of 2.400 GHz to 2.4835 GHz • Beacons at 1 Mbps, falls back to 5.5, 2, or 1 Mbps from 11 Mbps max.
802.11d		• Enhancement to 802.11a and 802.11b that allows for global roaming • Particulars can be set at Media Access Control (MAC) layer
802.11e		• Enhancement to 802.11 that includes quality of service (QoS) features • Facilitates prioritization of data, voice, and video transmissions
802.11g		• Extends the maximum data rate of WLAN devices that operate in the 2.4 GHz band, in a fashion that permits interoperation with 802.11b devices

		• Uses OFDM Modulation (Orthogonal FDM) • Operates at up to 54 megabits per second (Mbps), with fall-back speeds that include the "b" speeds
802.11h		• Enhancement to 802.11a that resolves interference issues • Dynamic frequency selection (DFS) • Transmit power control (TPC)
802.11i		• Enhancement to 802.11 that offers additional security for WLAN applications • Defines more robust encryption, authentication, and key exchange, as well as options for key caching and pre-authentication
802.11j		• Japanese regulatory extensions to 802.11a specification • Frequency range 4.9 GHz to 5.0 GHz
802.11k		• Radio resource measurements for networks using 802.11 family specifications
802.11m		• Maintenance of 802.11 family specifications • Corrections and amendments to existing documentation
802.11n		• Higher-speed standards • Several competing and non-compatible technologies; often called "pre-n" • Top speeds claimed of 108, 240, and 350+ MHz • Competing proposals come from the groups, EWC, TGn Sync, and WWiSE and are all variations based on MIMO (multiple input, multiple output)
802.11x		• Mis-used "generic" term for 802.11 family specifications
802.12	Demand Priority	Increases Ethernet data rate to 100 Mbps by controlling media utilization.
802.13	Not used	Not used

802.14	Cable modems	Withdrawn PAR. Standards project no longer endorsed by the IEEE.
802.15	Wireless Personal Area Networks	Communications specification that was approved in early 2002 by the IEEE for wireless personal area networks (WPANs).
802.15.1	Bluetooth	Short range (10m) wireless technology for cordless mouse, keyboard, and hands-free headset at 2.4 GHz.
802.15.3a	UWB	Short range, high-bandwidth "ultra wideband" link
802.15.4	ZigBee	Short range wireless sensor networks
802.15.5	Mesh Network	• Extension of network coverage without increasing the transmit power or the receiver sensitivity • Enhanced reliability via route redundancy • Easier network configuration - Better device battery life
802.16	Wireless Metropolitan Area Networks	This family of standards covers Fixed and Mobile Broadband Wireless Access methods used to create Wireless Metropolitan Area Networks (WMANs.) Connects Base Stations to the Internet using OFDM in unlicensed (900 MHz, 2.4, 5.8 GHz) or licensed (700 MHz, 2.5 – 3.6 GHz) frequency bands. Products that implement 802.16 standards can undergo WiMAX certification testing.
802.17	Resilient Packet Ring	IEEE working group description
802.18	Radio Regulatory TAG	IEEE 802.18 standards committee
802.19	Coexistence	IEEE 802.19 Coexistence Technical Advisory Group
802.20	Mobile Broadband Wireless Access	IEEE 802.20 mission and project scope
802.21	Media Independent Handoff	IEEE 802.21 mission and project scope

802.22	Wireless Regional Area Network	IEEE 802.22 mission and project scope

Shortest Path Routing Algorithm

- It finds the shortest path between a given pair of routers.
- The cost of link from one node to another maybe a function of
  - Distance
  - Bandwidth
  - Average Traffic
  - Communication cost
  - Delay etc

For Shortest Path Routing Algorithm, we have the **Dijkstra Algorithm**.
Dijkstra's algorithm has many variants but the most common one is to find the shortest paths from the source vertex to all other vertices in the graph.

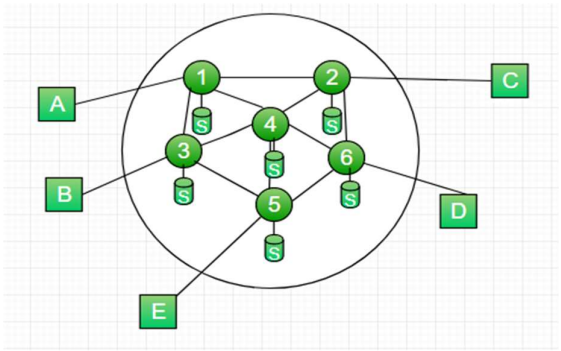
Algorithm Steps:

- Set all vertices distances = infinity except for the source vertex, set the source distance = 0.
- Push the source vertex in a min-priority queue in the form (distance, vertex), as the comparison in the min-priority queue will be according to vertices distances.
- Pop the vertex with the minimum distance from the priority queue (at first the popped vertex = source).
- Update the distances of the connected vertices to the popped vertex in case of "current vertex distance + edge weight < next vertex distance", then push the vertex
- with the new distance to the priority queue.
- If the popped vertex is visited before, just continue without using it.
- Apply the same algorithm again until the priority queue is empty.

Time Complexity of Dijkstra's Algorithm is O(V^3) but with min-priority queue it drops down to O(V + E log V).

Flooding Routing Algorithm

- Requires no network information like topology, load condition ,cost of diff. paths
- Every incoming packet to a node is sent out on every outgoing like except the one it arrived on.



- For Example in above figure
    - A incoming packet to (1) is sent out to (2), (3)
    - from (2) is sent to (6), (4) and from (3) it is sent to (4), (5)
    - from (4) it is sent to (6), (5), (3), from (6) it is sent to (2), (4), (5), from (5) it is sent to (4), (3)

Characteristics –

- All possible routes between Source and Destination is tried. A packet will always get through if path exists
- As all routes are tried, there will be atleast one route which is the shortest
- All nodes directly or indirectly connected are visited

Limitations –

- Flooding generates vast number of duplicate packets
- Suitable damping mechanism must be used

Techniques to eliminate Duplicate packets:

Hop-Count –

- A hop counter may be contained in the packet header which is decremented at each hop.
- with the packet being discarded when the counter becomes zero
- The sender initializes the hop counter. If no estimate is known, it is set to the full diameter of the subnet.
- Keep track of the packets which are responsible for flooding using a sequence number. Avoid sending them out a second time.

Sequence no. in packets –

- Avoid sending the same packet for the second time.
- Keep in each router per source a list of packets already seen.

Selective Flooding: Routers do not send every incoming packet out on every line, only on those lines that go in approximately in the direction of the destination.

Advantages:

- Highly Robust, emergency or immediate messages can be sent (eg military applications)
- Set up route in virtual circuit
- Flooding always chooses the shortest path
- Broadcast messages to all the nodes

Distance Vector Routing (DVR) Protocol

- A distance-vector routing (DVR) protocol requires that a router inform its neighbors of topology changes periodically.
- Historically known as the old ARPANET routing algorithm (or known as Bellman-Ford algorithm).

Bellman Ford Basics – Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes. Distances,based on a chosen metric, are computed using information from the neighbors' distance vectors.

Information kept by DV router -

- Each router has an ID
- Associated with each link connected to a router,
- there is a link cost (static or dynamic).
- Intermediate hops

Distance Vector Table Initialization -

- Distance to itself = 0
- Distance to ALL other routers = infinity number.

Distance Vector Algorithm –

- A router transmits its distance vector to each of its neighbors in a routing packet.
- Each router receives and saves the most recently received distance vector from each of its neighbors.
- A router recalculates its distance vector when:
  - It receives a distance vector from a neighbor containing different information than before.
  - It discovers that a link to a neighbor has gone down.

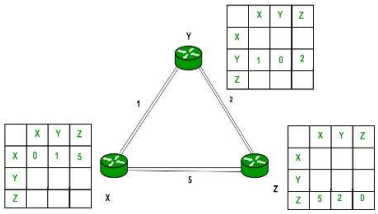
The DV calculation is based on minimizing the cost to each destination
Dx(y) = Estimate of least cost from x to y
C(x,v) = Node x knows cost to each neighbor v
Dx = [Dx(y): y ∈ N] = Node x maintains distance vector
Node x also maintains its neighbors' distance vectors
– For each neighbor v, x maintains Dv = [Dv(y): y ∈ N]

Note –

- From time-to-time, each node sends its own distance vector estimate to neighbors.
- When a node x receives new DV estimate from any neighbor v, it saves v's distance vector and it updates its own DV using B-F equation:

$$D_x(y) = \min \{ C(x,v) + D_v(y), D_x(y) \} \text{ for each node } y \in N$$

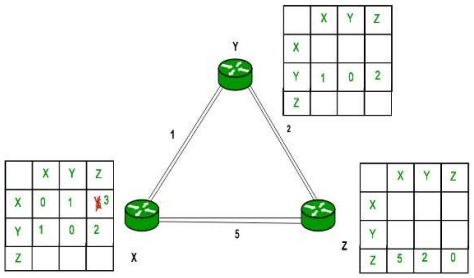
Example – Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.



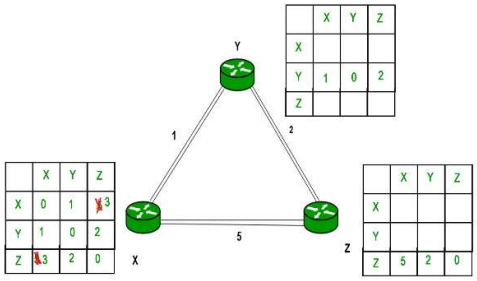
Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.

$$Dx(y) = \min \{ C(x,v) + Dv(y)\} \text{ for each node } y \in N$$

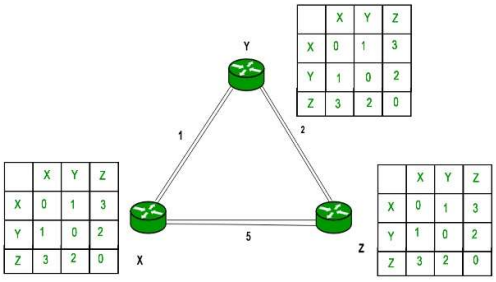
As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.



Similarly for Z also –



Finally the routing table for all –



Advantages –

- It is simpler to configure and maintain than link state routing.

Disadvantages –

- It is slower to converge than link state.
- It is at risk from the count-to-infinity problem.

- It creates more traffic than link state since a hop count change must be propagated to all routers and processed on each router. Hop count updates take place on a periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.
- For larger networks, distance vector routing results in larger routing tables than link state since each router must know about all other routers. This can also lead to congestion on WAN links.

Note – Distance Vector routing uses UDP(User datagram protocol) for transportation.

Link State Routing Algorithm

- Link state routing is the second family of routing protocols.
- While distance vector routers use a distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology.
- Based on this learned topology, each router is then able to compute its routing table by using a shortest path computation.

Features –

- **Link state packet** – A small packet that contains routing information.
- **Link state database** – A collection information gathered from link state packet.
- **Shortest path first algorithm (Dijkstra algorithm)** – A calculation performed on the database results into shortest path
- **Routing table** – A list of known paths and interfaces.

Calculation of shortest path –

To find shortest path, each node need to run the famous Dijkstra algorithm. This famous algorithm uses the following steps:

Step-1: The node is taken and chosen as a root node of the tree, this creates the tree with a single node, and now set the total cost of each node to some value based on the information in Link State Database

Step-2: Now the node selects one node, among all the nodes not in the tree like structure, which is nearest to the root, and adds this to the tree.The shape of the tree gets changed .

Step-3: After this node is added to the tree, the cost of all the nodes not in the tree needs to be updated because the paths may have been changed.

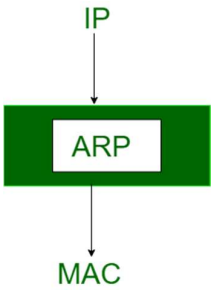
Step-4: The node repeats the Step 2. and Step 3. until all the nodes are added in the tree

Link State protocols in comparison to Distance Vector protocols have:

1. It requires large amount of memory.
2. Shortest path computations require many CPU circles.
3. If network use the little bandwidth ; it quickly reacts to topology changes
4. All items in the database must be sent to neighbors to form link state packets.
5. All neighbors must be trusted in the topology.
6. Authentication mechanisms can be used to avoid undesired adjacency and problems.
7. No split horizon techniques are possible in the link state routing.

ARP (Address Resolution Protocol)

- Most of the computer programs/applications use logical address (IP address) to send/receive messages, however the actual communication happens over the physical address (MAC address) i.e from layer 2 of OSI model.
- So, our mission is to get the destination MAC address which helps in communicating with other devices.
- This is where ARP comes into the picture, its functionality is to translate IP address to physical address.



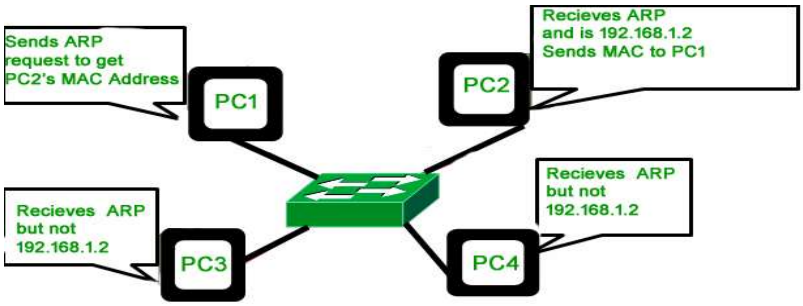
- The acronym ARP stands for Address Resolution Protocol which is one of the most important protocols of the Network layer in the OSI model.

Note: ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address.

ARP working

Before sending the IP packet, the MAC address of destination must be known. If not so, then sender broadcasts the ARP-discovery packet requesting the MAC address of intended destination. Since ARP-discovery is broadcast, every host inside that network will get this message but the packet will be discarded by everyone except that intended receiver host whose IP is associated. Now, this receiver will send a unicast packet with its MAC address (ARP-reply) to the sender of ARP-discovery packet. After the original sender receives the ARP-reply, it updates ARP-cache and start sending unicast message to the destination.

The above process continues till the second last network device in the path to reach the destination where it gets validated and ARP, in turn, responds with the destination MAC address.



The important terms associated with ARP are :

- **ARP Cache:** After resolving MAC address, the ARP sends it to the source where it stores in a table for future reference. The subsequent communications can use the MAC address from the table

- **ARP Cache Timeout:** It indicates the time for which the MAC address in the ARP cache can reside
- **ARP request:** This is nothing but broadcasting a packet over the network to validate whether we came across destination MAC address or not.
  ARP request packet contains:
  - The physical address of the sender.
  - The IP address of the sender.
  - The physical address of the receiver is 0s.
  - The IP address of the receiver

  Note, that the ARP packet is encapsulated directly into data link frame.
- **ARP response/reply:** It is the MAC address response that the source receives from the destination which aids in further communication of the data.

Cases when ARP is used:

CASE-1: The sender is a host and wants to send a packet to another host on the same network.

- Use ARP to find another host's physical address

CASE-2: The sender is a host and wants to send a packet to another host on another network.

- Sender looks at its routing table.
- Find the IP address of the next hop (router) for this destination.
- Use ARP to find the router's physical address

CASE-3: the sender is a router and received a datagram destined for a host on another network.

- Router check its routing table.
- Find the IP address of the next router.
- Use ARP to find the next router's physical address.

CASE-4: The sender is a router that has received a datagram destined for a host in the same network.

- Use ARP to find this host's physical address.

NOTE: An ARP request is a broadcast, and an ARP response is a Unicast.

Reverse Address Resolution Protocol (RARP)

- Reverse ARP is a networking protocol used by a client machine in a local area network to request its Internet Protocol address (IPv4) from the gateway-router's ARP table.
- The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.
- When a new machine is setup or any machine, which don't have memory to store IP address, needs an IP address for its own use.

- So, the machine sends a RARP broadcast packet which contains its own MAC address in both sender and receiver hardware address field.

A special host configured inside the local area network, called as RARP-server is responsible to reply for these kind of broadcast packets. Now the RARP server attempt to find out the entry in IP to MAC address mapping table. If any entry matches in table, RARP server send the response packet to the requesting device along with IP address.

- LAN technologies like Ethernet, Ethernet II, Token Ring and Fiber Distributed Data Interface (FDDI) support the Address Resolution Protocol.
- RARP is not being used in today's networks. Because we have much great featured protocols like BOOTP (Bootstrap Protocol) and DHCP(Dynamic Host Configuration Protocol).

IP

- An IP address is a unique identifier for every machine using the internet.
- An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.
- An IP address serves two main functions: host or network interface identification and location addressing.
- Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number.
- However, because of the growth of the Internet and the depletion of available IPv4 addresses, a new version of IP (IPv6), using 128 bits for the IP address, was standardized in 1998.
- An IP address serves two principal functions. It identifies the host, or more specifically its network interface, and it provides the location of the host in the network, and thus the capability of establishing a path to that host.

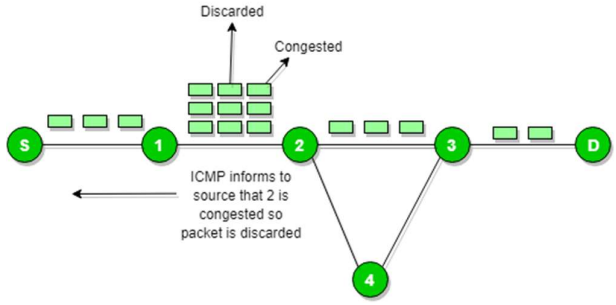
Internet Control Message Protocol (ICMP)

- Since IP does not have a inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide an error control.
- It is used for reporting errors and management queries.
- It is a supporting protocol and used by networks devices like routers for sending the error messages and operations information.
- e.g. the requested service is not available or that a host or router could not be reached.

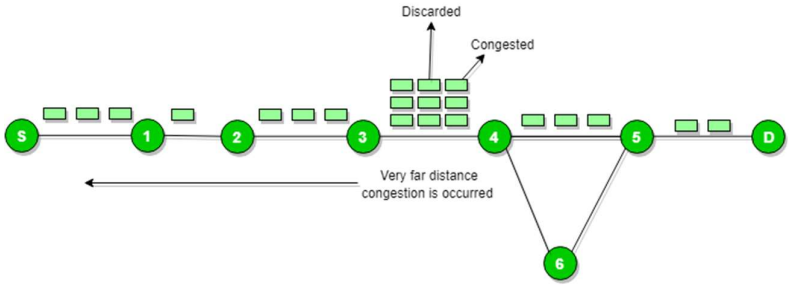
Source quench message:

Source quench message is a request to decrease traffic rate for messages sending to the host(destination). Or we can say, when receiving host detects that rate of sending packets (traffic rate) to it is too fast it sends the source quench message to the source to slow the pace down so that no packet can be lost.

ICMP will take source IP from the discarded packet and informs to source by sending source quench message.



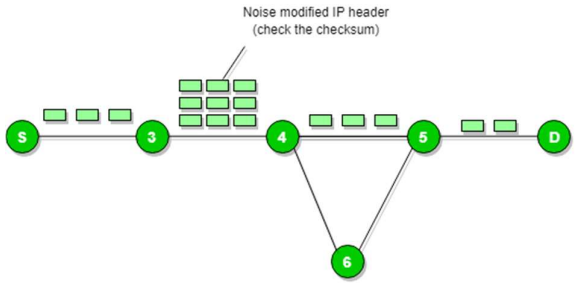
Then source will reduce the speed of transmission so that router will free for congestion.



When the congestion router is far away from the source the ICMP will send hop by hop source quench message so that every router will reduce the speed of transmission.

Parameter problem:

Whenever packets come to the router then calculated header checksum should be equal to recieved header checksum then only packet is accepted by the router.

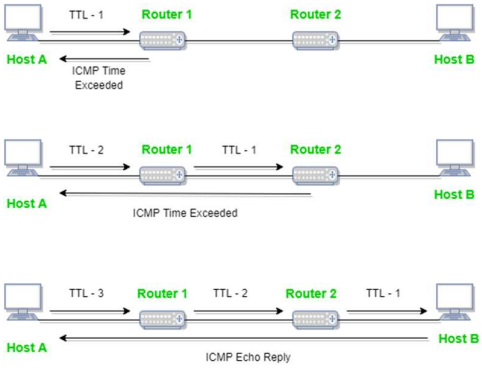


If there is mismatch packet will be dropped by the router.

ICMP will take the source IP from the discarded packet and informs to source by sending parameter problem message.

Time exceeded message:

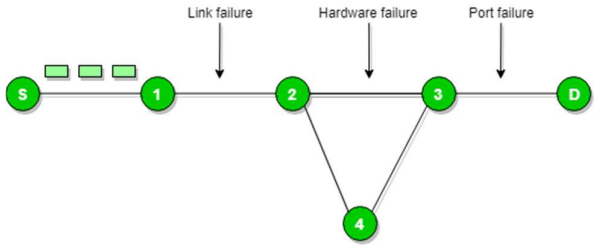
When some fragments are lost in a network then the holding fragment by the router will be droped then ICMP will take source IP from discarded packet and informs to the source, of



discarded datagram due to time to live field reaches to zero, by sending time exceeded message.

Destination un-reachable:

Destination unreachable is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason.



There is no necessary condition that only router give the ICMP error message some time destination host send ICMP error message when any type of failure (link failure,hardware failure,port failure etc) happen in the network.

Redirection message:

Redirect requests data packets be sent on an alternate route. The message informs to a host to update its routing information (to send packets on an alternate route).

Ex. If host tries to send data through a router R1 and R1 sends data on a router R2 and there is a direct way from host to R2. Then R1 will send a redirect message to inform the host that there is a best way to the destination directly through R2 available. The host then sends data packets for the destination directly to R2.

The router R2 will send the original datagram to the intended destination.

But if datagram contains routing information then this message will not be sent even if a better route is available as redirects should only be sent by gateways and should not be sent by Internet hosts.

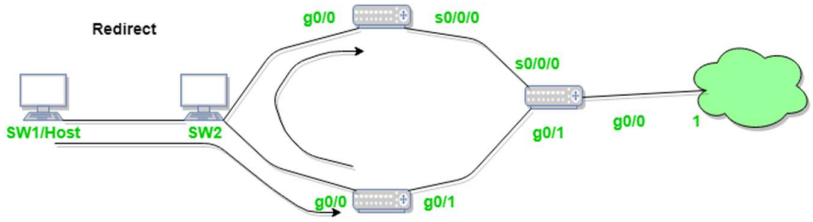


Figure - ICMP redirect Verification CCNP 2.0 100 - 101 (v - 71)

- ICMP Redirect
- ICMP Redirect for host
- ICMP Redirect for network
- How ICMP redirect work
- ICMP Redirect verification step by step

IGMP

- The Internet Group Management Protocol (IGMP) is an Internet protocol that provides a way for an Internet computer to report its multicast group membership to adjacent routers.
- Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content.

- Multicasting can be used for such applications as updating the address books of mobile computer users in the field, sending out company newsletters to a distribution list, and "broadcasting" high-bandwidth programs of streaming media to an audience that has "tuned in" by setting up a multicast group membership.

Using the Open Systems Interconnection (OSI) communication model, IGMP is part of the Network layer. IGMP is formally described in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 2236.

Difference between ICMP and IGMP

S.NO	ICMP	IGMP
1.	ICMP stands for Internet Control Message Protocol.	While IGMP stands for Internet Group Message Protocol.
2.	ICMP has **PING** features.	While it has the **Multicast** feature.
3.	Internet control message protocol is unicasting.	While internet group message protocol is multicasting.
4.	ICMP can be operate between host to host or host to router or router to router.	While IGMP can be used between client to multicast router.
5.	ICMP is a layer3 protocol.	IGMP is also a network layer or layer3 protocol.
6.	It controls the unicast communication and used for reporting error.	It controls the multicast communication.
7.	ICMP could be a mechanism employed by hosts and gateway to send notification of datagram downside back to sender.	While IGMP is employed to facilitate the synchronal transmission of a message to a bunch of recipients.

IPv6

- IPv6 (Internet Protocol version 6) is a set of specifications from the Internet Engineering Task Force (IETF) that is essentially an upgrade of IP version 4 (IPv4), a category of IP addresses in IPv4-based routing.
- The basics of IPv6 are similar to those of IPv4 -- devices can use IPv6 as source and destination addresses to pass packets over a network, and tools like ping work for network testing as they do in IPv4, with some slight variations.

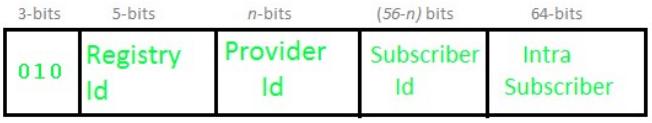
The specification (RFC8200) for IPv6 was published in 2017 and was elevated to Internet Standard (STD86).

Difference between IPv4 and IPv6

The most obvious improvement in IPv6 over IPv4 is that IP addresses are lengthened from 32 bits to 128 bits. This extension anticipates considerable future growth of the Internet and provides relief for what was perceived as an impending shortage of network addresses. IPv6 also supports auto-configuration to help correct most of the shortcomings in version 4, and it has integrated security and mobility features.

Types of IPv6 address:

- Provider based Unicast address:



- Geography based Unicast address:

Benefits of IPv6

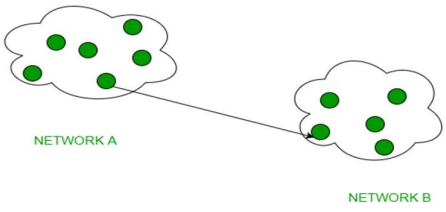
- Supports source and destination addresses that are 128 bits (16 bytes) long
- Uses a link-local scope all-nodes multicast address
- Does not require manual configuration or DHCP.
- Uses host address (AAAA) resource records in DNS to map host names to IPv6 addresses.
- Uses pointer resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.
- Supports a 1280-byte packet size (without fragmentation).
- Uses Flow Label field to identify packet flow for quality of service (QoS) handling by router.
- Uses Internet Control Message Protocol version 6 (ICMPv6) Router Solicitation and Router Advertisement messages to determine the IP address of the best default gateway.
- Uses Multicast Neighbor Solicitation messages to resolve IP addresses to link-layer addresses.
- Uses Multicast Listener Discovery (MLD) messages to manage membership in local subnet

Unicast, Broadcast and Multicast Routing Protocols

- The cast term here signifies some data (stream of packets) is being transmitted to the recipient(s) from client(s) side over the communication channel that help them to communicate.

1. Unicast –

This type of information transfer is useful when there is a participation of single sender and single recipient. So, in short you can term it as a one-to-one transmission. For example, a device having IP address 10.1.2.0 in a network wants to send the traffic stream(data packets)



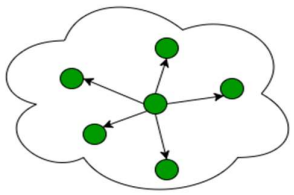
UNICAST EXAMPLE

to the device with IP address 20.12.4.2 in the other network,then unicast comes into picture. This is the most common form of data transfer over the networks.

2. Broadcast –

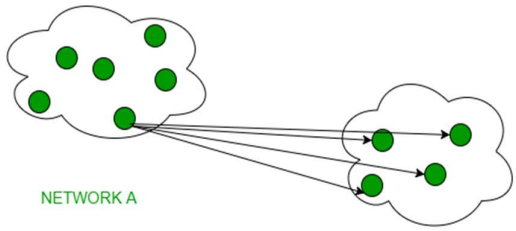
Broadcasting transfer (one-to-all) techniques can be classified into two types :

- **Limited Broadcasting –**
  Suppose you have to send stream of packets to all the devices over the network that you reside, this broadcasting comes handy. For this to achieve,it will append 255.255.255.255 (all the 32 bits of IP address set to 1) called as Limited Broadcast Address in the destination address of the datagram (packet) header which is reserved for information tranfer to all the recipients from a single client (sender) over the network.



NETWORK CLUSTER

- **Direct Broadcasting –**
  This is useful when a device in one network wants to transfer packet stream to all the devices over the other network.This is achieved by translating all the Host ID part bits of the destination address to 1,referred as Direct Broadcast Address in the datagram header for information transfer.



This mode is mainly utilized by television networks for video and audio distribution.
One important protocol of this class in Computer Networks is Address Resolution Protocol (ARP) that is used for resolving IP address into physical address which is necessary for underlying communication.

3. Multicast –

In multicasting, one/more senders and one/more recipients participate in data transfer traffic. In this method traffic recline between the boundaries of unicast (one-to-one) and broadcast (one-to-all). Multicast lets server's direct single copies of data streams that are then simulated and routed to hosts that request it. IP multicast requires support of some other protocols like IGMP (Internet Group Management Protocol), Multicast routing for its working. Also in Classful IP addressing Class D is reserved for multicast groups.

UNIT 4
TRANSPORT LAYER

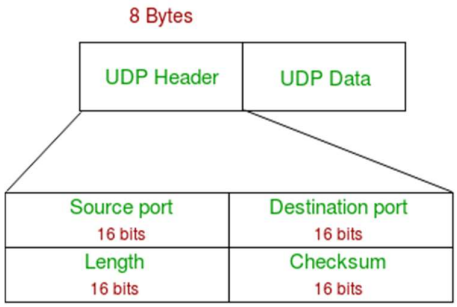
Various responsibilities of a Transport Layer –

- **Process to process delivery –** While Data Link Layer requires the MAC address (48 bits address contained inside the Network Interface Card of every host machine) of source-destination hosts to correctly deliver a frame and Network layer requires the IP address for appropriate routing of packets , in a similar way Transport Layer requires a Port number to correctly deliver the segments of data to the correct process amongst the multiple processes running on a particular host. A port number is a 16 bit address used to identify any client-server program uniquely.
- **End-to-end Connection between hosts –** The transport layer is also responsible for creating the end-to-end Connection between hosts for which it mainly uses TCP and UDP. TCP is a secure, connection- orientated protocol which uses a handshake protocol to establish a robust connection between two end- hosts. TCP ensures reliable delivery of messages and is used in various applications. UDP, on the other hand, is a stateless and unreliable protocol which ensures best-effort delivery. It is suitable for the applications which have little concern with flow or error control and requires to send the bulk of data like video conferencing. It is often used in multicasting protocols.
- **Multiplexing and 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 streams from various applications simultaneously over a network. The transport layer accepts these packets from different processes differentiated by their port numbers and passes them to the network layer after adding proper headers. Similarly, Demultiplexing is required at the receiver side to obtain the data coming from various processes. Transport receives the segments of data from the network layer and delivers it to the appropriate process running on the receiver's machine.
- **Congestion Control –** Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occur. As a result retransmission of packets from the sources increases the congestion further. In this situation, the Transport layer provides Congestion Control in different ways. It uses open loop congestion control to prevent the congestion and closed loop congestion control to remove the congestion in a network once it occurred. TCP provides AIMD- additive increase multiplicative decrease, leaky bucket technique for congestion control.
- **Data integrity and Error correction –** Transport layer checks for errors in the messages coming from application layer by using error detection codes, computing checksums, it checks whether the received data is not corrupted and uses the ACK and NACK services to inform the sender if the data has arrived or not and checks for the integrity of data.
- **Flow control –** The transport layer provides a flow control mechanism between the adjacent layers of the TCP/IP model. TCP also prevents data loss due to a fast sender and slow receiver by imposing some flow control techniques. It uses the method of sliding window protocol which is accomplished by the receiver by sending a window back to the sender informing the size of data it can receive.

User Datagram Protocol (UDP)
User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is unreliable and connectionless protocol. So, there is no need to establish connection prior to data transfer.

Though Transmission Control Protocol (TCP) is the dominant transport layer protocol used with most of Internet services; provides assured delivery, reliability and much more but all these services cost us with additional overhead and latency. Here, UDP comes into picture. For the realtime services like computer gaming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also save bandwidth.
User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

UDP Header –
UDP header is 8-bytes fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. First 8 Bytes contains all necessary header information and remaining part consist of data. UDP port number fields are each 16 bits long, therefore range for port numbers defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or process.



- **Source Port :** Source Port is 2 Byte long field used to identify port number of source.
- **Destination Port :** It is 2 Byte long field, used to identify the port of destined packet.
- **Length :** Length is the length of UDP including header and the data. It is 16-bits field.
- **Checksum :** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, pseudo header of information from the IP header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

Notes – Unlike TCP, Checksum calculation is not mandatory in UDP. No Error control or flow control is provided by UDP. Hence UDP depends on IP and ICMP for error reporting.

Applications of UDP:
- Used for simple request response communication when size of data is less and hence there is lesser concern about flow and error control.
- It is suitable protocol for multicasting as UDP supports packet switching.
- UDP is used for some routing update protocols like RIP(Routing Information Protocol).
- Normally used for real time applications which can not tolerate uneven delays between sections of a received message.

- Following implementations uses UDP as a transport layer protocol:
    1. NTP (Network Time Protocol)
    2. DNS (Domain Name Service)
    3. BOOTP, DHCP.
    4. NNP (Network News Protocol)
    5. Quote of the day protocol
    6. TFTP, RTSP, RIP, OSPF.
- Application layer can do some of the tasks through UDP-
    1. Trace Route
    2. Record Route
    3. Time stamp
- UDP takes datagram from Network Layer, attach its header and send it to the user. So, it works fast.
- Actually, UDP is null protocol if you remove checksum field.

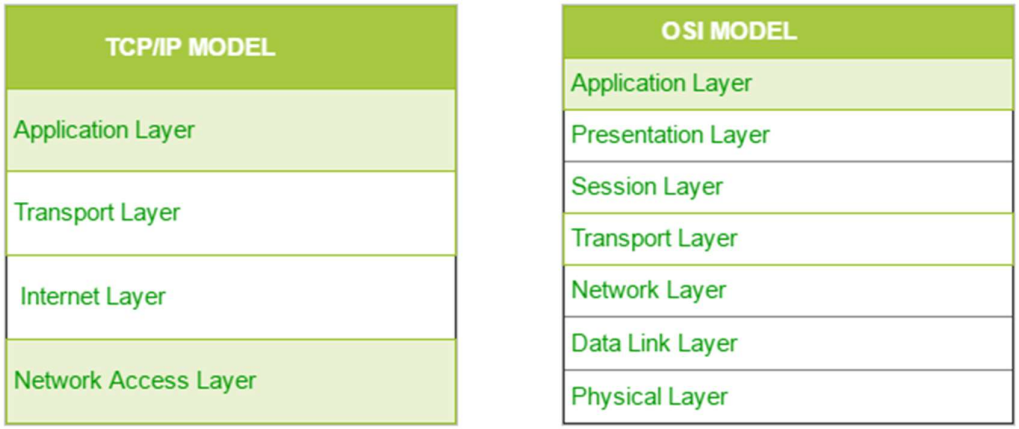
When to use UDP?

1. Reduce the requirement of computer resources.
2. When using the Multicast or Broadcast to transfer.
3. The transmission of Real-time packets, mainly in multimedia applications.

TCP

It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer



1. Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.

We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

2. Internet Layer –
This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

- **IP** – stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6.
  IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
- **ICMP** – stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
- **ARP** – stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

3. Host-to-Host Layer –
This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

- **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
- **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. Process Layer –
This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

- **HTTP and HTTPS** – HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
- **SSH** – SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.

- **NTP** – NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

Features

- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.

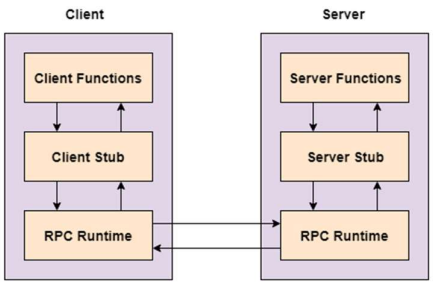
RPC

- A remote procedure call is an interprocess communication technique that is used for client-server based applications. It is also known as a subroutine call or a function call.
- A client has a request message that the RPC translates and sends to the server. This request may be a procedure or a function call to a remote server.
- When the server receives the request, it sends the required response back to the client. The client is blocked while the server is processing the call and only resumed execution after the server is finished.

The sequence of events in a remote procedure call are given as follows:

- The client stub is called by the client.
- The client stub makes a system call to send the message to the server and puts the parameters in the message.
- The message is sent from the client to the server by the client's operating system.
- The message is passed to the server stub by the server operating system.
- The parameters are removed from the message by the server stub.
- Then, the server procedure is called by the server stub.

A diagram that demonstrates this is as follows:



Advantages:

Remote procedure calls support process oriented and thread oriented models.

- The internal message passing mechanism of RPC is hidden from the user.

- The effort to re-write and re-develop the code is minimum in remote procedure calls.
- Remote procedure calls can be used in distributed environment as well as the local environment.
- Many of the protocol layers are omitted by RPC to improve performance.

Disadvantages:

- The remote procedure call is a concept that can be implemented in different ways. It is not a standard.
- There is no flexibility in RPC for hardware architecture. It is only interaction based.
- There is an increase in costs because of remote procedure call.

Congestion Control

- A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

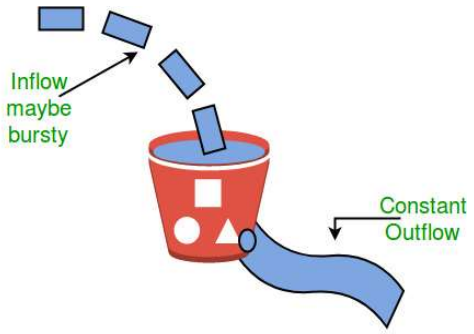
Effects of Congestion

- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

Congestion control algorithms

1. **Leaky Bucket Algorithm**

Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate. When the bucket is full with water additional water entering spills over the sides and is lost.



Similarly, each network interface contains a leaky bucket and the following steps are involved in leaky bucket algorithm:

- When host wants to send packet, packet is thrown into the bucket.
- The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
- Bursty traffic is converted to a uniform traffic by the leaky bucket.
- In practice the bucket is a finite queue that outputs at a finite rate.

2. **Token bucket Algorithm**

Need of token bucket Algorithm:

The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

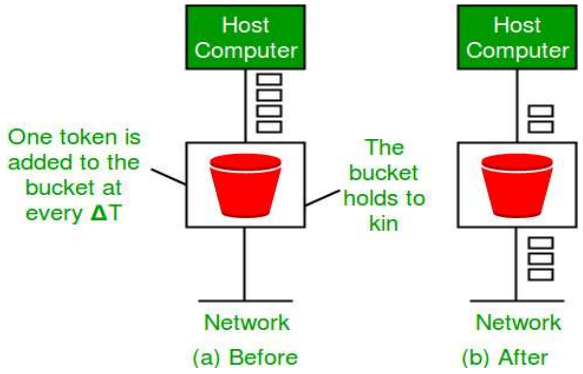
Steps of this algorithm can be described as follows:

1. In regular intervals tokens are thrown into the bucket. *f*
2. The bucket has a maximum capacity. *f*
3. If there is a ready packet, a token is removed from the bucket, and the packet is sent.
4. If there is no token in the bucket, the packet cannot be sent.

Let's understand with an example,
In figure (A) we see a bucket holding three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token. In figure (B) We see that three of the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.

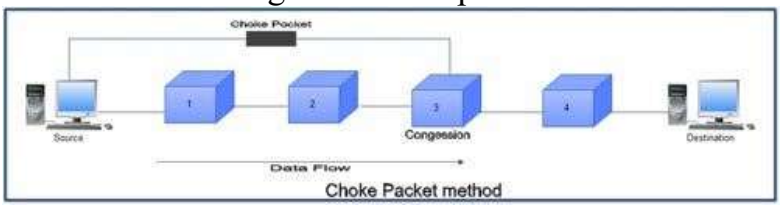
Ways in which token bucket is superior to leaky bucket:
The leaky bucket algorithm controls the rate at which the packets are introduced in the network, but it is very conservative in nature. Some flexibility is introduced in the token bucket algorithm. In the token bucket, algorithm tokens are generated at each tick (up to a certain limit). For an incoming packet to be transmitted, it must capture a token and the transmission takes place at the same rate. Hence some of the busty packets are transmitted at the same rate if tokens are available and thus introduces some amount of flexibility in the system.

Formula: M * s = C + ρ * s
where S – is time taken
M – Maximum output rate
ρ – Token arrival rate
C – Capacity of the token bucket in byte



Choke Packet

- In this method of congestion control, congested router or node sends a special type of packet called choke packet to the source to inform it about the congestion.
- Here, congested node does not inform its upstream node about the congestion as in backpressure method.
- In choke packet method, congested node sends a warning directly to the source station i.e. the intermediate nodes through which the packet has traveled are not warned.



Choke Packet Method

Implicit Signaling

- In implicit signaling, there is no communication between the congested node or nodes and the source.
- The source guesses that there is congestion somewhere in the network when it does not receive any acknowledgment. Therefore the delay in receiving an acknowledgment is interpreted as congestion in the network.
- On sensing this congestion, the source slows down.
- This type of congestion control policy is used by TCP.

Explicit Signaling

- In this method, the congested nodes explicitly send a signal to the source or destination to inform about the congestion.
- Explicit signaling is different from the choke packet method. In choke packed method, a separate packet is used for this purpose whereas in explicit signaling method, the signal is included in the packets that carry data .
- Explicit signaling can occur in either the forward direction or the backward direction .
- In backward signaling, a bit is set in a packet moving in the direction opposite to the congestion. This bit warns the source about the congestion and informs the source to slow down.
- In forward signaling, a bit is set in a packet moving in the direction of congestion. This bit warns the destination about the congestion. The receiver in this case uses policies such as slowing down the acknowledgements to remove the congestion.

Quality of Service (QoS)

Quality-of-Service (QoS) refers to traffic control mechanisms that seek to either differentiate performance based on application or network-operator requirements or provide predictable or guaranteed performance to applications, sessions or traffic aggregates. Basic phenomenon for QoS means in terms of packet delay and losses of various kinds.

Need for QoS –

- Video and audio conferencing require bounded delay and loss rate.
- Video and audio streaming requires bounded packet loss rate, it may not be so sensitive to delay.
- Time-critical applications (real-time control) in which bounded delay is considered to be an important factor.
- Valuable applications should be provided better services than less valuable applications.

QoS Specification –

QoS requirements can be specified as:

- Delay
- Delay Variation(Jitter)
- Throughput
- Error Rate

There are two types of QoS Solutions:

- **Stateless Solutions –** Routers maintain no fine grained state about traffic, one positive factor of it is that it is scalable and robust. But it has weak services as there is no guarantee about kind of delay or performance in a particular application which we have to encounter.
- **Stateful Solutions –** Routers maintain per flow state as flow is very important in providing the Quality-of-Service i.e. providing powerful services such as guaranteed services and high resource utilization, provides protection and is much less scalable and robust.

APPLICATION LAYER

DNS

- The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.
- It associates various information with domain names assigned to each of the participating entities.
- Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols.
- By providing a worldwide, distributed directory service, the Domain Name System has been an essential component of the functionality of the Internet since 1985.
- The Domain Name System delegates the responsibility of assigning domain names and mapping those names to Internet resources by designating authoritative name servers for each domain.
- It serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses.

There are 4 DNS servers involved in loading a webpage:

- **DNS recursor** - The recursor can be thought of as a librarian who is asked to go find a particular book somewhere in a library. The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers. Typically the recursor is then responsible for making additional requests in order to satisfy the client's DNS query.
- **Root nameserver** - The root server is the first step in translating (resolving) human readable host names into IP addresses. It can be thought of like an index in a library that points to different racks of books - typically it serves as a reference to other more specific locations.
- **TLD nameserver** - The top level domain server (TLD) can be thought of as a specific rack of books in a library. This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is "com").
- **Authoritative nameserver** - This final nameserver can be thought of as a dictionary on a rack of books, in which a specific name can be translated into its definition. The authoritative nameserver is the last stop in the nameserver query. If the authoritative

name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor (the librarian) that made the initial request.

Simple Mail Transfer Protocol (SMTP)

Email is emerging as one of the most valuable services on the internet today. Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver's side.

SMTP Fundamentals

SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port. After successfully establishing the TCP connection the client process sends the mail instantly.

SMTP Protocol

The SMTP model is of two type :

- End-to- end method
- Store-and- forward method

The end to end model is used to communicate between different organizations whereas the store and forward method are used within an organization. A SMTP client who wants to send the mail will contact the destination's host SMTP directly in order to send the mail to the destination. The SMTP server will keep the mail to itself until it is successfully copied to the receiver's SMTP.

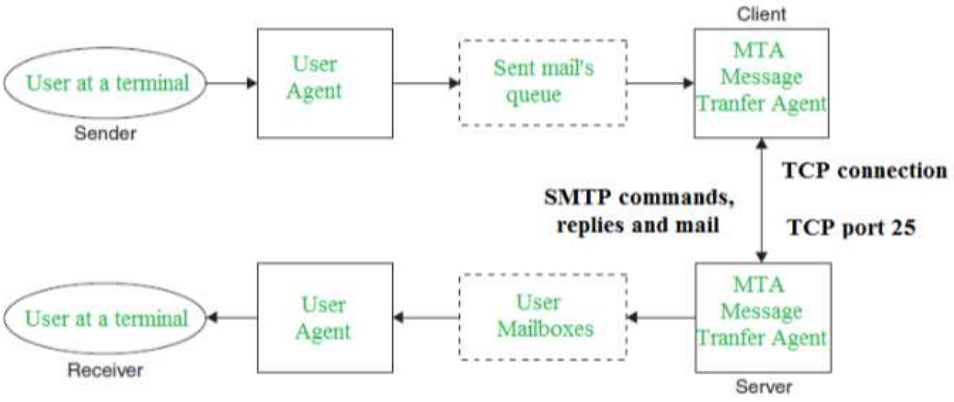
The client SMTP is the one which initiates the session let us call it as the client- SMTP and the server SMTP is the one which responds to the session request and let us call it as receiver-SMTP. The client- SMTP will start the session and the receiver-SMTP will respond to the request.

Model of SMTP system

In the SMTP model user deals with the user agent (UA) for example Microsoft Outlook, Netscape, Mozilla, etc. In order to exchange the mail using TCP, MTA is used. The users sending the mail do not have to deal with the MTA it is the responsibility of the system admin to set up the local MTA. The MTA maintains a small queue of mails so that it can schedule repeat delivery of mail in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents.

Both the SMTP-client and MSTP-server should have 2 components:

- User agent (UA)
- Local MTA



Communication between sender and the receiver :
The senders, user agent prepare the message and send it to the MTA. The MTA functioning is to transfer the mail across the network to the receivers MTA. To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.

SENDING EMAIL:
Mail is sent by a series of request and response messages between the client and a server. The message which is sent across consists of a header and the body. A null line is used to terminate the mail header. Everything which is after the null line is considered as the body of the message which is a sequence of ASCII characters. The message body contains the actual information read by the receipt.

RECEIVING EMAIL:
The user agent at the server side checks the mailboxes at a particular time of intervals. If any information is received it informs the user about the mail. When the user tries to read the mail it displays a list of mails with a short description of each mail in the mailbox. By selecting any of the mail user can view its contents on the terminal.

Some SMTP Commands:

- **HELO** – Identifies the client to the server, fully qualified domain name, only sent once per session
- **MAIL** – Initiate a message transfer, fully qualified domain of originator
- **RCPT** – Follows MAIL, identifies an addressee, typically the fully qualified name of the addressee and for multiple addressees use one RCPT for each addressee
- **DATA** – send data line by line

Simple Network Management Protocol (SNMP)
If an organization has 1000 of devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used.
SNMP is an application layer protocol which uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults and sometimes even used to configure remote devices.

SNMP components –
There are 3 components of SNMP:

- **SNMP Manager** – It is a centralised system used to monitor network.It is also known as Network Management Station (NMS)
- **SNMP agent** – It is a software management software module installed on a managed device. Managed devices can be network devices like PC, router, switches, servers etc.
- **Management Information Base** – MIB consists of information of resources that are to be managed. These information is organised hierarchically. It consists of objects instances which are essentially variables.

SNMP messages –
Different variables are:

- **GetRequest** – SNMP manager sends this message to request data from SNMP agent. It is simply used to retrieve data from SNMP agent. In response to this, SNMP agent responds with requested value through response message.
- **GetNextRequest** – This message can be sent to discover what data is available on a SNMP agent. The SNMP manager can request for data continuously until no more data is left. In this way, SNMP manager can take knowledge of all the available data on SNMP agent.
- **GetBulkRequest** – This message is used to retrieve large data at once by the SNMP manager from SNMP agent. It is introduced in SNMPv2c.
- **SetRequest** – It is used by SNMP manager to set the value of an object instance on the SNMP agent.
- **Response** – It is a message send from agent upon a request from manager. When sent in response to Get messages, it will contain the data requested. When sent in response to Set message, it will contain the newly set value as confirmation that the value has been set.
- **Trap** – These are the message send by the agent without being requested by the manager. It is sent when a fault has occurred.
- **InformRequest** – It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to set trap continuously until it receives an Inform message. It is same as trap but adds an acknowledgement that trap doesn't provide.

SNMP security levels –
It defines the type of security algorithm performed on SNMP packets. These are used in only SNMPv3. There are 3 security levels namely:

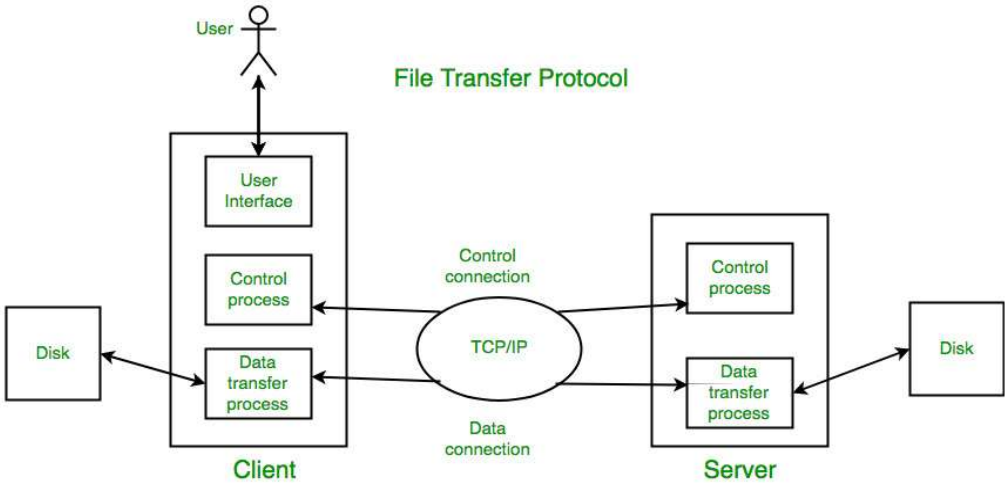
- **noAuthNoPriv** – This (no authentication, no privacy) security level uses community string for authentication and no encryption for privacy.
- **authNopriv** – This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.
- **authPriv** – This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses DES-56 algorithm.

SNMP versions –
There are 3 versions of SNMP:

- **SNMPv1** – It uses community strings for authentication and use UDP only.
- **SNMPv2c** – It uses community strings for authentication. It uses UDP but can be configured to use TCP.
- **SNMPv3** – It uses Hash based MAC with MD5 or SHA for authentication and DES-56 for privacy.This version uses TCP. Therefore, conclusion is the higher the version of SNMP, more secure it will be.

FTP

- File Transfer Protocol(FTP) is an application layer protocol which moves files between local and remote file systems. It runs on the top of TCP, like HTTP. To transfer a file, 2 TCP connections are used by FTP in parallel: control connection and data connection.
- It can be invoked from the command prompt or some graphical user interface.
- It also allows to update (delete, rename, move and copy) files at a server.
- It uses a reserved port no. 21



Control connection:
For sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files, etc., FTP makes use of control connection. The control connection is initiated on port number 21.

Data connection:
For sending the actual file, FTP makes use of data connection. A data connection is initiated on port number 20.
FTP sends the control information out-of-band as it uses a separate control connection. Some protocols send their request and response header lines and the data in the same TCP connection. For this reason, they are said to send their control information in-band. HTTP and SMTP are such examples.

FTP Operations

- **USER** – This command sends the user identification to the server.
- **PASS** – This command sends the user password to the server.
- **CWD** – This command allows the user to work with a different directory or dataset for file storage or retrieval without altering his login or accounting information.
- **RMD** – This command causes the directory specified in the path-name to be removed as a directory.
- **MKD** – This command causes the directory specified in the pathname to be created as a directory.
- **PWD** – This command causes the name of the current working directory to be returned in the reply.
- **RETR** – This command causes the remote host to initiate a data connection and to send the requested file over the data connection.
- **STOR** – This command causes to store a file into the current directory of the remote host.
- **LIST** – Sends a request to display the list of all the files present in the directory.
- **ABOR** – This command tells the server to abort the previous FTP service command and any associated transfer of data.
- **QUIT** – This command terminates a USER and if file transfer is not in progress, the server closes the control connection.

FTP Session:

When a FTP session is started between a client and a server, the client initiates a control TCP connection with the server side. The client sends control information over this. When the server receives this, it initiates a data connection to the client side. Only one file can be sent over one data connection. But the control connection remains active throughout the user session. As we know HTTP is stateless i.e. it does not have to keep track of any user state. But FTP needs to maintain a state about its user throughout the session.

FTP allows three types of data structures :

- **File Structure** – In file-structure there is no internal structure and the file is considered to be a continuous sequence of data bytes.
- **Record Structure** – In record-structure the file is made up of sequential records.
- **Page Structure** – In page-structure the file is made up of independent indexed pages.

HTTP

- It is used to access the data on the World Wide Web (WWW).
- The function of HTTP is the combination of FTP and SMTP.
- HTTP is similar to FTP, because it uses only one TCP connection, i.e., data is data is transferred between client and server.
- In SMTP, the messages are stored and forwarded to the destination but HTTP messages are delivered immediately.
- HTTP uses the services of TCP on well known port no. 80.

Difference between HTTP, FTP and SMTP

Parameter	HTTP	FTP	SMTP
Port number	80	20 and 21	25
Type of band transfer	In-band	Out-of-band	In-band
State	Stateless	Maintains state	–
Number of TCP connections	1	2 (Data Connection and Control Connection)	1
Type of TCP connection	Can use both Persistent and Non-persistent	Persistent for Control connection. Non-persistent for Data Connection	Persistent
Type of Protocol	Pull Protocol (Mainly)	–	Push Protocol (Primarily)
Type of Transfer	Transfer files between Web server and Web client	Transfer directly between computers	Transfers mails via Mail Servers

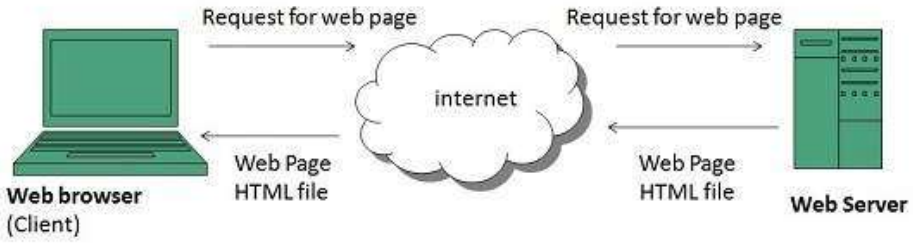
World Wide Web (WWW)

- WWW stands for World Wide Web. A technical definition of the World Wide Web is : all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP).
- A broader definition comes from the organization that Web inventor Tim Berners-Lee helped found, the World Wide Web Consortium (W3C).
- The World Wide Web is the universe of network-accessible information, an embodiment of human knowledge.
- In simple terms, The World Wide Web is a way of exchanging information between computers on the Internet, tying them together into a vast collection of interactive multimedia resources.

WWW Operation

WWW works on client- server approach. Following steps explains how the web works:

- User enters the URL (say, http://www.tutorialspoint.com) of the web page in the address bar of web browser.
- Then browser requests the Domain Name Server for the IP address corresponding to www.tutorialspoint.com.
- After receiving IP address, browser sends the request for web page to the web server using HTTP protocol which specifies the way the browser and web server communicates.
- Then web server receives request using HTTP protocol and checks its search for the requested web page. If found it returns it back to the web browser and close the HTTP connection.
- Now the web browser receives the web page, It interprets it and display the contents of web page in web browser's window.



Firewalls

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

- **Accept:** allow the traffic
- **Reject:** block the traffic but reply with an "unreachable error"
- **Drop:** block the traffic with no reply

How Firewall Works

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.

From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.

Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses type code instead of port number which identifies purpose of that packet.

Types of Firewall

Firewalls are generally of two types: Host-based and Network-based.

- **Host- based Firewalls:** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
- **Network-based Firewalls:** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Bluetooth

- Bluetooth is an open wireless technology standard for transmitting fixed and mobile electronic device data over short distances.
- Bluetooth was introduced in 1994 as a wireless substitute for RS-232 cables.
- Bluetooth communicates with a variety of electronic devices and creates personal networks operating within the unlicensed 2.4 GHz band.
- Operating range is based on device class.
- A variety of digital devices use Bluetooth, including MP3 players, mobile and peripheral devices and personal computers.
- In contrast to other wireless technologies, Bluetooth equips its network and devices with high-level services like file pushing, voice transmission and serial line emulation.

Bluetooth is used for the following:

- Wireless control and communication between mobile and hands-free headsets
- Wireless networking between multiple computers in areas with limited service
- Wireless communication with PCs and peripheral input/output (I/O) devices
- With Object Exchange (OBEX), to transfer files, contact details and calendar appointments between multiple devices
- To replace conventional wired communication, like GPS receivers, medical equipment, traffic control devices and bar code scanners
- For low-bandwidth applications, when a higher USB bandwidth is not desired
- Bridge multiple industrial Ethernet networks

E-Mail

- Electronic mail (email) is a digital mechanism for exchanging messages through Internet or intranet communication platforms.
- Email messages are relayed through email servers, which are provided by all Internet service providers (ISP).
- Emails are transmitted between two dedicated server folders: sender and recipient. A sender saves, sends or forwards email messages, whereas a recipient reads or downloads emails by accessing an email server.

Email messages are comprised of three components, as follows:

- **Message envelope:** Describes the email's electronic format
- **Message header:** Includes sender/recipient information and email subject line
- **Message body:** Includes text, image and file attachments

S/MIME

- Secure MIME (S/MIME) is an Internet standard for digitally signing MIME-based email data and its public key encryption.
- It was initially developed by RSA Security, Inc. and is based on the company's public key encryption mechanism.
- Most email services and software use S/MIME to secure email communication.

- S/MIME enables email security features by providing encryption, authentication, message integrity and other related services.
- It ensures that an email message is sent by a legitimate sender and provides encryption for incoming and outgoing messages.
- To enable S/MIME based communication, the sender and receiver must be integrated with public key and signatures issued from a certificate authority (CA).
- A digital signature is used to validate a sender's identity, whereas a public key provides encryption and decryption services.

IMAP

- Internet Message Access Protocol (IMAP) is a standard protocol for accessing email on a remote server from a local client.
- IMAP is an application layer Internet Protocol using the underlying transport layer protocols to establish host-to-host communication services for applications.
- This allows the use of a remote mail server. The well-known port address for IMAP is 143.
- The IMAP architecture enables users to send and receive emails through a remote server, without support from a particular device.
- This type of email access is ideal for travelers receiving or answering emails from their home desktop or office computer.
- This term is also known as interactive mail access protocol, Internet mail access protocol, and interim mail access protocol
- With IMAP, all emails remain on the server until the client deletes them. IMAP also permits multiple clients to access and control the same mailbox.
- Some of IMAP benefits include the ability to delete messages, search for keywords in the body of emails, create and manage multiple mailboxes or folders, and view the headings for easy visual scans of emails.
- IMAP is still used extensively, but is less important now that so much email is sent via web-based interfaces such as Gmail, Hotmail, Yahoo Mail, etc.

Cryptography

- Cryptography involves creating written or generated codes that allow information to be kept secret.
- Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data.
- Information security uses cryptography on several levels.
- The information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored.
- Cryptography also aids in nonrepudiation. This means that the sender and the delivery of a message can be verified.
- Cryptography is also known as cryptology.

Cryptography also allows senders and receivers to authenticate each other through the use of key pairs. There are various types of algorithms for encryption, some common algorithms include:

- **Secret Key Cryptography (SKC):** Here only one key is used for both encryption and decryption. This type of encryption is also referred to as symmetric encryption.
- **Public Key Cryptography (PKC):** Here two keys are used. This type of encryption is also called asymmetric encryption. One key is the public key that anyone can access. The other key is the private key, and only the owner can access it. The sender encrypts the information using the receiver's public key. The receiver decrypts the message using his/her private key. For nonrepudiation, the sender encrypts plain text using a private key, while the receiver uses the sender's public key to decrypt it. Thus, the receiver knows who sent it.
- **Hash Functions:** These are different from SKC and PKC. They use no key and are also called one-way encryption. Hash functions are mainly used to ensure that a file has remained unchanged.

Authentication

- In the context of computer systems, authentication is a process that ensures and confirms a user's identity.
- Authentication is one of the five pillars of information assurance (IA).
- The other four are integrity, availability, confidentiality and nonrepudiation.
- Authentication begins when a user tries to access information.
- First, the user must prove his access rights and identity. When logging into a computer, users commonly enter usernames and passwords for authentication purposes.
- This login combination, which must be assigned to each user, authenticates access. However, this type of authentication can be circumvented by hackers.
- A better form of authentication, biometrics, depends on the user's presence and biological makeup (i.e., retina or fingerprints). This technology makes it more difficult for hackers to break into computer systems.
- The Public Key Infrastructure (PKI) authentication method uses digital certificates to prove a user's identity.
- There are other authentication tools, too, such as key cards and USB tokens. One of the greatest authentication threats occurs with email, where authenticity is often difficult to verify. For example, unsecured emails often appear legitimate.

Security protocols

- Network security protocols are a type network protocol that ensures the security and integrity of data in transit over a network connection.
- Network security protocols define the processes and methodology to secure network data from any illegitimate attempt to review or extract the contents of data.
- Network security protocols are primarily designed to prevent any unauthorized user, application, service or device from accessing network data. This applies to virtually all data types regardless of the network medium used.

- Network security protocols generally implement cryptography and encryption techniques to secure the data so that it can only be decrypted with a special algorithm, logical key, mathematical formula and/or a combination of all of them.
- Some of the popular network security protocols include Secure File Transfer Protocol (SFTP), Secure Hypertext Transfer Protocol (HTTPS) and Secure Socket Layer (SSL).

Public Key Encryption

When the two parties communicate to each other to transfer the intelligible or sensible message, referred to as plaintext, is converted into apparently random nonsense for security purpose referred to as ciphertext.

The process of changing the plaintext into the ciphertext is referred to as encryption.

The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext.

Once the ciphertext is produced, it may be transmitted.

The security of conventional encryption depends on the major two factors:

- The Encryption algorithm
- Secrecy of the key

The algorithm will produce a different output depending on the specific key being used at the time. Changing the key changes the output of the algorithm.

Once the ciphertext is produced, it may be transmitted. Upon reception, the ciphertext can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption.

Decryption:

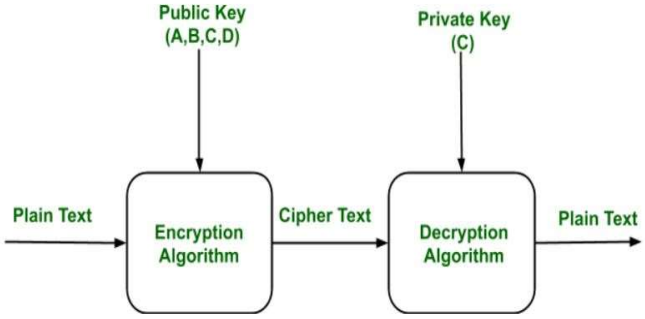
The process of changing the ciphertext to the plaintext that process is known as decryption.

Asymmetric is a form of Cryptosystem in which encryption and decryption are performed using different keys-Public key (known to everyone) and Private key (Secret key). This is known as Public Key Encryption.

Characteristics:

- Public key Encryption is important because it is infeasible to determine the decryption key given only the knowledge of the cryptographic algorithm and encryption key.
- Either of the two key (Public and Private key) can be used for encryption with other key used for decryption.
- Due to Public key cryptosystem, public keys can be freely shared, allowing users an easy and convenient method for encrypting content and verifying digital signatures, and private keys can be kept secret, ensuring only the owners of the private keys can decrypt content and create digital signatures.
- The most widely used public-key cryptosystem is RSA (Rivest–Shamir–Adleman). The difficulty of finding the prime factors of a composite number is the backbone of RSA.

Example:
Public keys of every user are present in the Public key Register. If B wants to send a confidential message to C, then B encrypt the message using C Public key. When C receives the message from B then C can decrypt it using its own Private key. No other recipient other than C can decrypt the message because only C know C's private key.



Components of Public Key Encryption:

- **Plain Text:** This is the message which is readable or understandable. This message is given to the Encryption algorithm as an input.
- **Cipher Text:** The cipher text is produced as an output of Encryption algorithm. We cannot simply understand this message.
- **Encryption Algorithm:** The encryption algorithm is used to convert plain text into cipher text.
- **Decryption Algorithm:** It accepts the cipher text as input and the matching key (Private Key or Public key) and produces the original plain text
- **Public and Private Key:** One key either Private key (Secret key) or Public Key (known to everyone) is used for encryption and other is used for decryption

Weakness:

- Public key Encryption is vulnerable to Brute-force attack.
- This algorithm also fails when the user lost his private key, then the Public key Encryption becomes the most vulnerable algorithm.
- Public Key Encryption also is weak towards man in the middle attack. In this attack a third party can disrupt the public key communication and then modify the public keys.
- If user private key used for certificate creation higher in the PKI(Public Key Infrastructure) server hierarchy is compromised, or accidentally disclosed, then a "man-in-the-middle attack" is also possible, making any subordinate certificate wholly insecure. This is also the weakness of Public key Encryption.

Applications:

- Confidentiality can be achieved using Public Key Encryption. In this the Plain text is encrypted using receiver public key. This will ensures that no one other than receiver private key can decrypt the cipher text.
- Digital signature is for senders authentication purpose. In this sender encrypt the plain text using his own private key. This step will make sure the authentication of the sender because receiver can decrypt the cipher text using senders pubic key only.
- This algorithm can use in both Key-management and securely transmission of data.

Digital Signature

- A digital signature guarantees the authenticity of an electronic document or message in digital communication and uses encryption techniques to provide proof of original and unmodified documentation.
- Digital signatures are used in e-commerce, software distribution, financial transactions and other situations that rely on forgery or tampering detection techniques.
- A digital signature is also known as an electronic signature.

A digital signature is applied and verified, as follows:

- The document or message sender (signer) or public/private key supplier shares the public key with the end user(s).
- The sender, using his private key, appends the encrypted signature to the message or document.
- The end user decrypts the document and verifies the signature, which lets the end user know that the document is from the original sender.