Data communication

Unit-01

Introduction to computer network

A computer network is a collection of computing devices that are connected with each other for the purpose of information and resource sharing among a wide variety of users.

Each device in the network is called a node which is connected to other nodes through wired or wireless media.

The features of a computer network are −

- **Sharing** − Computer networks enable sharing of files, software, hardware resources and computing capabilities.
- **Speed:** The communication speed among the components is fast enough to be comparable with a centralized system.
- **Scalability** − Sizes of computer networks dynamically increase with time. The networks have to be scalable so that they can evolve adequately for future deployments.
- **Integration** − All the components of the network work in a coordinated manner for a seamless user experience.
- **Security** − Networks allow security and access rights to the users for restricted sharing of resources and information.
- **Cost Effectiveness** − Networking reduces the deployment cost of hardware and software of a centralized system.

Characteristics of a Computer Network

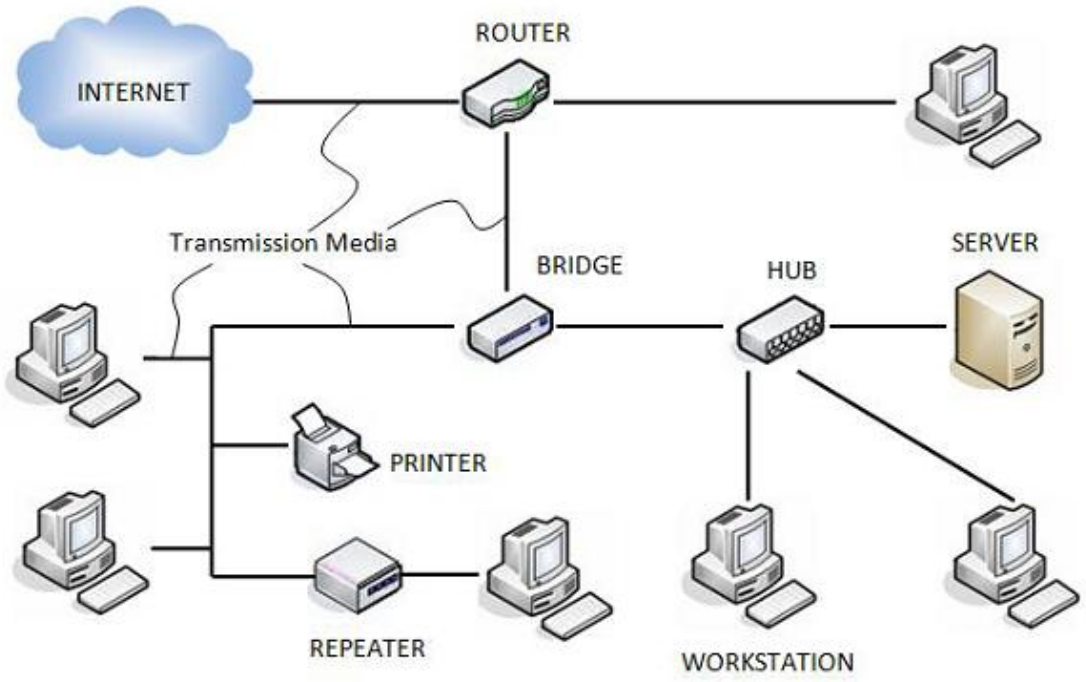
- Share resources from one computer to another.
- Create files and store them in one computer, access those files from the other computer(s) connected over the network.

- Connect a printer, scanner, or a fax machine to one computer within the network and let other computers of the network use the machines available over the network.

Computer networks components

Computer networks components comprise both physical parts as well as the software required for installing computer networks, both at organizations and at home. The hardware components are the server, client, peer, transmission medium, and connecting devices. The software components are operating system and protocols.

The following figure shows a network along with its components −



COMPUTER NETWORK COMPONENTS

Hardware Components

- **Servers** −Servers are high-configuration computers that manage the resources of the network. The network operating system is typically installed in the server and so they give user accesses to the network resources. Servers can be of various kinds: file servers, database servers, print servers etc.
- **Clients** − Clients are computers that request and receive service from the servers to access and use the network resources.
- **Peers** − Peers are computers that provide as well as receive services from other peers in a workgroup network.

- **Transmission Media** − Transmission media are the channels through which data is transferred from one device to another in a network. Transmission media may be guided media like coaxial cable, fibre optic cables etc; or maybe unguided media like microwaves, infra-red waves etc.
- **Connecting Devices** − Connecting devices act as middleware between networks or computers, by binding the network media together. Some of the common connecting devices are:
  a. Routers
  b. Bridges
  c. Hubs
  d. Repeaters
  e. Gateways
  f. Switches

Software Components

- **Networking Operating System** − Network Operating Systems is typically installed in the server and facilitate workstations in a network to share files, database, applications, printers etc.
- **Protocol Suite** − A protocol is a rule or guideline followed by each computer for data communication. Protocol suite is a set of related protocols that are laid down for computer networks. The two popular protocol suites are −
  - a. OSI Model (Open System Interconnections)
  - b. TCP / IP Model

Types of computer network

- **LAN - Local Area Network**
- A Local Area Network (LAN) is a private network that connects computers and devices within a limited area like a residence, an office, a building or a campus. On a small scale, LANs are used to connect personal computers to printers. However, LANs can also extend to a few kilometers when used by companies, where a large number of computers share a variety of resources like hardware (e.g. printers, scanners, audiovisual devices etc), software (e.g. application programs) and data.
- **MAN - Metropolitan Area Network**

- A Metropolitan Area Network (MAN) is a larger network than LAN. It often covers multiple cities or towns. It is quiet expensive and a single organization may not have own it.

WAN - Wide Area Network

- A Wide Area Network (WAN) is a much larger network than LAN and MAN. It often covers multiple contries or contenants. It is quiet expensive and a single organization may not have own it. Satellite is used to manage WAN.
- Following are the important differences between LAN, MAN and WAN.

Sr. No.	Key	LAN	MAN	WAN
1	Definition	LAN stands for Local Area Network.	MAN stands for Metropolitan Area Network.	WAN stands for Wide Area Network.
2	Ownership	LAN is often owned by private organizations.	MAN ownership can be private or public.	WAN ownership can be private or public.
3	Speed	LAN speed is quiet high.	MAN speed is average.	WAN speed is lower than that of LAN.
4	Delay	Network Propagation Delay is short in LAN.	Network Propagation Delay is moderate in MAN.	Network Propagation Delay is longer in WAN.
5	Congestion	LAN has low congestion as compared to WAN.	MAN has higher congestion than LAN.	WAN has higher congestion than both MAN and LAN.
6	Fault Tolerance	Fault Tolerance of LAN is higher than WAN.	Fault Tolerance of MAN is lower than LAN.	Fault Tolerance of WAN is lower than both LAN and MAN.
7	Maintenance	Designing and maintaining LAN is	Designing and maintaining WAN is	Designing and maintaining WAN is complex and more

Sr. No.	Key	LAN	MAN	WAN
		easy and less costly than WAN.	complex and more costly than LAN.	costly than both LAN and MAN.

Wired Network –

In the networking world, "**Wired**" as the name suggests refers to any physical medium connected through wires and cables. The wires/cables can be copper wire, twisted pair or even fibre optic. Wired connectivity is responsible for providing high security with high Bandwidth provisioned for each user.
In fact, Wired connectivity is considered highly reliable and incurs very low delay, unlike Wireless connectivity.

Wireless Network –

"**Wireless**" as the term refers, uses air as a medium to send electromagnetic waves or infrared waves. Wireless devices have antennas for communication. Wireless connectivity provides a major benefit of user mobility and ease of deployment. Wireless becomes more useful in areas where Wires can't be reached.

What is Difference b/w Wired & Wireless Network?

The following table denotes & explain the difference in both wired and wireless network –

PARAMETER	WIRED	WIRELESS
Communication Medium	Copper, Fiber etc.	Air
Standard	IEEE 802.3	802.11 family
Mobility and Roaming	Limited	Higher
Security	High	Lower than Wired. Also easy to hack
Speed / Bandwidth	High Speed upto 1 Gbps	Lower speed than Wired Network.
Access to Network	Physical Access Required	Proximity Required
Delay	Low	High
Reliability	High	Lower than Wired

PARAMETER	WIRED	WIRELESS
Flexibility to change	Less flexible to changes	More flexible configuration
Working principle	CSMA/CD, operates by detecting the occurrence of a collision.	CSMA/CA , hence reduces possibility of collision be avoiding collision from happening
Interference and Fluctuations vulnerability	Very Less	High
Installation activity	Cumbersome and manpower intensive	Less labor intensive and easy
Installation Time	Takes longer time to perform	Very less deployment time
Dedicated / Shared Connection	Dedicated	Shared
Installation Cost	High	Low
Maintenance (Upgrade) cost	High	Low
Related equipment	Router, Switch , Hub	Wireless Router, Access Point
Benefits	* Greater Speed * Higher noise immunity * Highly reliable * Greater Security	* No Hassles of Cable * Best for mobile devices * Greater mobility * Easy installation and management

Network Software & Network Standardization

Design Issues for the Layers of Computer Networks

A number of design issues exist for the layer to layer approach of computer networks. Some of the main design issues are as follows −

Reliability

Network channels and components may be unreliable, resulting in loss of bits while data transfer. So, an important design issue is to make sure that the information transferred is not distorted.

Scalability

Networks are continuously evolving. The sizes are continually increasing leading to congestion. Also, when new technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

Addressing

At a particular time, innumerable messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that each layer can identify the sender and receivers of each message.

Error Control

Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

Flow Control

If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.

Resource Allocation

Computer networks provide services in the form of network resources to the end users. The main design issue is to allocate and deallocate resources to processes. The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

Statistical Multiplexing

It is not feasible to allocate a dedicated path for each message while it is being transferred from the source to the destination. So, the data channel needs to be multiplexed, so as to allocate a fraction of the bandwidth or time to each host.

Routing

There may be multiple paths from the source to the destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time. There are several routing algorithms that are used in network systems.

Security

A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

Protocol Hierarchies in Computer Network

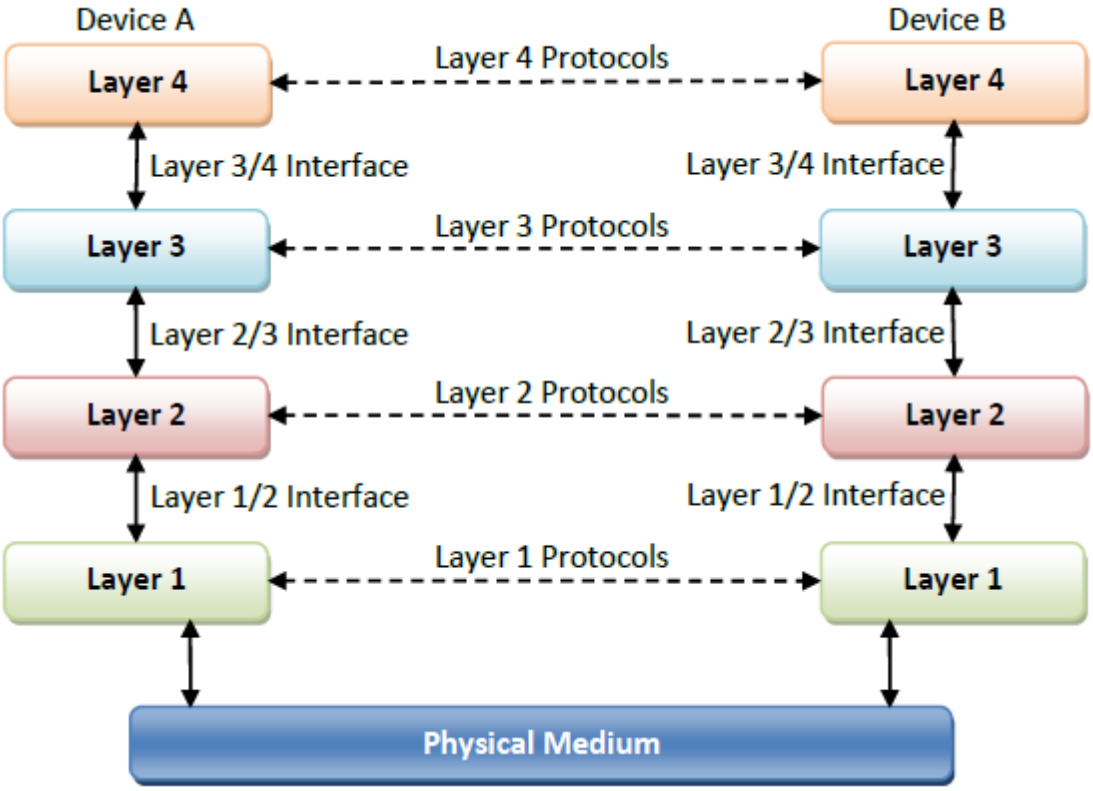
A **protocol** is simply defined as a set of rules and regulations for data communication. Rules are basically defined for each and every step and process at time of communication among two or more computers. Networks are needed to follow these protocols to transmit data successfully. All protocols might be implemented using hardware, software, or combination of both of them. There are three aspects of protocols given below :

- **Syntax –**
  It is used to explain data format that is needed to be sent or received.
- **Semantics –**
  It is used to explain exact meaning of each of sections of bits that are usually transferred.
- **Timings –**
  It is used to explain exact time at which data is generally transferred along with speed at which it is transferred

Protocol Hierarchies

Most networks are organized as a stack of layers, one on the top of another. The number of layers and their names vary from network to network. Each layer has a specified function and adheres to specified protocols. Thus we obtain a stack of protocols.

The following figure illustrates a four-layer network −

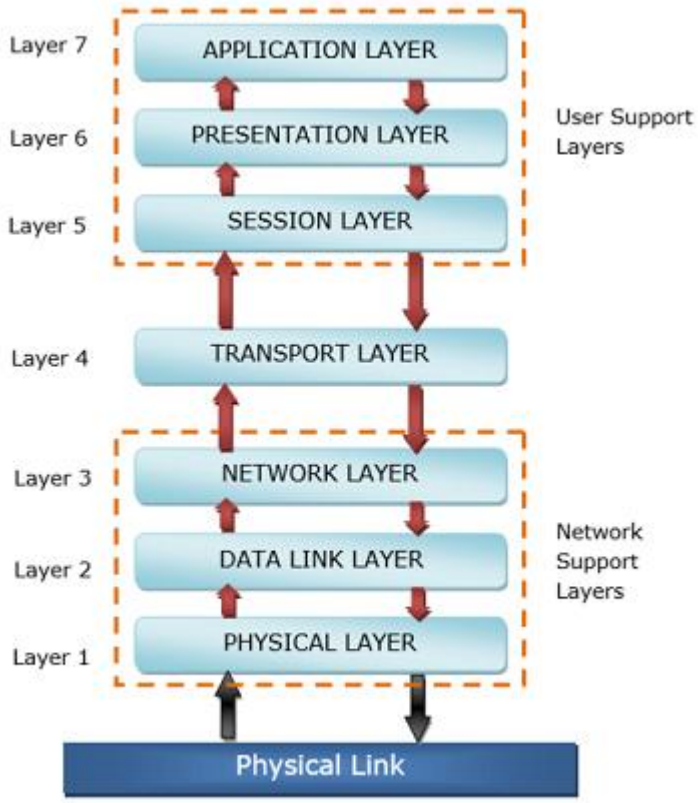


The above figure represents communication between Device A and Device B. The data stream from one device to the other is not sent directly but has to pass through a number of layers. The layers in the same levels are called peers and have a set of protocols for communication. Between each adjacent layer is an interface that defines the services that are being offered by a lower layer to the next higher layer. The dotted arrows depict virtual communication between peer layers, while the solid arrows represent the physical communications between the adjacent layers.

Let us consider a situation where Device A wants to send a message to Device B. Device A passes its information to the highest layer. As soon as a data stream reaches a layer, it performs some specified functions on it and passes it to the layer below. This continues until the data stream reaches the lowest layer. Layer 1 passes a bit stream of 0s and 1s to the physical medium that communicates it to the Layer 1 of the receiving end. Each layer in the receiving end performs certain functions on the data stream adhering to the protocol with its peer and passes it to the layer above. This continues until the information reaches the highest layer. The highest layer then conveys the message to Device B in the same format sent by Device A.

OSI Reference Model

OSI or Open System Interconnection model was developed by International Standards Organization (ISO). It gives a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. It has seven interconnected layers. The seven layers of the OSI Model are a physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer, as shown in the following diagram −



The physical layer, data link layer and the network layer are the network support layers. The layers manage a physical transfer of data from one device to another. Session layer, presentation layer, and application layer are the user support layers. These layers allow communication among unrelated software in dissimilar environments. Transport layer links the two groups.

The main functions of each of the layers are as follows −

- **Physical Layer −** Its function is to transmit individual bits from one node to another over a physical medium.
- **Data Link Layer −** It is responsible for the reliable transfer of data frames from one node to another connected by the physical layer.
- **Network Layer −** It manages the delivery of individual data packets from source to destination through appropriate addressing and routing.

- **Transport Layer −**It is responsible for delivery of the entire message from the source host to destination host.
- **Session Layer −** It establishes sessions between users and offers services like dialog control and synchronization.
- **Presentation Layer −** It monitors syntax and semantics of transmitted information through translation, compression, and encryption.
- **Application Layer −** It provides high-level APIs (application program interface) to the users.

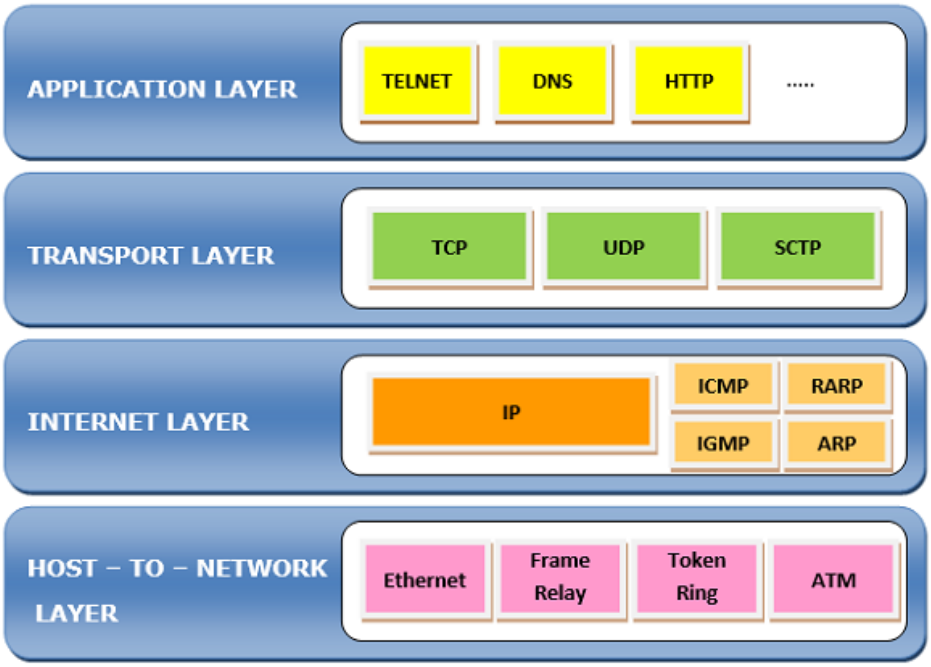
TCP/IP Reference Model

TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defence) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol.

The four layers in the TCP/IP protocol suite are −

- **Host-to- Network Layer −**It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols.
- **Internet Layer −**It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.
- **Transport Layer −** It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- **Application Layer −** This is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.

The following diagram shows the layers and the protocols in each of the layers −



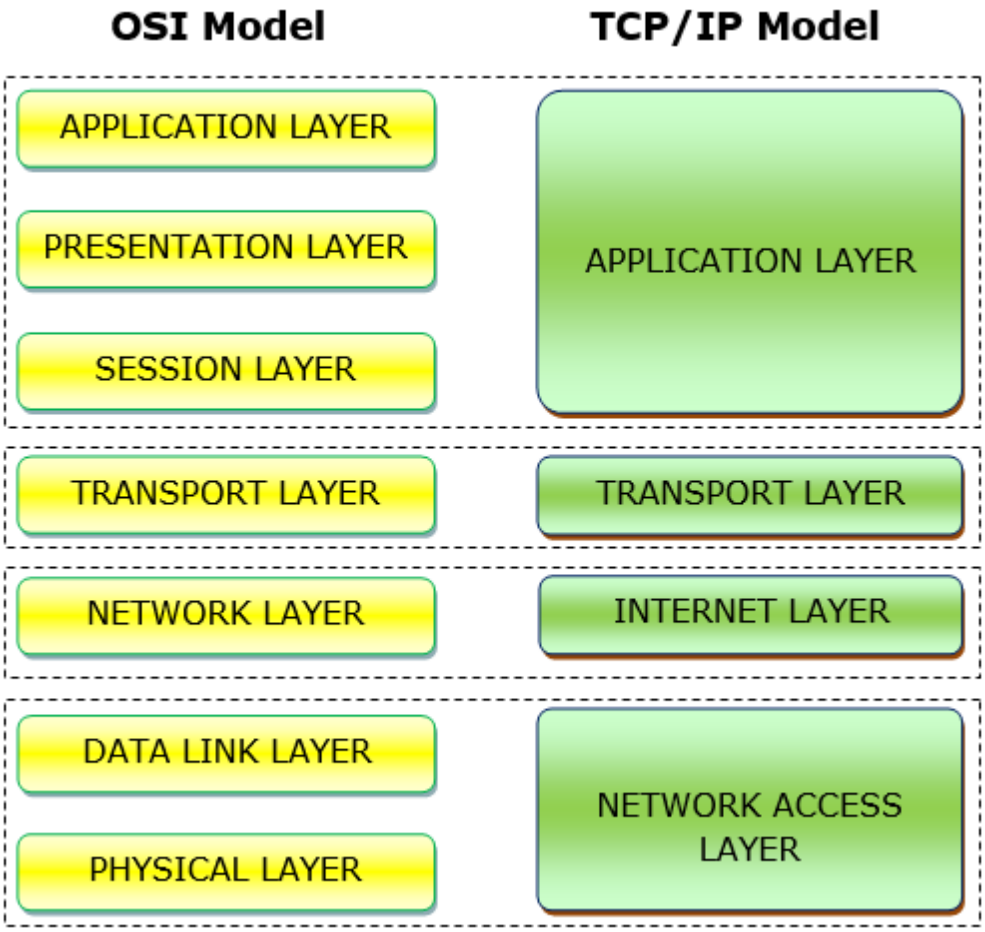
Similarities between OSI and TCP / IP Reference Models

- Both the reference models are based upon layered architecture.
- The layers in the models are compared with each other. The physical layer and the data link layer of the OSI model correspond to the link layer of the TCP/IP model. The network layers and the transport layers are the same in both the models. The session layer, the presentation layer and the application layer of the OSI model together form the application layer of the TCP/IP model.
- In both the models, protocols are defined in a layer-wise manner.
- In both models, data is divided into packets and each packet may take the individual route from the source to the destination.

Differences between OSI and TCP / IP Reference Models

- OSI model is a generic model that is based upon functionalities of each layer. TCP/IP model is a protocol-oriented standard.
- OSI model distinguishes the three concepts, namely, services, interfaces, and protocols. TCP/IP does not have a clear distinction between these three.
- OSI model gives guidelines on how communication needs to be done, while TCP/IP protocols layout standards on which the Internet was developed. So, TCP/IP is a more practical model.
- In OSI, the model was developed first and then the protocols in each layer were developed. In the TCP/IP suite, the protocols were developed first and then the model was developed.
- The OSI has seven layers while the TCP/IP has four layers.

The following diagram shows the corresponding layers of OSI and TCP/IP models −



Unit-02 (Physical layer)

1.Introduction of Physical layer

Physical layer in the OSI model plays the role of interacting with actual hardware and signaling mechanism. Physical layer is the only layer of OSI network model which actually deals with the physical connectivity of two different stations. This layer defines the hardware equipment, cabling, wiring, frequencies, pulses used to represent binary signals etc.

Physical layer provides its services to Data-link layer. Data-link layer hands over frames to physical layer. Physical layer converts them to electrical pulses, which represent binary data.The binary data is then sent over the wired or wireless media.

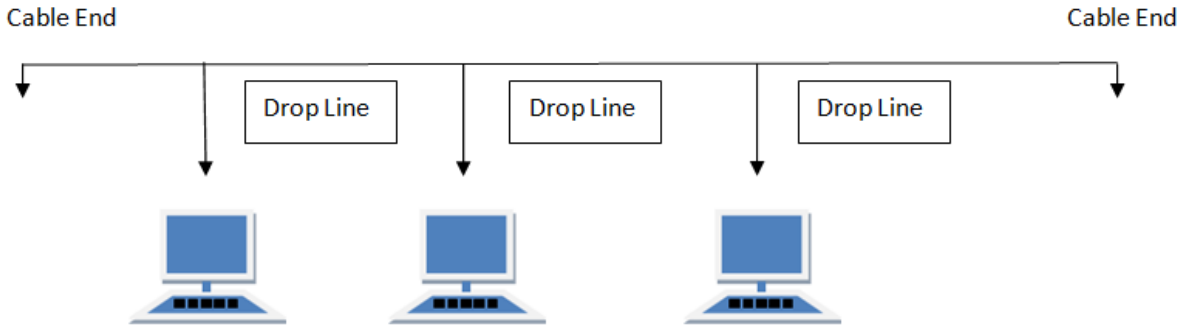
2.Topology

Network Topology is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection.

Network topologies describe the methods in which all the elements of a network are mapped. The topology term refers to both the physical and logical layout of a network.

BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

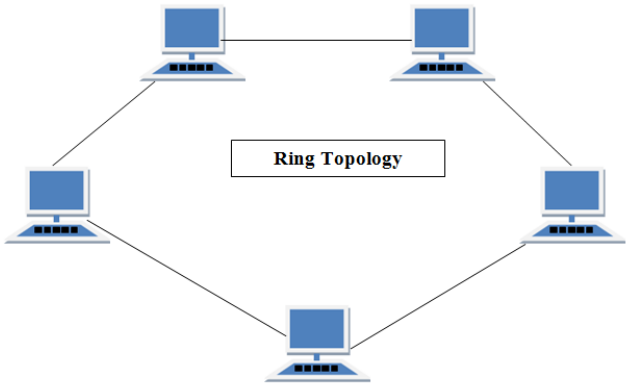
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

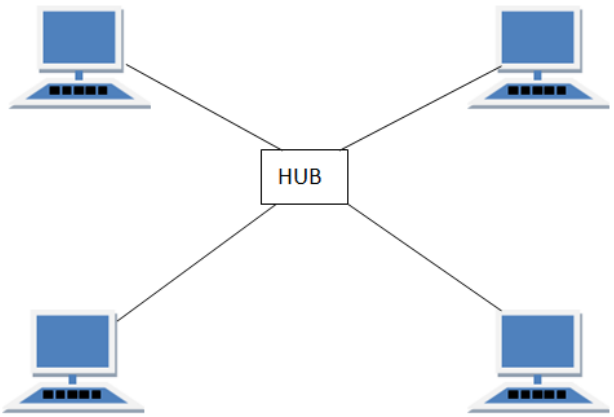
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

STAR Topology

In this type of topology all the computers 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.



Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has `n(n-1)/2` physical channels to link `n` devices.

There are two techniques to transmit data over the Mesh topology, they are :

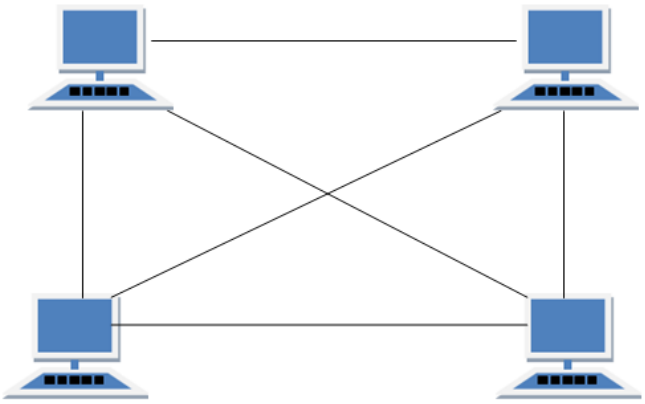
1. Routing
2. Flooding

MESH Topology: Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

MESH Topology: Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.



Types of Mesh Topology

1. **Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :** Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

Advantages of Mesh Topology

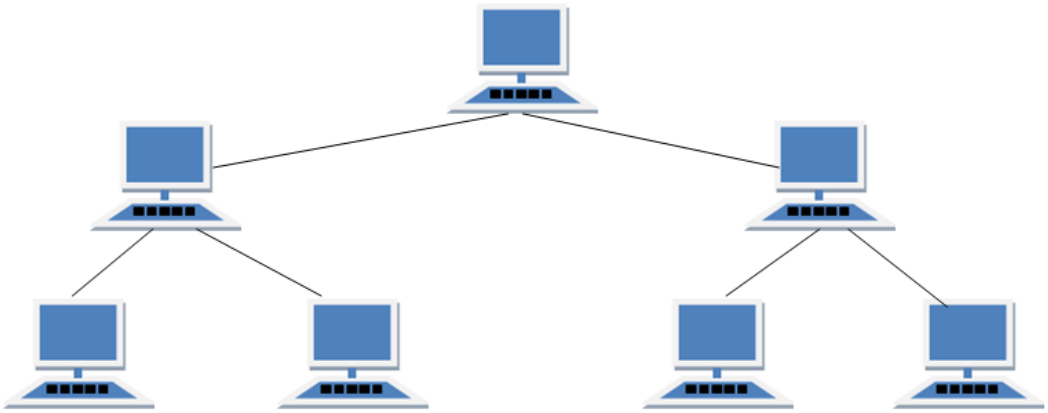
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

2.Considerations when choosing a Topology

The following are the key factors you should pay attention to when choosing a network topology.

1. Budget

A rule of thumb is to never make technology procurement decisions based on price alone. There's no denying though that you can only cut your coat according to your cloth. If a topology is unaffordable, it's off the table no matter how perfectly suited it might be for your situation.

In any case, irrespective of what your preferred topology is, there'll almost always be a lower-priced alternative that's nearly as effective. On pricing

matters, bus and ring topologies are quite cost-effective while star, mesh, tree and hybrid topologies are expensive.

2. Hardware Resources

Certain network topologies work best with certain hardware. And vise-versa. So before you make a decision on the topology to adopt, perform an inventory of your current hardware. You may also already have the hardware needed to implement a certain type of topology. So as opposed to buying everything from scratch, such existing resources give you a head start.

For instance, you may have hardware limitations such as the length of the network cable. In that case, you'd go for a topology that requires the least amount of cable for connecting nodes. Bus and star topologies perform pretty well in this regard.

3. Ease of Implementation

If you'll contract a third party to install and/or maintain your network, then the complexity of the network topology you choose is perhaps a non-issue.
A competent networking professional will have the education and experience needed to comprehend what each topology entails and implement it accordingly.
However, if you expect to leave network implementation in the hands of novices or individuals without the requisite IT training, then the ease of the topology should be a major factor in your choice. In this case, the bus and star topologies score pretty well. The mesh, tree and hybrid, on the other hand, are complex and difficult for a layman to install or understand.

4. Size of Network

How many devices are going to be on your network? How geographically dispersed are they? How far from the 'center' is the furthest device? Some topologies are inadequate or expensive when applied to large networks. A

topology that works perfectly for a 5-device network may prove a disaster when applied to a 10,000-device organization.

Part of the inventorying process we referred to in point 2 should include determining the total number of devices to be interconnected. Armed with this information, you can choose the topology that would best serve the purpose. The tree topology works well with large networks. The bus topology is best suited for small organizations.

5. Reliability

When it comes to reliability, network topologies aren't created equal. If you are looking for high reliability because you are in an industry where even brief downtime and delays are frowned upon (e.g. banking), then network reliability is a fundamental consideration. Choose the topology that delivers the highest reliability.

Ring topology performs pretty well under heavy loads but is prone to a single point of failure. Star topology doesn't depend on any node but the network will collapse if the hub fails. Mesh and hybrid topologies score highest on the reliability front.

6. Future Expansion

If you expect your organization to grow in size in the medium to long-term, opt for a network topology that's readily scalable. Identify the topology that's easy to add new nodes to, without negatively affecting network performance or the user experience of other devices on the network.

The tree topology is perhaps the most compatible with future expansion requirements as it's fairly easy to extend or shrink the network. The bus topology is also easy to expand but only to a certain extent which is why it would only work for small networks.

Choosing a network topology is one of the most important decisions you'll make for your technology infrastructure and will have far-reaching ramifications over the long-term. A wrong choice can prove to be an expensive mistake. It's a decision that requires careful thought in order to get it right from the start.

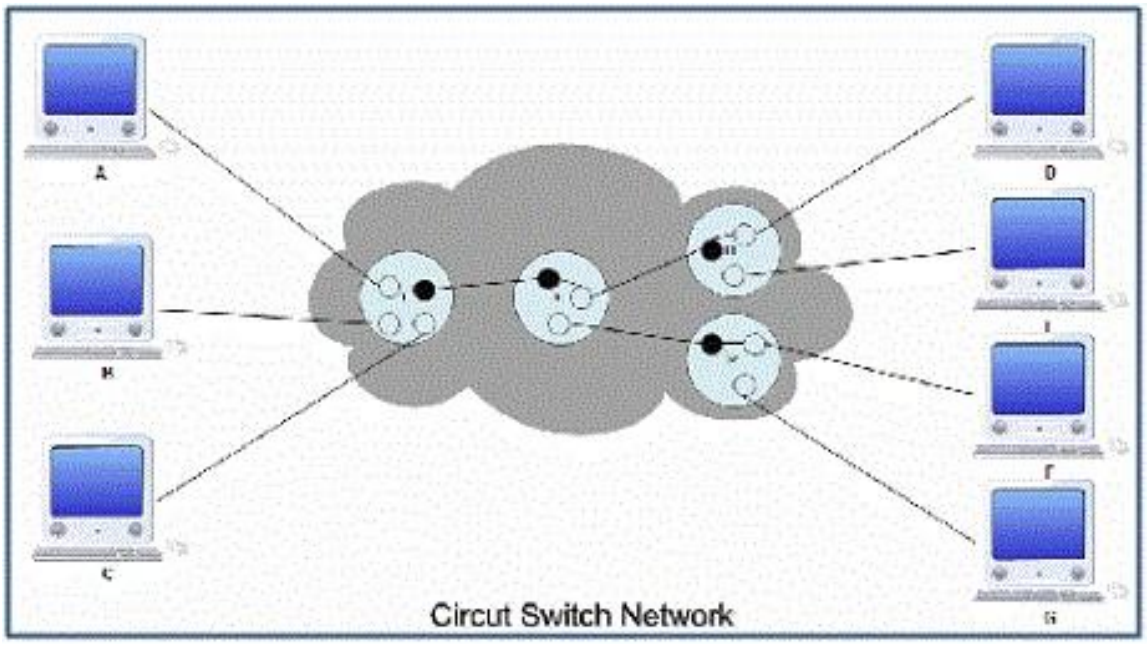
4.Switching method

Whenever we are dealing with a **large network** or say a very long-distance data transmission has to take place, this can't be done directly without any external hardware support. Hence, we must have a dedicated path for our data packets to traverse. Since there are so many choices for which path to take, so we have to select a particular path. This selecting of the path on which our data packets will be transmitted is known as **Switching**.

We can now categorize and sub-categorize the switching techniques as shown below:

1. Circuit Switching
2. Message Switching
3. Packet Switching

1) Circuit Switching



- Circuit Switching is a technique that directly connects the sender and the receiver in an unbroken path.
- For example take telephone switching equipment establishes a path that connects the caller's and reciever's telephone by making a physical connection.
- Routing decisions in circuit must be made when the circuit is first established, but there are no decisions made after that time.
- A complete end to end path must exist before communication can take place.
- Once the connection has been initiated and completed, the destination device must acknowledge that it is ready and able to carry on a transfer.

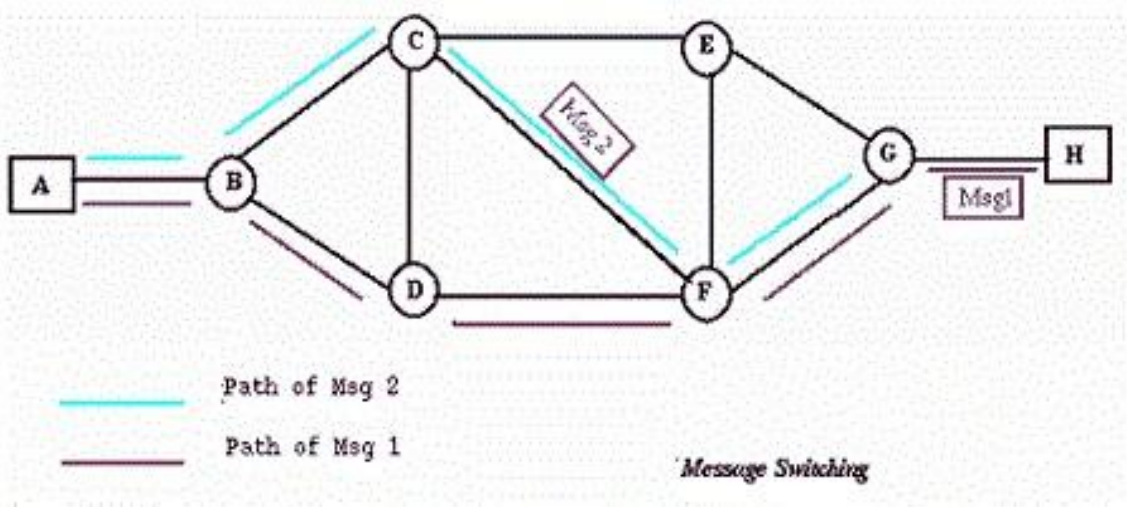
Advantages:

- The communication channel is end to end dedicated

Disadvantages:

- More bandwidth is required.
- Connection establishment time is more.
- More expensive than any other switching techniques because a dedicated path is required for each connection.
- Inefficient use of communication channel.

2) Message Switching



- In message switching there is no dedicated path required between two communicating devices, because the message switching is the follow the connectionless network.
- With message switching there is no need to establish dedicated path between two stations.
- When a station sends a message, the destination address is appended to the message.
- The message is then transmitted through the network in its entirety, from node to node.
- Each node receives the entire message, stores it in its entirety on disk and then transmits the message to the next node. This type of network is called a store and forward network.

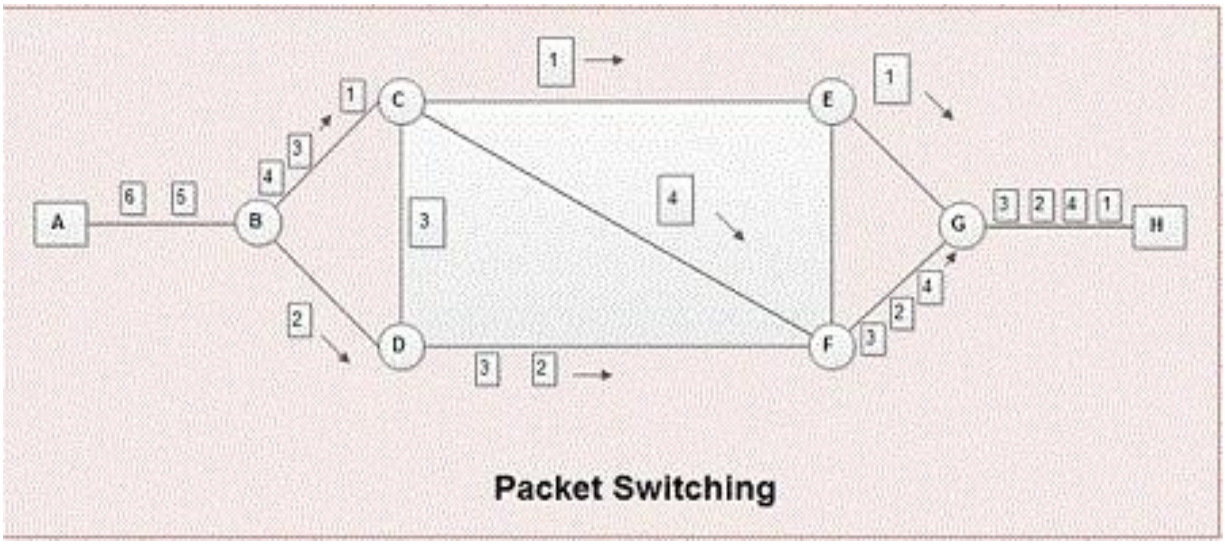
Advantages:

- Efficient traffic management.
- Large storing capacity required.

Disadvantages:

- Is not compatible with interactive applications.
- Store and forward devices are example.

3) Packet Switching



- In packet switching message are broken up into packet.
- Each packet is tagged with appropriate source and destination address.
- Individual packets take different routes to reach the destination.

Packet switching: Datagram

- Datagram packet switching is a packet switching technology by which each packet is treated as a separate entity and are called as datagram.
- Packets have their own complete addressing information attached.
- Each packet follows different routes to reach the destination.
- So, the packets may arrive at different times, and may be in a disturbed order. In this case reordering is done.

Packet switching: Virtual

- In this type of switching a preplanned route is established before the packets are sent.
- Sender sends a **"call request packet"** to establish a logical connection and receiver sends back an acknowledgement packet **"packet accepted"**.
- It is a cross between circuit switching network and packet switching network.

Advantages:

- Packet switching is cost effective.
- Offers improved delay characteristics.
- Packet can be rerouted if any problem occurs.

Disadvantages:

- Packet switching protocols are typically more complex.
- If packet gets lost sender needs to resend the data.

- This is a technique for transmitting and receiving independent signals over a common communication channel through synchronized switches at each end of the transmission line. This technique is widely used for long-distance communication links and also supports heavy data traffic loads from both the ends. It is also known as a digital circuit-switched method.

Advantages of Circuit Switching:

- Establishment of a dedicated channel
- Improves data transmission rate
- Improves data loss
- Improves delay in the data flow

Disadvantages of Circuit Switching:

- Establishing a dedicated channel sometimes **takes a very long duration** of time.
- The amount of bandwidth required is more for establishing a dedicated channel.
- Even if a channel is free, it **cannot be used to transmit any other data** from any other source.

the entire data to be shared, a message is the smallest individual unit. Unlike circuit switching there's no dedicated path between the sender and the receiver, hence they are connected through several intermediate nodes which helps and ensures proper data transfer. These messages switched data networks are also known as a hop-by-hop system.

They have 2 important characteristics:

1. **Store & forward:** since the users aren't directly connected, the intermediate nodes are then responsible for transferring the entire message to the next node in the path. To do so, each node must have a storage capacity, because a message will only be delivered if the next node and the link between them are available to connect otherwise it will be stored indefinitely. A store-and-forward switch thus forwards a message only if sufficient resources are available and the next node is ready to accept the data. Hence, it's called store-&-forward property. The store-and-forward was earlier used in telegraph message switching centers.
2. **Message delivery:** here the entire information is compiled into a single message and then that message is transmitted from source to destination. To successfully reach its destination each message must contain the routing information in its header section.

Advantages of Message Switching:

- Stores the message when the next node is not available
- Reduces traffic congestion.
- Data channels are shared by network devices.
- Manages traffic efficiently by assigning priorities.

Disadvantages of Message Switching:

- Storing of messages causes delays.
- The whole network requires a large storage capacity.

5.Relationship between Packet Size and Transmission time

The **transmission time** is the amount of time from the beginning until the end of a message transmission. In the case of a digital message, it is the time from the first bit until the last bit of a message has left the transmitting node. The packet transmission time in seconds can be obtained from the *packet size* in bit and the bit rate in bit/s as:

Packet transmission time = Packet size / Bit rate

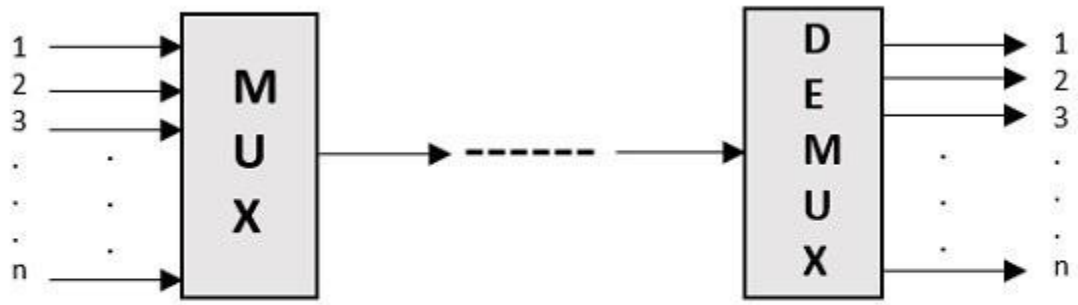
What is a Multiplexing?

Multiplexing is the process of combining multiple signals into one signal, over a shared medium. If the analog signals are multiplexed, then it is called as **analog multiplexing**. Similarly, if the digital signals are multiplexed, then it is called as **digital multiplexing**.

Multiplexing was first developed in telephony. A number of signals were combined to send through a single cable. The process of multiplexing divides a communication channel into several number of logical channels, allotting each one for a different message signal or a data stream to be transferred. The device that does multiplexing can be called as **Multiplexer** or **MUX**.

The reverse process, i.e., extracting the number of channels from one, which is done at the receiver is called as **de-multiplexing**. The device that does de-multiplexing can be called as **de-multiplexer** or **DEMUX**.

The following figures illustrates the concept of MUX and DEMUX. Their primary use is in the field of communications.



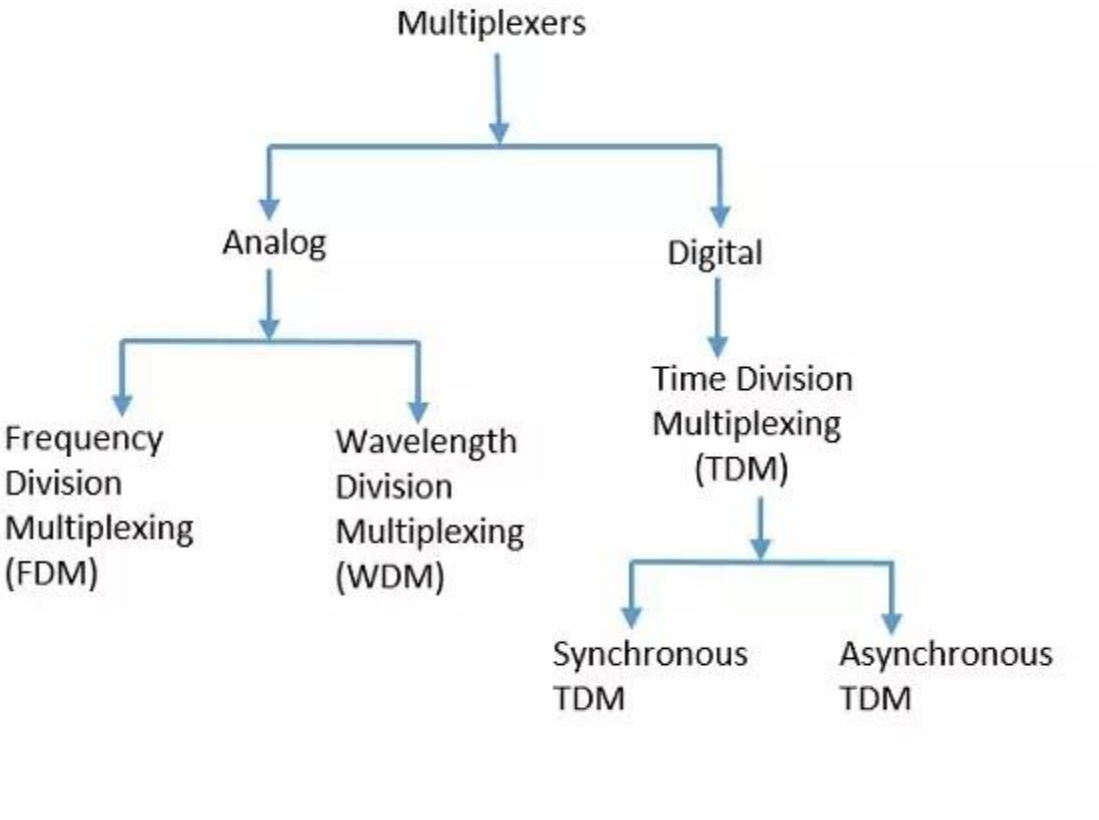
Multiplexing and Demultiplexing

Types of Multiplexing Techniques

The **3 types of multiplexing** techniques include the following.

- Frequency Division Multiplexing (FDM)
- Wavelength Division Multiplexing (WDM)
- Time Division Multiplexing (TDM)

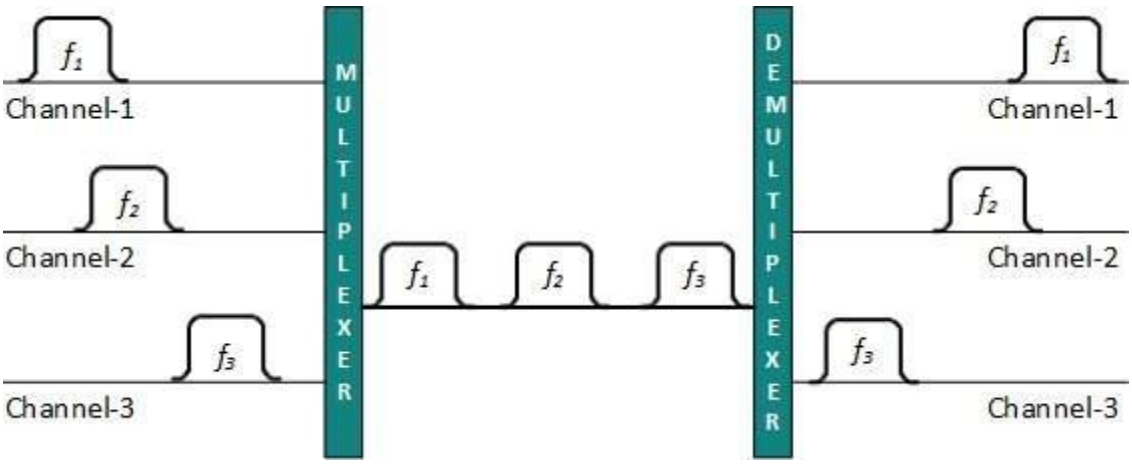
There are mainly two types of multiplexers, namely analog and digital. They are further divided into FDM, WDM, and TDM.



1). Frequency Division Multiplexing (FDM)

Frequency Division Multiplexing

When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel. Each user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.



2). Wavelength Division Multiplexing (WDM)

Light has different wavelength (colors). In fiber optic mode, multiple optical carrier signals are multiplexed into an optical fiber by using different wavelengths. This is an analog multiplexing technique and is done conceptually in the same manner as FDM but uses light as signals.

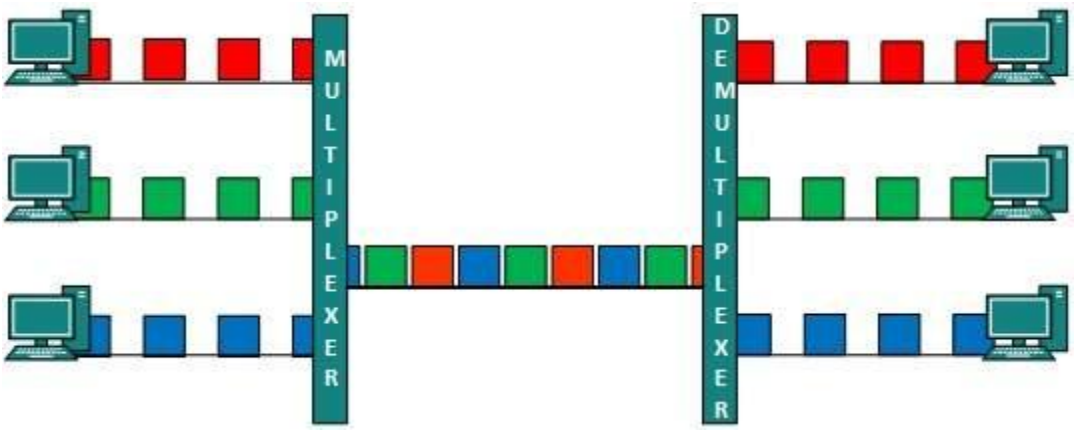
Further, on each wavelength time division multiplexing can be incorporated to accommodate more data signals.

3). Time Division Multiplexing (TDM)

TDM is applied primarily on digital signals but can be applied on analog signals as well. In TDM the shared channel is divided among its user by means of time slot. Each user can transmit data within the provided time slot only. Digital signals are divided in frames,

equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot.

TDM works in synchronized mode. Both ends, i.e. Multiplexer and De-multiplexer are timely synchronized and both switch to next channel simultaneously.



Types of Time Division Multiplexing

The different types of TDM include the following.

- Synchronous TDM
- Asynchronous TDM
- Interleaving TDM
- Statistical TDM

1). Synchronous TDM

The synchronous TDM is very useful in both analog as well as digital signals. In this type of TDM, the connection of input is allied to a frame. For example, if there are n-connections in the frame, then a frame will be separated into n-time slots, and for every unit, each slot is assigned to every input line.

In the sampling of synchronous TDM, the speed is similar for every signal, as well as this sampling needs a clock (CLK) signal at both the ends of sender & receiver. In this type of TDM, the multiplexer assigns the similar slot for each device at every time.

2).Asynchronous TDM

In asynchronous TDM, for different signals, the rate of sampling is also different, and it doesn't need a general clock (CLK). If the device has nothing for transmitting, then the time slot is assigned to a new device. The design of a commutator otherwise de-commutator is not easy & the bandwidth is low for this type of multiplexing, and it is applicable for not synchronous transmit form network.

Applications of Multiplexing

The applications of multiplexing include the following.

- Analog Broadcasting
- Digital Broadcasting
- Telephony
- Video Processing
- Telegraphy

Unit -03

1.Data link layer

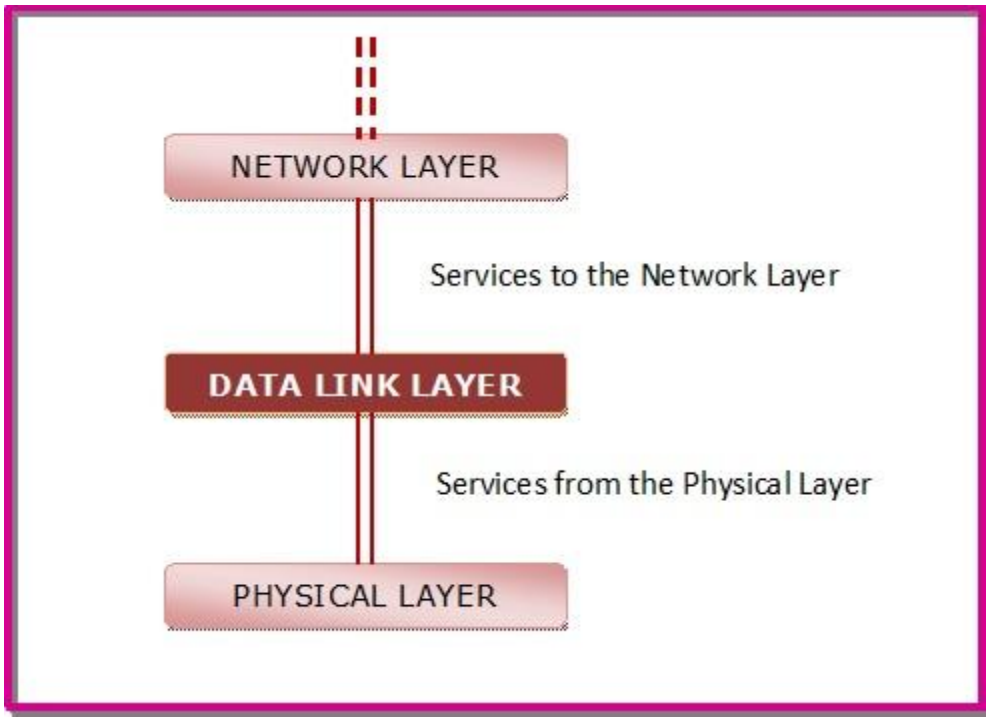
The data link layer in the OSI (Open System Interconnections) Model, is in between the physical layer and the network layer. This layer converts the raw transmission facility provided by the physical layer to a reliable and error-free link.

The main functions and the design issues of this layer are

- Providing services to the network layer
- Framing
- Error Control
- Flow Control

Services to the Network Layer

In the OSI Model, each layer uses the services of the layer below it and provides services to the layer above it. The data link layer uses the services offered by the physical layer. The primary function of this layer is to provide a well defined service interface to network layer above it.



The types of services provided can be of three types −

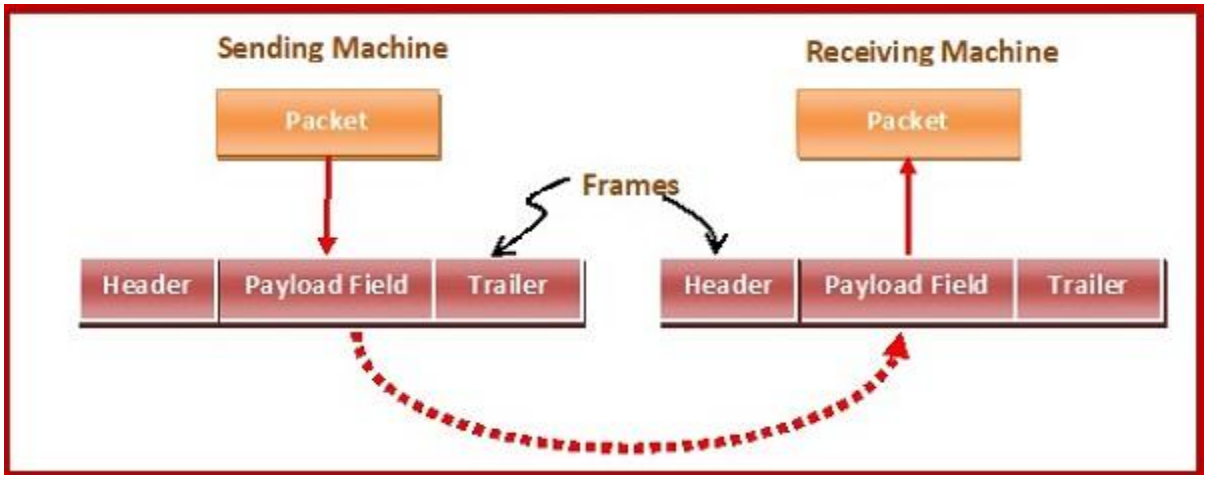
- Unacknowledged connectionless service
- Acknowledged connectionless service
- Acknowledged connection - oriented service

Framing

The data link layer encapsulates each data packet from the network layer into frames that are then transmitted.

A frame has three parts, namely −

- Frame Header
- Payload field that contains the data packet from network layer
- Trailer



Error Control

The data link layer ensures error free link for data transmission. The issues it caters to with respect to error control are −

- Dealing with transmission errors
- Sending acknowledgement frames in reliable connections
- Retransmitting lost frames
- Identifying duplicate frames and deleting them
- Controlling access to shared channels in case of broadcasting

Flow Control

The data link layer regulates flow control so that a fast sender does not drown a slow receiver. When the sender sends frames at very high speeds, a slow receiver may not be able to handle it. There will be frame losses even if the transmission is error-free. The two common approaches for flow control are −

- Feedback based flow control
- Rate based flow control

2.ARQ(Automatic Repeat Request)

Automatic Repeat Request (ARQ) is a group of error – control protocols for transmission of data over noisy or unreliable communication network. These protocols reside in the Data Link Layer and in the Transport Layer of the OSI (Open Systems Interconnection) reference model. They are named so because they provide for automatic retransmission of frames that are corrupted or lost during transmission. ARQ is also called Positive Acknowledgement with Retransmission (PAR).

ARQs are used to provide reliable transmissions over unreliable upper layer services. They are often used in Global System for Mobile (GSM) communication.

Working Principle

In these protocols, the receiver sends an acknowledgement message back to the sender if it receives a frame correctly. If the sender does not receive the acknowledgement of a transmitted frame before a specified period of time, i.e. a timeout occurs, the sender understands that the frame has been corrupted or lost during transit. So, the sender retransmits the frame. This process is repeated until the correct frame is transmitted.

Types of ARQ Protocols

There are three ARQ protocols in the data link layer.

- **Stop – and – Wait ARQ** − Stop – and – wait ARQ provides unidirectional data transmission with flow control and error control mechanisms, appropriate for noisy channels. The sender keeps a copy of the sent frame. It then waits for a finite time to receive a positive acknowledgement from receiver. If the timer expires, the frame is retransmitted. If a positive acknowledgement is received then the next frame is sent.
- **Go – Back – N ARQ** − Go – Back – N ARQ provides for sending multiple frames before receiving the acknowledgement for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgement of a frame is not received within the time period, all frames starting from that frame are retransmitted.
- **Selective Repeat ARQ** − This protocol also provides for sending multiple frames before receiving the acknowledgement for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

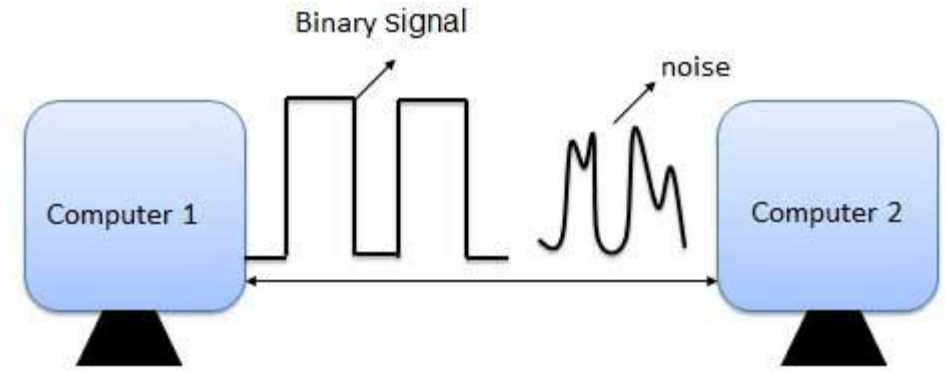
3.Error detection and Error correction

There are many reasons such as noise, cross-talk etc., which may help data to get corrupted during transmission. The upper layers work on some generalized view of network architecture and are not aware of actual hardware data processing.Hence, the upper layers expect error-free transmission between the systems. Most of the applications would not function expectedly if they receive erroneous data. Applications such as voice and video may not be that affected and with some errors they may still function well.

Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.

What is Error?

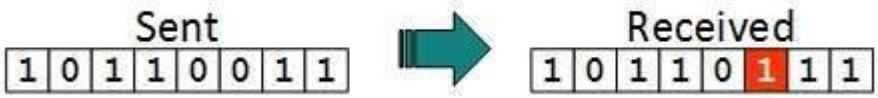
Error is a condition when the output information does not match with the input information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from one system to other. That means a 0 bit may change to 1 or a 1 bit may change to 0.



Types of Errors

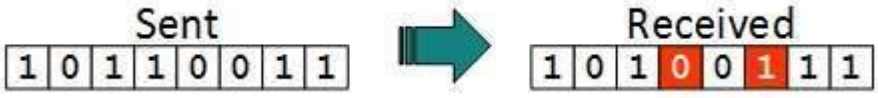
There may be three types of errors:

- **Single bit error**



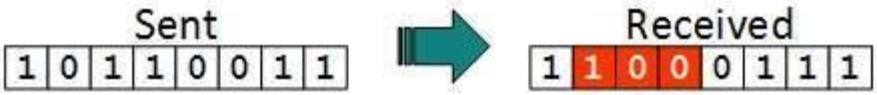
In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**



Frame is received with more than one bits in corrupted state.

- **Burst error**



Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

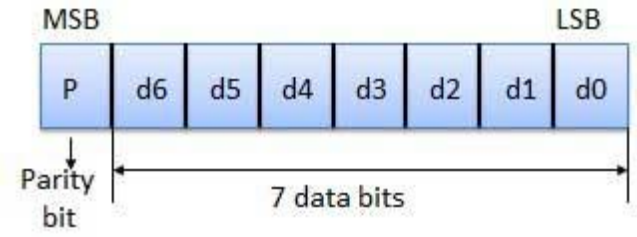
- Error detection
- Error correction

Error Detection

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

Parity Checking of Error Detection

It is the simplest technique for detecting and correcting errors. The MSB of an 8-bits word is used as the parity bit and the remaining 7 bits are used as data or message bits. The parity of 8-bits transmitted word can be either even parity or odd parity.



Even parity -- Even parity means the number of 1's in the given word including the parity bit should be even (2,4,6,....).

Odd parity -- Odd parity means the number of 1's in the given word including the parity bit should be odd (1,3,5,....).

Use of Parity Bit

The parity bit can be set to 0 and 1 depending on the type of the parity required.

- For even parity, this bit is set to 1 or 0 such that the no. of "1 bits" in the entire word is even. Shown in fig. (a).
- For odd parity, this bit is set to 1 or 0 such that the no. of "1 bits" in the entire word is odd. Shown in fig. (b).

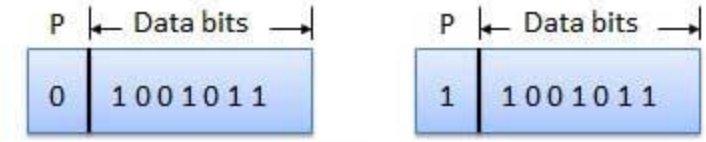


Fig. (a)

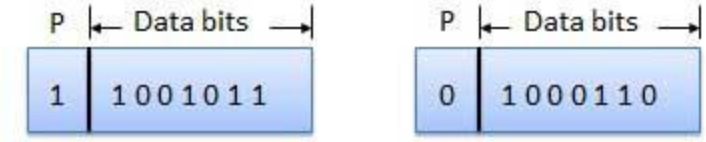
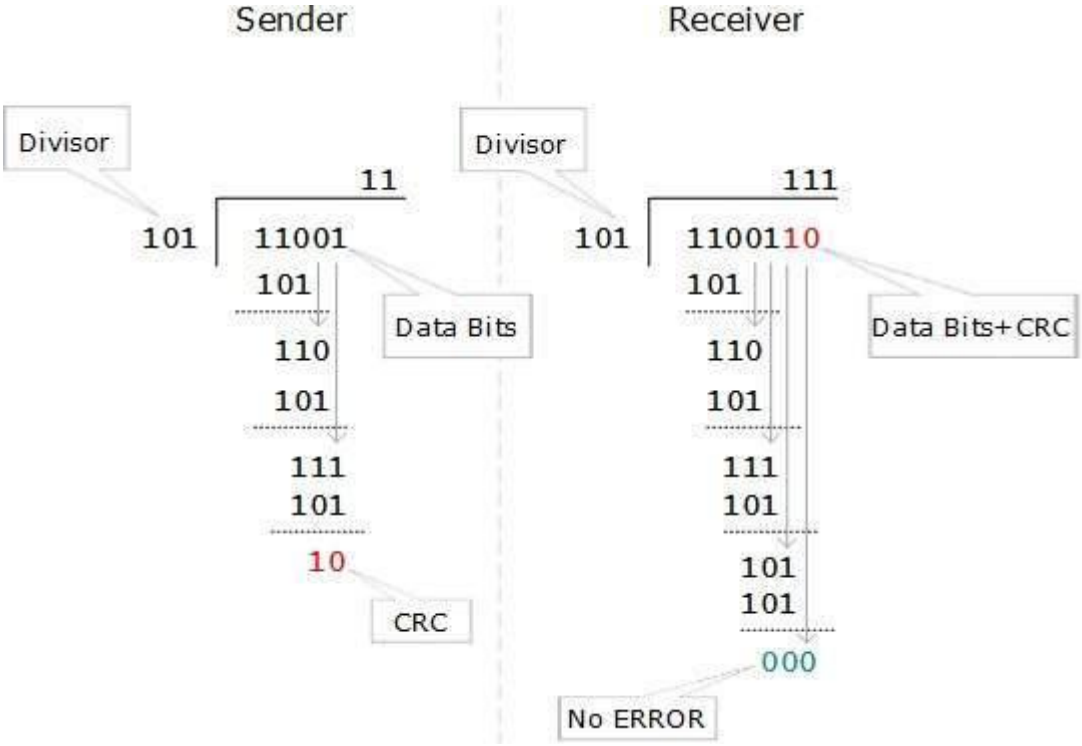


Fig. (b)

Cyclic Redundancy Check (CRC)

CRC is a different approach to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.



At the other end, the receiver performs division operation on codewords using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occurred in transit.

Error Correction

In the digital world, error correction can be done in two ways:

- **Backward Error Correction** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
- **Forward Error Correction** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.

To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection.For example, we take ASCII words (7 bits data), then there could be 8 kind of information we need: first seven bits to tell us which bit is error and one more bit to tell that there is no error.

For m data bits, r redundant bits are used. r bits can provide 2r combinations of information. In m+r bit codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about m+r bit locations plus no-error information, i.e. m+r+1.

$$2^r >= m+r+1$$

Hamming Distance

Hamming code is a block code that is capable of detecting up to two simultaneous bit errors and correcting single-bit errors. It was developed by R.W. Hamming for error correction.

In this coding method, the source encodes the message by inserting redundant bits within the message. These redundant bits are extra bits that are generated and inserted at specific positions in the message itself to enable error detection and correction. When the destination receives this message, it performs recalculations to detect errors and find the bit position that has error.

The Hamming distance between two strings, a and b is denoted as d(a,b).

It is used for error detection or error correction when data is transmitted over computer networks. It is also using in coding theory for comparing equal length data words.

Calculation of Hamming Distance

In order to calculate the Hamming distance between two strings, and , we perform their XOR operation, (a⊕ b), and then count the total number of 1s in the resultant string.

Example

Suppose there are two strings 1101 1001 and 1001 1101.

11011001 ⊕ 10011101 = 01000100. Since, this contains two 1s, the Hamming distance, d(11011001, 10011101) = 2.

Minimum Hamming Distance

In a set of strings of equal lengths, the minimum Hamming distance is the smallest Hamming distance between all possible pairs of strings in that set.

Example

Suppose there are four strings 010, 011, 101 and 111.

010 ⊕ 011 = 001, d(010, 011) = 1.

010 ⊕ 101 = 111, d(010, 101) = 3.

010 ⊕ 111 = 101, d(010, 111) = 2.

011 ⊕ 101 = 110, d(011, 101) = 2.

011 ⊕ 111 = 100, d(011, 111) = 1.

101 ⊕ 111 = 010, d(011, 111) = 1.

Hence, the Minimum Hamming Distance, d_{min} = 1.

Encoding a message by Hamming Code

The procedure used by the sender to encode the message encompasses the following steps −

- **Step 1** − Calculation of the number of redundant bits.
- **Step 2** − Positioning the redundant bits.
- **Step 3** − Calculating the values of each redundant bit.

Once the redundant bits are embedded within the message, this is sent to the user.

Step 1 − Calculation of the number of redundant bits.

If the message contains mmnumber of data bits, rrnumber of redundant bits are added to it so that mr is able to indicate at least (m + r+ 1) different states. Here, (m + r) indicates location of an error in each of (m + r) bit positions and one additional state indicates no error. Since, rr bits can indicate $2^r r$ states, $2^r r$ must be at least equal to (m + r + 1). Thus the following equation should hold $2^r \geq m+r+1$

Step 2 − Positioning the redundant bits.

The *r* redundant bits placed at bit positions of powers of 2, i.e. 1, 2, 4, 8, 16 etc. They are referred in the rest of this text as r_1 (at position 1), r_2 (at position 2), r_3 (at position 4), r_4 (at position 8) and so on.

Step 3 − Calculating the values of each redundant bit.

The redundant bits are parity bits. A parity bit is an extra bit that makes the number of 1s either even or odd. The two types of parity are −

- **Even Parity** − Here the total number of bits in the message is made even.
- **Odd Parity** − Here the total number of bits in the message is made odd.

Each redundant bit, r_i, is calculated as the parity, generally even parity, based upon its bit position. It covers all bit positions whose binary representation includes a 1 in the i^{th} position except the position of r_i. Thus −

- r_1 is the parity bit for all data bits in positions whose binary representation includes a 1 in the least significant position excluding 1 (3, 5, 7, 9, 11 and so on)
- r_2 is the parity bit for all data bits in positions whose binary representation includes a 1 in the position 2 from right except 2 (3, 6, 7, 10, 11 and so on)
- r_3 is the parity bit for all data bits in positions whose binary representation includes a 1 in the position 3 from right except 4 (5-7, 12-15, 20-23 and so on)

Decoding a message in Hamming Code

Once the receiver gets an incoming message, it performs recalculations to detect errors and correct them. The steps for recalculation are −

- **Step 1** − Calculation of the number of redundant bits.
- **Step 2** − Positioning the redundant bits.
- **Step 3** − Parity checking.
- **Step 4** − Error detection and correction

Step 1 − Calculation of the number of redundant bits

Using the same formula as in encoding, the number of redundant bits are ascertained.

$2^r \geq m + r + 1$ where *m* is the number of data bits and *r* is the number of redundant bits.

Step 2 − Positioning the redundant bits

The *r* redundant bits placed at bit positions of powers of 2, i.e. 1, 2, 4, 8, 16 etc.

Step 3 − Parity checking

Parity bits are calculated based upon the data bits and the redundant bits using the same rule as during generation of c_1,c_2 ,c_3 ,c_4 etc. Thus

c_1 = parity(1, 3, 5, 7, 9, 11 and so on)

c_2 = parity(2, 3, 6, 7, 10, 11 and so on)

c_3 = parity(4-7, 12-15, 20-23 and so on)

Step 4 − Error detection and correction

The decimal equivalent of the parity bits binary values is calculated. If it is 0, there is no error. Otherwise, the decimal value gives the bit position which has error. For example, if $c_1c_2c_3c_4$ = 1001, it implies that the data bit at position 9, decimal equivalent of 1001, has error. The bit is flipped to get the correct message.

Data link layer protocol

Data Link Layer protocols are generally responsible to simply ensure and confirm that the bits and bytes that are received are identical to the bits and bytes being transferred. It is basically a set of specifications that are used for implementation of data link layer just above the physical layer of the Open System Interconnections (OSI) Model.

Some Common Data Link Protocols :
There are various data link protocols that are required for Wide Area Network (WAN)and modem connections. Logical Link Control (LLC) is a data link protocol of Local Area Network (LAN). Some of data link protocols are given below :

1.Synchronous Data Link Protocol (SDLC)
2. High-Level Data Link Protocol (HDLC)
3. Serial Line Interface Protocol (SLIP)
4. Point to Point Protocol (PPP)
5. Link Control Protocol (LCP)
6. Link Access Procedure (LAP)
7. Network Control Protocol (NCP)

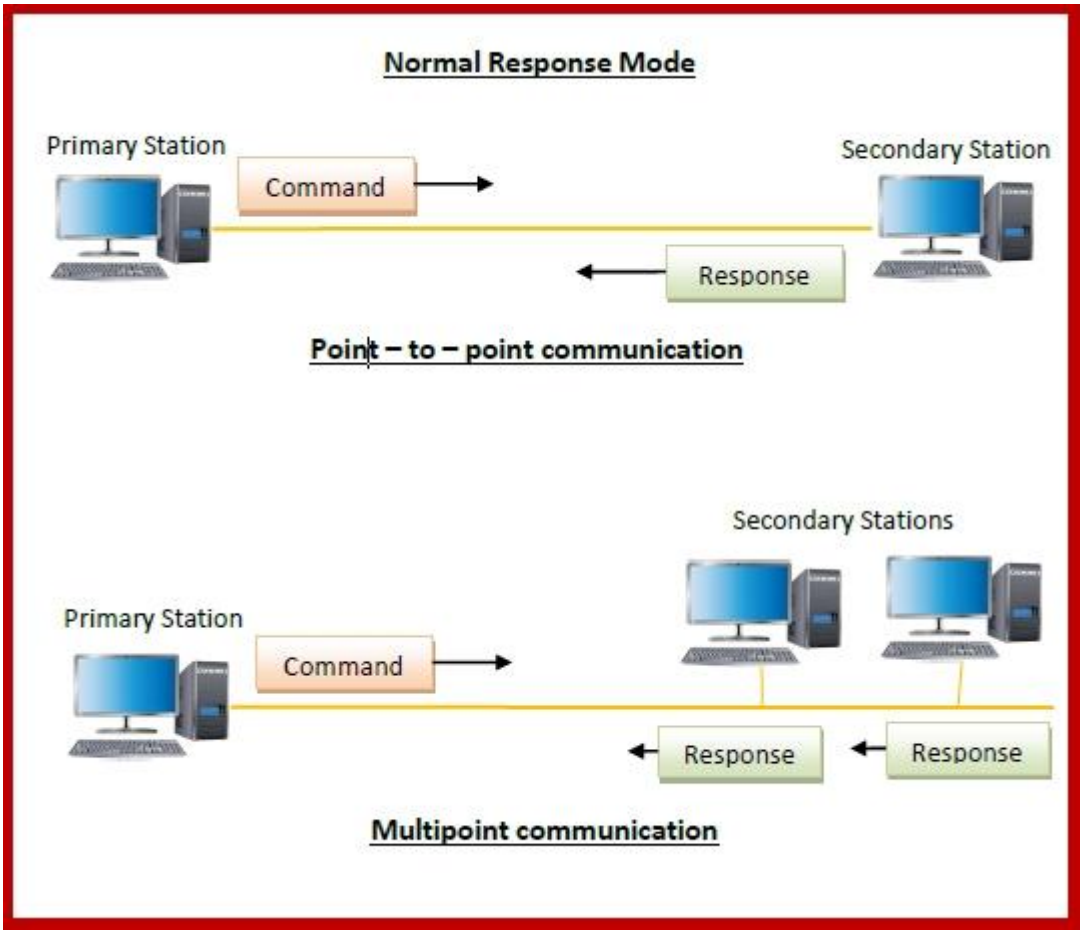
High-Level Data Link Protocol (HDLC)

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.

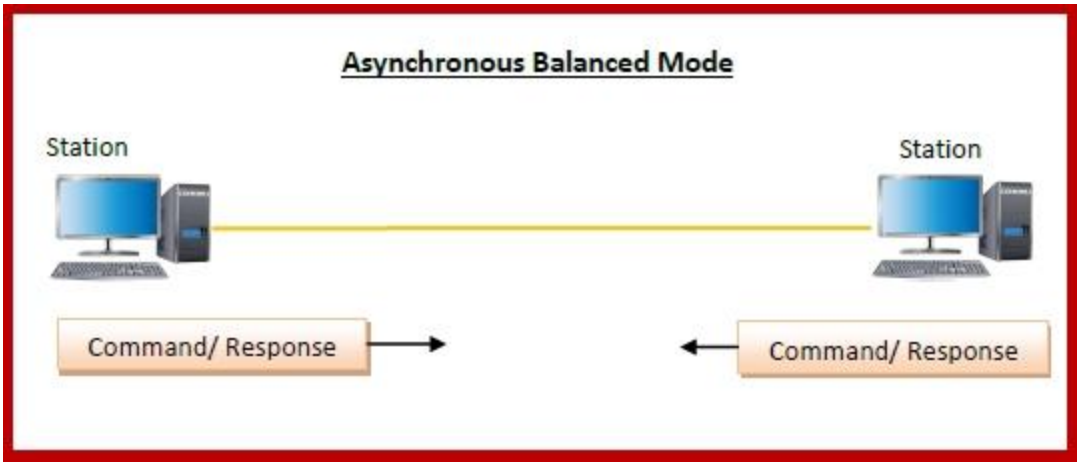
Transfer Modes

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.



Transmission Control Protocol (TCP)

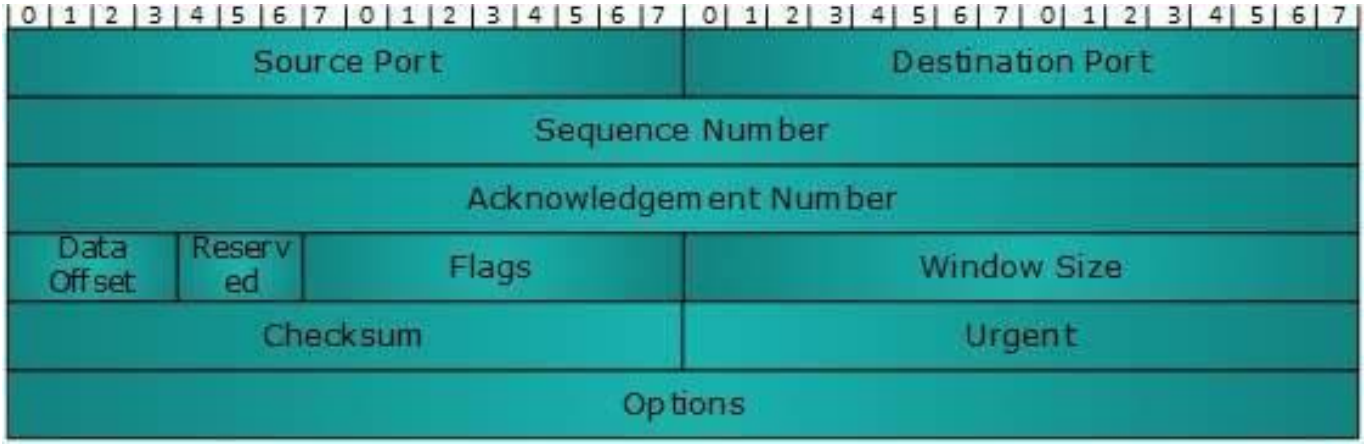
The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet.

Features

- TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- TCP ensures that the data reaches intended destination in the same order it was sent.
- 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.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

Header

The length of TCP header is minimum 20 bytes long and maximum 60 bytes.



- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.

- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Data Offset (4-bits)** - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits)** - Reserved for future use and all are set zero by default.
- **Flags (1-bit each)**
    - **NS** - Nonce Sum bit is used by Explicit Congestion Notification signaling process.
    - **CWR** - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.
    - **ECE** -It has two meanings:
        - If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.
        - If SYN bit is set to 1, ECE means that the device is ECT capable.
    - **URG** - It indicates that Urgent Pointer field has significant data and should be processed.
    - **ACK** - It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.
    - **PSH** - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.
    - **RST** - Reset flag has the following features:
        - It is used to refuse an incoming connection.
        - It is used to reject a segment.
        - It is used to restart a connection.
    - **SYN** - This flag is used to set up a connection between hosts.
    - **FIN** - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.

- **Windows Size** - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.
- **Checksum** - This field contains the checksum of Header, Data and Pseudo Headers.
- **Urgent Pointer** - It points to the urgent data byte if URG flag is set to 1.
- **Options** - It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

Unit-04 (network layer)

Network layer is majorly focused on getting packets from the source to the destination, routing error handling and congestion control.

- Addressing**:**
  Maintains the address at the frame header of both source and destination and performs addressing to detect various devices in network.
- **Packeting:**
  This is performed by Internet Protocol. The network layer converts the packets from its upper layer.
- Routing**:**
  It is the most important functionality. The network layer chooses the most relevant and best path for the data transmission from source to destination.
- **Inter-networking:**
  It works to deliver a logical connection across multiple devices.

Network layer design issues:

The network layer comes with some design issues they are described as follows:

1. Store and Forward packet switching:
The host sends the packet to the nearest router. This packet is stored there until it has fully arrived once the link is fully processed by verifying the checksum then it is forwarded to the next router till it reaches the destination. This mechanism is called "Store and Forward packet switching."

2. Services provided to Transport Layer:
Through the network/transport layer interface, the network layer transfers it's services to the transport layer. These services are described below.
But before providing these services to the transfer layer following goals must be kept in mind :-

- Offering services must not depend on router technology.
- The transport layer needs to be protected from the type, number and topology of the available router.
- The network addresses for the transport layer should use uniform numbering pattern also at LAN and WAN connections.

Based on the connections there are 2 types of services provided :

- **Connectionless –** The routing and insertion of packets into subnet is done individually. No added setup is required.
- **Connection-Oriented –** Subnet must offer reliable service and all the packets must be transmitted over a single route.

3. Implementation of Connectionless Service:
Packet are termed as "datagrams" and corresponding subnet as "datagram subnets".
When the message size that has to be transmitted is 4 times the size of the packet, then the network layer divides into 4 packets and transmits each packet to router via. a few protocol.Each data packet has destination address and is routed independently irrespective of the packets.

4. Implementation of Connection Oriented service:
To use a connection-oriented service, first we establishes a connection, use it and then release it. In connection-oriented services, the data packets are delivered to the receiver in the same order in which they have been sent by the sender.
It can be done in either two ways :

- **Circuit Switched Connection –** A dedicated physical path or a circuit is established between the communicating nodes and then data stream is transferred.
- **Virtual Circuit Switched Connection –** The data stream is transferred over a packet switched network, in such a way that it seems to the user that there is a dedicated path from the sender to the receiver. A virtual path is established here. While, other connections may also be using the same path.

Routing

Routing is the process of forwarding of a packet in a network so that it reaches its intended destination. The main goals of routing are:

1. **Correctness:** The routing should be done properly and correctly so that the packets may reach their proper destination.

2. **Simplicity:** The routing should be done in a simple manner so that the overhead is as low as possible. With increasing complexity of the routing algorithms the overhead also increases.
3. **Robustness:** Once a major network becomes operative, it may be expected to run continuously for years without any failures. The algorithms designed for routing should be robust enough to handle hardware and software failures and should be able to cope with changes in the topology and traffic without requiring all jobs in all hosts to be aborted and the network rebooted every time some router goes down.
4. **Stability:** The routing algorithms should be stable under all possible circumstances.
5. **Fairness:** Every node connected to the network should get a fair chance of transmitting their packets. This is generally done on a first come first serve basis.
6. **Optimality:** The routing algorithms should be optimal in terms of throughput and minimizing mean packet delays. Here there is a trade-off and one has to choose depending on his suitability.

Next →← Prev

Routing algorithm

- In order to transfer the packets from source to the destination, the network layer must dete through which packets can be transmitted.
- Whether the network layer provides datagram service or virtual circuit service, the main job to provide the best route. The routing protocol provides this job.
- The routing protocol is a routing algorithm that provides the best path from the source to th path is the path that has the "least-cost path" from source to the destination.
- Routing is the process of forwarding the packets from source to the destination but the best packets is determined by the routing algorithm.

Classification of a Routing algorithm

The Routing algorithm is divided into two categories:

- Adaptive Routing algorithm
- Non-adaptive Routing algorithm

Adaptive Routing algorithm

- An adaptive routing algorithm is also known as dynamic routing algorithm.
- This algorithm makes the routing decisions based on the topology and network traffic.
- The main parameters related to this algorithm are hop count, distance and estimated transi

An adaptive routing algorithm can be classified into three parts:

- **Centralized algorithm:** It is also known as global routing algorithm as it computes the lea source and destination by using complete and global knowledge about the network. This alg connectivity between the nodes and link cost as input, and this information is obtained befo any calculation. **Link state algorithm** is referred to as a centralized algorithm since it is aw link in the network.
- **Isolation algorithm:** It is an algorithm that obtains the routing information by using local gathering information from other nodes.
- **Distributed algorithm:** It is also known as decentralized algorithm as it computes the leas source and destination in an iterative and distributed manner. In the decentralized algorithm knowledge about the cost of all the network links. In the beginning, a node contains the info own directly attached links and through an iterative process of calculation computes the leas destination. A Distance vector algorithm is a decentralized algorithm as it never knows the c source to the destination, instead it knows the direction through which the packet is to be fo least cost path.

Non-Adaptive Routing algorithm

- Non Adaptive routing algorithm is also known as a static routing algorithm.
- When booting up the network, the routing information stores to the routers.
- Non Adaptive routing algorithms do not take the routing decision based on the network topo

The Non-Adaptive Routing algorithm is of two types:

Flooding: In case of flooding, every incoming packet is sent to all the outgoing links except the on reached. The disadvantage of flooding is that node may contain several copies of a particular packe

Random walks: In case of random walks, a packet sent by the node to one of its neighbors rando using random walks is that it uses the alternative routes very efficiently.

Differences b/w Adaptive and Non-Adaptive Routing Algorithm

Basis Of Comparison	Adaptive Routing algorithm	Non-Adaptive Routing algorithm
Define	Adaptive Routing algorithm is an algorithm that constructs the routing table based on the network conditions.	The Non-Adaptive Routing algorithm is an algorithm that constructs the static table to determine which node to send the packet.
Usage	Adaptive routing algorithm is used by dynamic routing.	The Non-Adaptive Routing algorithm is used by static routing.
Routing decision	Routing decisions are made based on topology and network traffic.	Routing decisions are the static tables.

Categorization	The types of adaptive routing algorithm, are Centralized, isolation and distributed algorithm.	The types of Non Adaptive routing algorithm are flooding and random walks.
Complexity	Adaptive Routing algorithms are more complex.	Non-Adaptive Routing algorithms are simple.

Distance Vector Routing Algorithm

- **The Distance vector algorithm is iterative, asynchronous and distributed.**
  - **Distributed:** It is distributed in that each node receives information from one or more of its directly attached neighbors, performs calculation and then distributes the result back to its neighbors.
  - **Iterative:** It is iterative in that its process continues until no more information is available to be exchanged between neighbors.
  - **Asynchronous:** It does not require that all of its nodes operate in the lock step with each other.
- The Distance vector algorithm is a dynamic algorithm.
- It is mainly used in ARPANET, and RIP.
- Each router maintains a distance table known as **Vector**.

Working of Distance Vector Routing Algorithm:

- **Knowledge about the whole network:** Each router shares its knowledge through the entire network. The Router sends its collected knowledge about the network to its neighbors.
- **Routing only to neighbors:** The router sends its knowledge about the network to only those routers which have direct links. The router sends whatever it has

about the network through the ports. The information is received by the router and uses the information to update its own routing table.

- **Information sharing at regular intervals:** Within 30 seconds, the router sends the information to the neighboring routers.

Distance Vector Routing Algorithm

Let $d_x(y)$ be the cost of the least-cost path from node x to node y. The least costs are related by Bellman-Ford equation,

$$d_x(y) = \min_v\{c(x,v) + d_v(y)\}$$

Where the minv is the equation taken for all x neighbors. After traveling from x to v, if we consider the least-cost path from v to y, the path cost will be $c(x,v)+d_v(y)$. The least cost from x to y is the minimum of $c(x,v)+d_v(y)$ taken over all neighbors.

With the Distance Vector Routing algorithm, the node x contains the following routing information:

- For each neighbor v, the cost c(x,v) is the path cost from x to directly attached neighbor, v.
- The distance vector x, i.e., $D_x = [D_x(y) : y \text{ in } N]$, containing its cost to all destinations, y, in N.
- The distance vector of each of its neighbors, i.e., $D_v = [D_v(y) : y \text{ in } N]$ for each neighbor v of x.

Distance vector routing is an asynchronous algorithm in which node x sends the copy of its distance vector to all its neighbors. When node x receives the new distance vector from one of its neighboring vector, v, it saves the distance vector of v and uses the Bellman-Ford equation to update its own distance vector. The equation is given below:

$$d_x(y) = \min_v\{ c(x,v) + d_v(y)\} \quad \text{for each node } y \text{ in } N$$

The node x has updated its own distance vector table by using the above equation and sends its updated table to all its neighbors so that they can update their own distance vectors.

Advantages of Distance Vector routing –

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

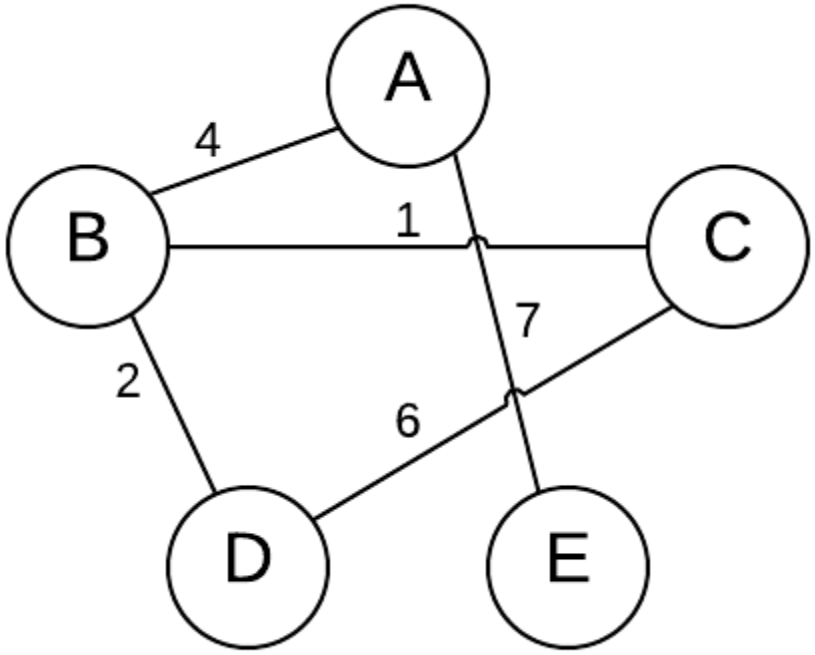
Disadvantages of Distance Vector routing –

- 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.

Shortest path algorithm

Shortest path algorithms are a family of algorithms designed to solve the shortest path problem. The shortest path problem is something most people have some intuitive familiarity with: given two points, A and B, what is the shortest path between them? In computer science, however, the shortest path problem can take different forms and so different algorithms are needed to be able to solve them all.

- For simplicity and generality, shortest path algorithms typically operate on some input graph, GG. This graph is made up of a set of vertices, VV, and edges, EE, that connect them. If the edges have weights, the graph is called a weighted graph. Sometimes these edges are bidirectional and the graph is called undirected. Sometimes there can be even be cycles in the graph. Each of these subtle differences are what makes one algorithm work better than another for certain graph type. An example of a graph is shown below.



-
- There are also different types of shortest path algorithms. Maybe you need to find the shortest path between point A and B, but maybe you need to shortest path between point A and all other points in the graph.

Types of shortest path algorithm

1.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.

Dijkstra's algorithm allows us to find the shortest path between any two vertices of a graph.

It differs from the minimum spanning tree because the shortest distance between two vertices might not include all the vertices of the graph.

Algorithm Steps:

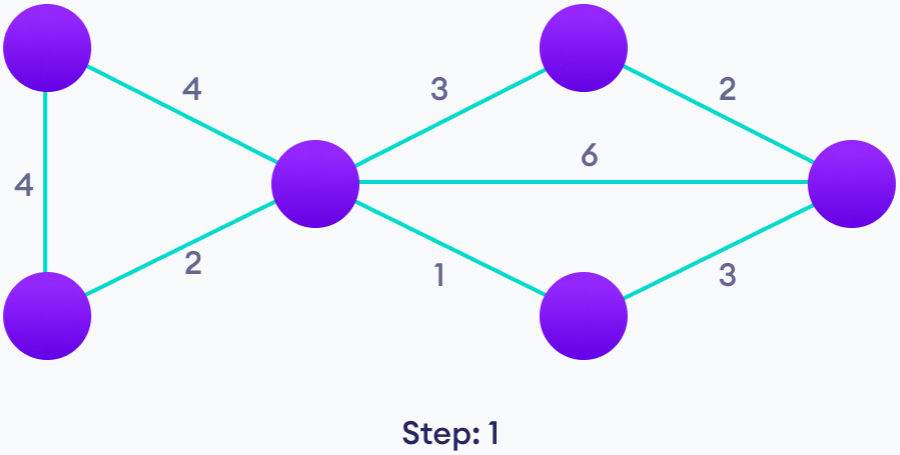
- Set all vertices distances = infinity except for the source vertex, set the source distance = 0.
- Push the source vertex in a min-priority queue in the form (distance , vertex), as the comparison in the min-priority queue will be according to vertices distances.
- Pop the vertex with the minimum distance 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.

How Dijkstra's Algorithm works

Dijkstra's Algorithm works on the basis that any subpath `B -> D` of the shortest path `A -> D` between vertices A and D is also the shortest path between vertices B and D.

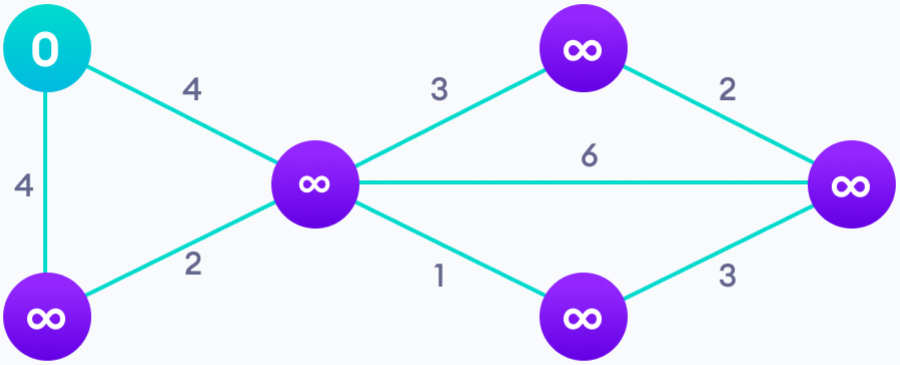
Example of Dijkstra's algorithm

It is easier to start with an example and then think about the algorithm.



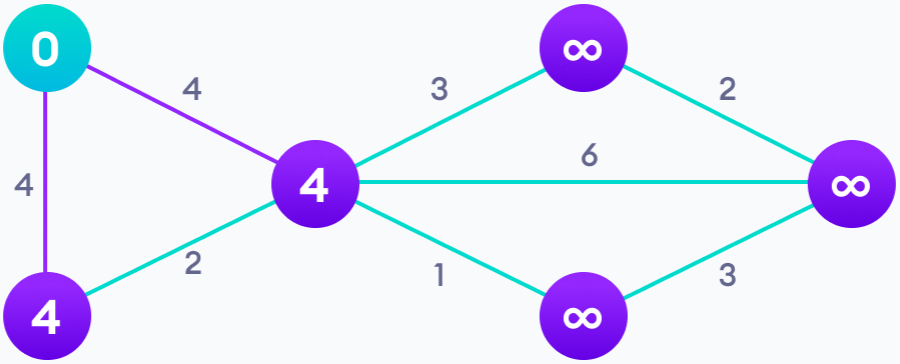
Step: 1

Start with a weighted graph



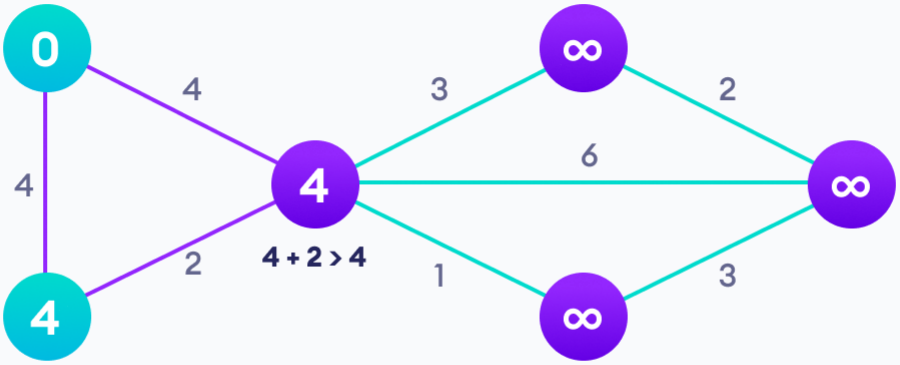
Step: 2

Choose a starting vertex and assign infinity path values to all other devices



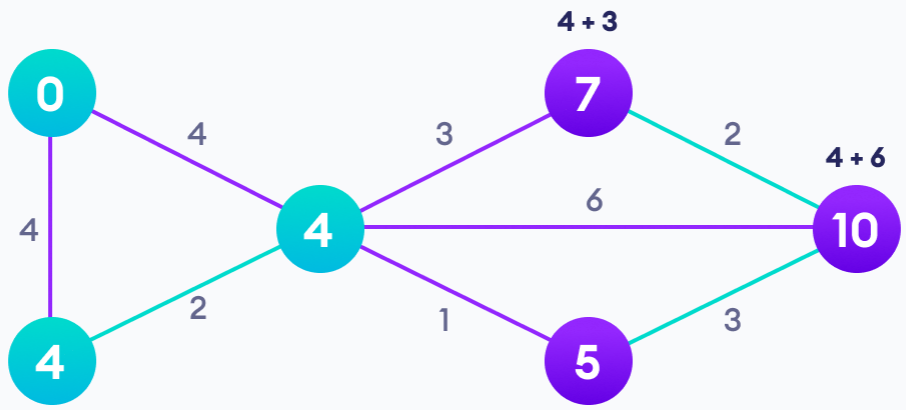
Step: 3

Go to each vertex and update its path length



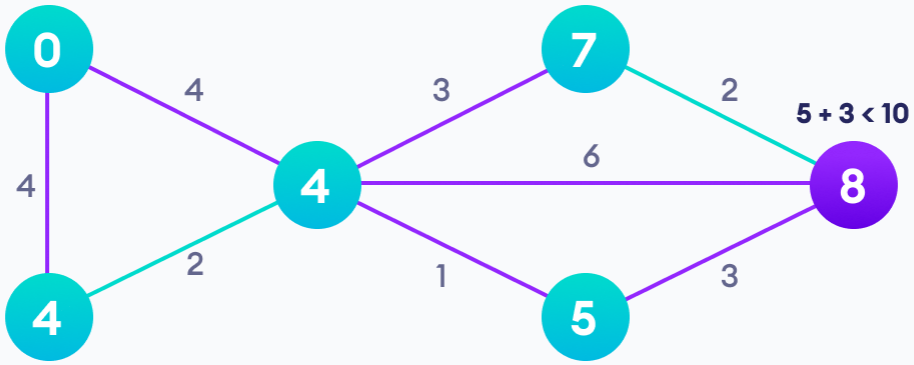
Step: 4

If the path length of the adjacent vertex is lesser than new path length, don't update it



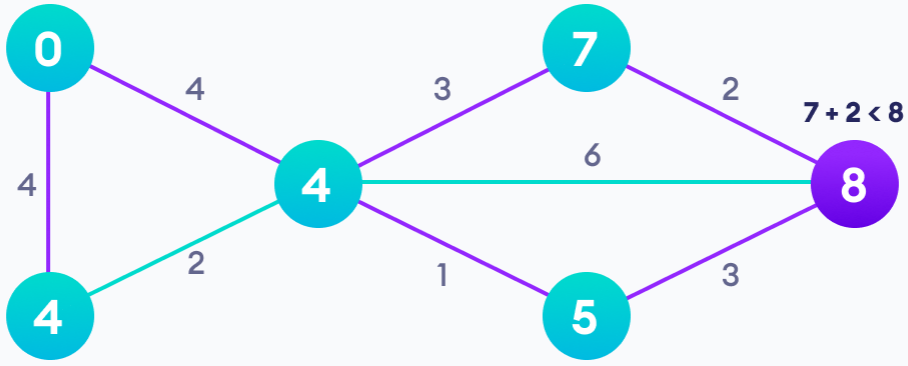
Step: 5

Avoid updating path lengths of already visited vertices



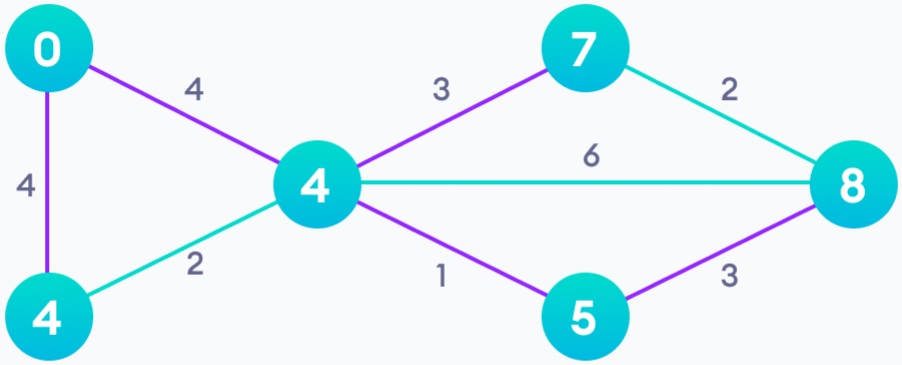
Step: 6

After each iteration, we pick the unvisited vertex with the least path length. So we choose 5 before 7



Step: 7

Notice how the rightmost vertex has its path length updated twice



Step: 8

Repeat until all the vertices have been visited

Djikstra used this property in the opposite direction i.e we overestimate the distance of each vertex from the starting vertex. Then we visit each node and its neighbors to find the shortest subpath to those neighbors.

The algorithm uses a greedy approach in the sense that we find the next best solution hoping that the end result is the best solution for the whole problem.

Advantages:-

1) It is used in Google Maps
2) It is used in finding Shortest Path.
3) It is used in geographical Maps
4) To find locations of Map which refers to vertices of graph.
5) Distance between the location refers to edges.
6) It is used in IP routing to find Open shortest Path First.
7) It is used in the telephone network.

Disadvantages:-

1) It do blind search so wastes lot of time while processing.
2) It cannot handle negative edges.
3) This leads to acyclic graphs and most often cannot obtain the right shortest path.

Hierarchical Routing

This is essentially a 'Divide and Conquer' strategy. The network is divided into different regions and a router for a particular region knows only about its own domain and other routers. Thus, the network is viewed at two levels:

1. The Sub-network level, where each node in a region has information about its peers in the same region and about the region's interface with other regions. Different regions may have different 'local' routing algorithms. Each local algorithm handles the traffic between nodes of the same region and also directs the outgoing packets to the appropriate interface.
2. The Network Level, where each region is considered as a single node connected to its interface nodes. The routing algorithms at this level handle the routing of packets between two interface nodes, and is isolated from intra-regional transfer.

Networks can be organized in hierarchies of many levels; e.g. local networks of a city at one level, the cities of a country at a level above it, and finally the network of all nations.

In Hierarchical routing, the interfaces need to store information about:

- All nodes in its region which are at one level below it.
- Its peer interfaces.
- At least one interface at a level above it, for outgoing packages.

Advantages of Hierarchical Routing :

- Smaller sizes of routing tables.
- Substantially lesser calculations and updates of routing tables.

Disadvantage :

- Once the hierarchy is imposed on the network, it is followed and possibility of direct paths is ignored. This may lead to sub optimal routing.

Flooding routing algorithm

Flooding is used in computer networks routing algorithm in which every incoming packet is sent through every outgoing link except the one it arrived on.

Flooding is used in bridging and in systems such as Usenet and peer-to-peer file sharing and as part of some routing protocols, including OSPF, DVMRP, and those used in ad-hoc wireless networks (WANETs).

Types of flooding

There are generally two types of flooding available, **uncontrolled flooding** and **controlled flooding**

In ***uncontrolled flooding*** each node unconditionally distributes packets to each of its neighbors. Without conditional logic to prevent indefinite recirculation of the same packet, broadcast storms are a hazard.

Controlled flooding has its own two algorithms to make it reliable, SNCF (Sequence Number Controlled Flooding)and RPF (Reverse Path Forwarding). In SNCF, the node attaches its own address and sequence number to the packet, since every node has a memory of addresses and sequence numbers. If it receives a packet in memory, it drops it immediately while in RPF, the node will only send the packet forward. If it is received from the next node, it sends it back to the sender.

Link State Routing –

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 of link state routing protocols –

- **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.

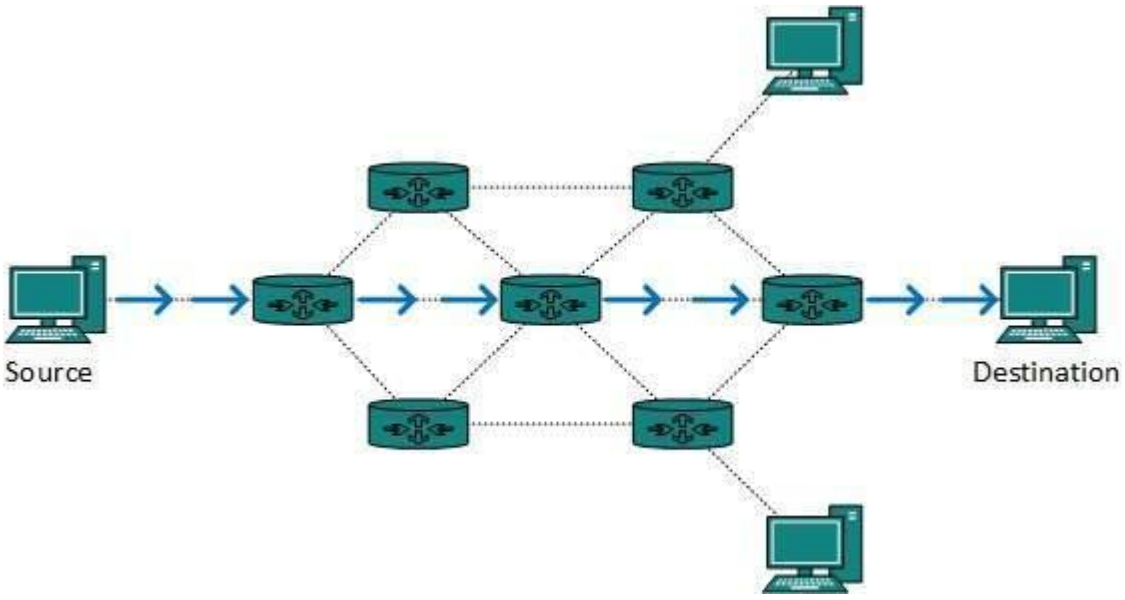
Calculation of shortest path –
To find shortest path, each node need to run the famous **Dijkstra algorithm**. This famous algorithm uses the following steps:

- **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

Difference between different casting

Unicast routing

Most of the traffic on the internet and intranets known as unicast data or unicast traffic is sent with specified destination. Routing unicast data over the internet is called unicast routing. It is the simplest form of routing because the destination is already known. Hence the router just has to look up the routing table and forward the packet to next hop.



Broadcast routing

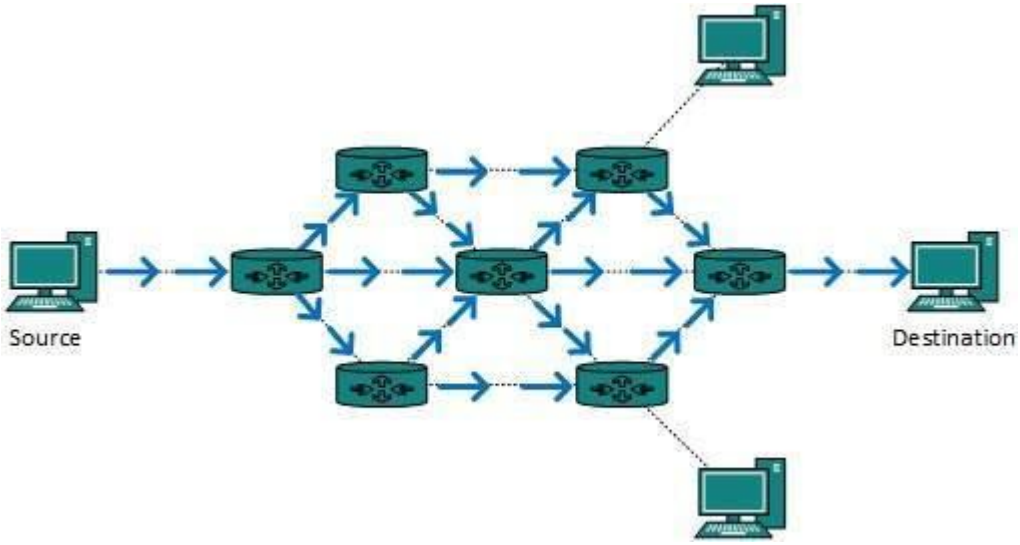
By default, the broadcast packets are not routed and forwarded by the routers on any network. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices.

Broadcast routing can be done in two ways (algorithm):

- A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses. All packets are sent as unicast but because they are sent to all, it simulates as if router is broadcasting.

  This method consumes lots of bandwidth and router must destination address of each node.

- Secondly, when router receives a packet that is to be broadcasted, it simply floods those packets out of all interfaces. All routers are configured in the same way.

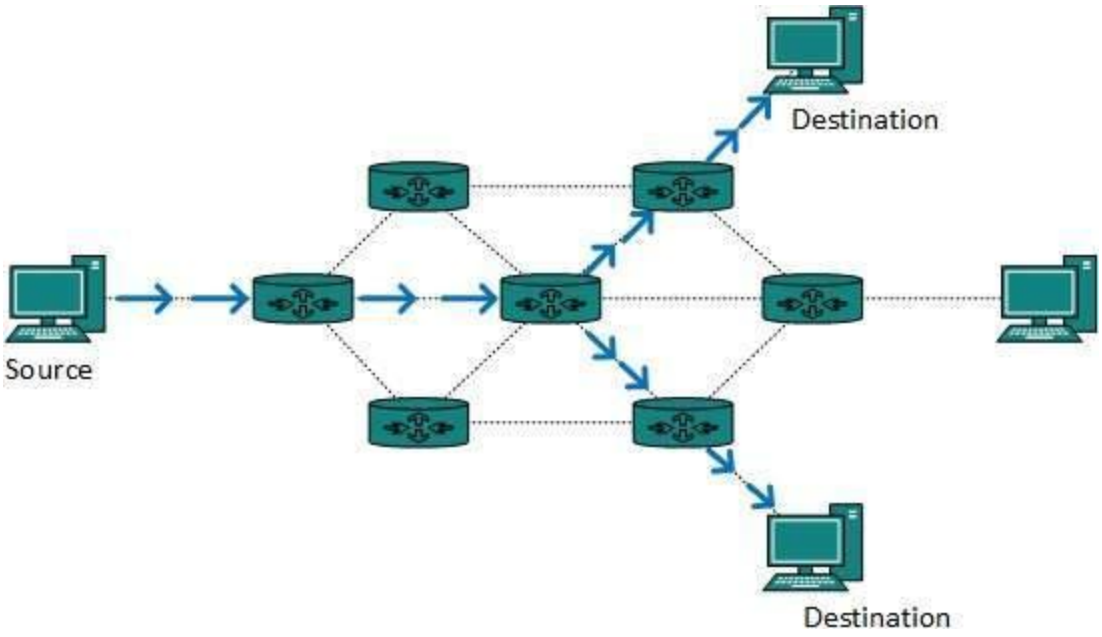


  This method is easy on router's CPU but may cause the problem of duplicate packets received from peer routers.

  Reverse path forwarding is a technique, in which router knows in advance about its predecessor from where it should receive broadcast. This technique is used to detect and discard duplicates.

Multicast Routing

Multicast routing is special case of broadcast routing with significance difference and challenges. In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing, the data is sent to only nodes which wants to receive the packets.

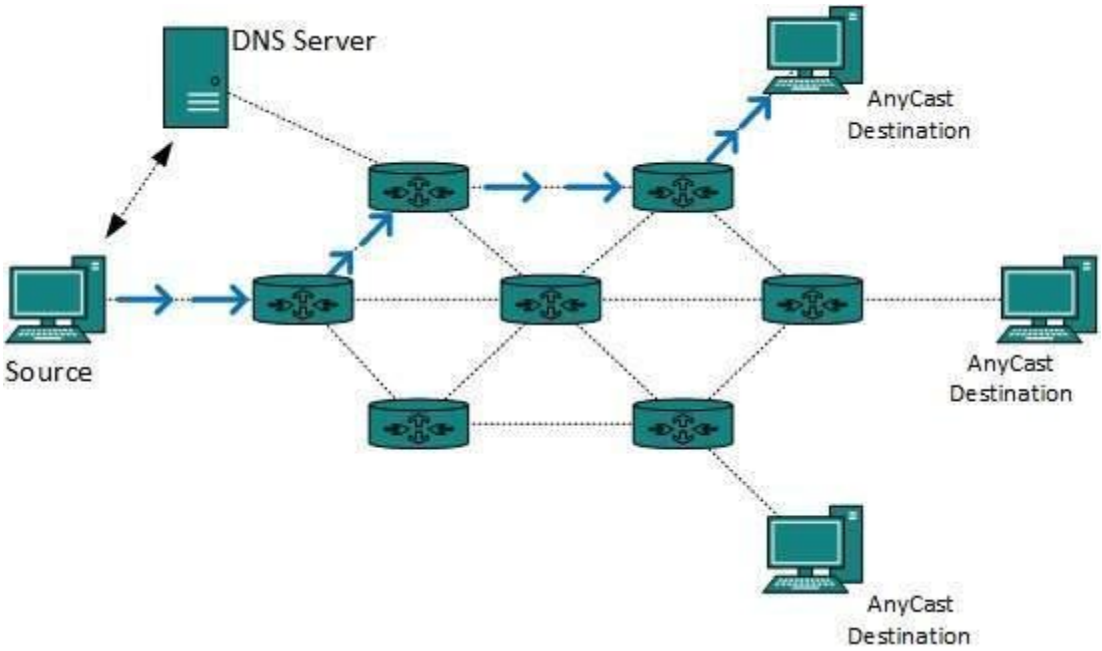


The router must know that there are nodes, which wish to receive multicast packets (or stream) then only it should forward. Multicast routing works spanning tree protocol to avoid looping.

Multicast routing also uses reverse path Forwarding technique, to detect and discard duplicates and loops.

Anycast Routing

Anycast packet forwarding is a mechanism where multiple hosts can have same logical address. When a packet destined to this logical address is received, it is sent to the host which is nearest in routing topology.



Anycast routing is done with help of DNS server. Whenever an Anycast packet is received it is enquired with DNS to where to send it. DNS provides the IP address which is the nearest IP configured on it.

What is congestion?

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 in a network may occur when the load on the network (i.e. the number of packets sent to the network) is greater than the capacity of the network (i.e. the number of packets a network can handle.)

Causes of Network Congestion – And How to Prevent Them

i. The input traffic rate exceeds the capacity of the output lines.

ii. The routers are too slow to perform bookkeeping tasks (queuing buffers, updating tables, etc.).

iii. The routers' buffer is too limited.

iv. Congestion in a subnet can occur if the processors are slow. Slow speed CPU at routers will perform the routine tasks such as queuing buffers, updating table etc slowly.

v. Outdated or non-compatible hardware

vi. Too many devices
vii. Bandwidth hogs

viii. Poor network design and subnets

Congestion control

Congestion Control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. Congestion control mechanisms are divided into two categories, one category prevents the congestion from happening and the other category removes congestion after it has taken place.

It is 2 types

1. Open Loop Congestion Control

2.Closed Loop Congestion Control

1. Open Loop Congestion Control

i. In this method, policies are used to prevent the congestion before it happens.

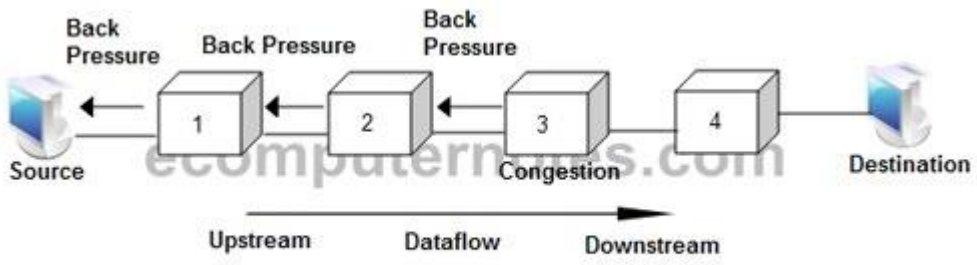
ii. Congestion control is handled either by the source or by the destination.

2.Closed Loop Congestion Control

Closed loop congestion control mechanisms try to remove the congestion after it happens.The various methods used for closed loop congestion control are:

i. Backpressure

a. Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow.



Backpressure Method

b. The backpressure technique can be applied only to virtual circuit networks. In such virtual circuit each node knows the upstream node from which a data flow is coming.

c. In this method of congestion control, the congested node stops receiving data from the immediate upstream node or nodes.

d. This may cause the upstream node on nodes to become congested, and they, in turn, reject data from their upstream node or nodes.

e. As shown in fig node 3 is congested and it stops receiving packets and informs its upstream node 2 to slow down. Node 2 in turns may be congested and informs node 1 to slow down. Now node 1 may create congestion and informs the source node to slow down. In this way the congestion is alleviated. Thus, the pressure on node 3 is moved backward to the source to remove the congestion.

ii. Choke Packet a. 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.

b. Here, congested node does not inform its upstream node about the congestion as in backpressure method.

c. 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.

iii. Implicit Signaling

a. In implicit signaling, there is no communication between the congested node or nodes and the source.

b. 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.

c. On sensing this congestion, the source slows down.

d. This type of congestion control policy is used by TCP.

iv. Explicit Signaling

a. In this method, the congested nodes explicitly send a signal to the source or destination to inform about the congestion.

b. 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 .

c. Explicit signaling can occur in either the forward direction or the backward direction .

d. 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.

e. 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.

Difference between Flow Control and Congestion Control

Both **Flow Control** and **Congestion Control** are the traffic controlling methods in different situations.
The main difference between flow control and congestion control is that, In flow control, Traffics are controlled which are flow from sender to a receiver. On the other hand, In congestion control, Traffics are controlled entering to the network.

S.NO	Flow Control	Congestion Control
1.	In flow control, Traffics are controlled which are flow from sender to a receiver.	In this, Traffics are controlled entering to the network.
2.	Data link layer and Transport layer handle it.	Network layer and Transport layer handle it.
3.	In this, Receiver's data is prevented from being overwhelmed.	In this, Network is prevented from congestion.

4.	In flow control, Only sender is responsible for the traffic.	In this, Transport layer is responsible for the traffic.
5.	In this, Traffic is prevented by slowly sending by the sender.	In this, Traffic is prevented by slowly transmitting by the transport layer.
6.	In flow control, buffer overrun is restrained in the receiver.	In congestion control, buffer overrun is restrained in the intermediate systems in the network.

IP protocol (IPV4):

The Internet Protocol version 4 (IPv4) is a delivery mechanism used by the TCP/IP protocols. IPv4 is an unreliable and connectionless datagram protocol- which operates on a best effort delivery model. The term best-effort means that IPv4 provides no error control or flow control.

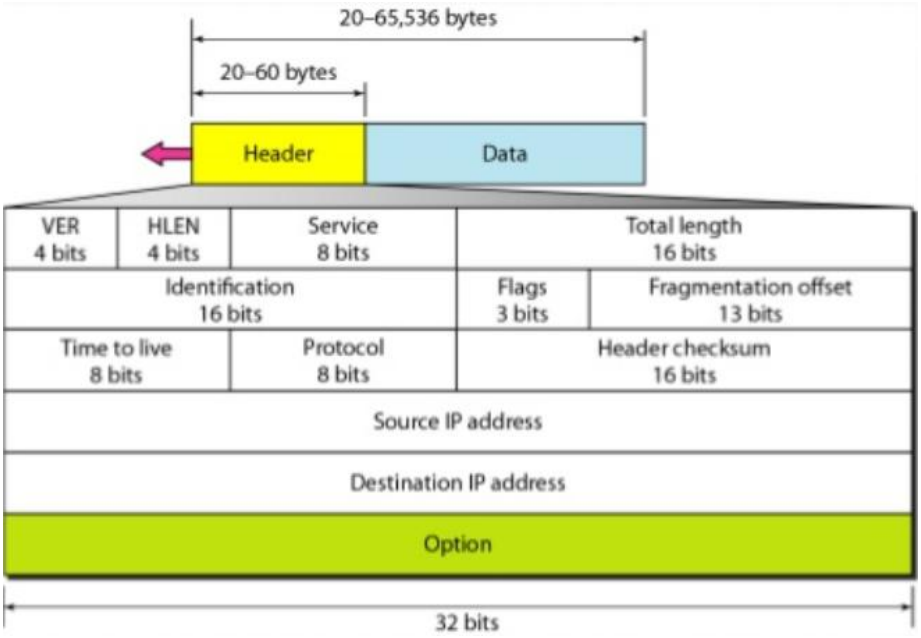
If reliability is important, IPv4 must be paired with a reliable protocol such as TCP.

IPv4 uses 32-bit (4 bytes) addressing, which gives 2^{32} addresses.

IPv4 addresses are written in the dot-decimal notation, which comprises of four octets of the address expressed individually in decimal and separated by periods, for instance, 192.168.1.5.

IPv4 Datagram Header

IPv4 is a connectionless protocol for a packet- switching network that uses the datagram approach. This means that each datagram is handled independently, and each datagram can follow a different route to the destination.



Packets in the IPv4 layer are called datagrams. A datagram is a variable-length packet consisting of two parts: header and data. The header is 20 to 60 bytes in length and contains information essential to routing.

- **Version (VER):** This 4-bit field defines the version of the IPv4 protocol. Currently, the version is 4. However, version 6 (or IPng) may totally replace version 4 in the future.

- **Header length (HLEN):** This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes).

- **Services:** IETF has changed the interpretation and name of this 8-bit field. This field, previously called service type, is now called differentiated services.

- **Type of service:** Low Delay, High Throughput, Reliability (8 bits)

- **Total Length:** Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes

- **Identification:** Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)

- **Flags:** 3 flags of 1 bit each: reserved bit (must be zero), do not fragment flag, more fragments flag (same order)

- **Fragment Offset:** Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes

- **Time to live:** Datagram's lifetime (8 bits), It prevents the datagram to loop in the network

- **Protocol:** Name of the protocol to which the data is to be passed (8 bits)

- **Header Checksum:** 16 bits header checksum for checking errors in the datagram header

- **Source IP address:** 32 bits IP address of the sender

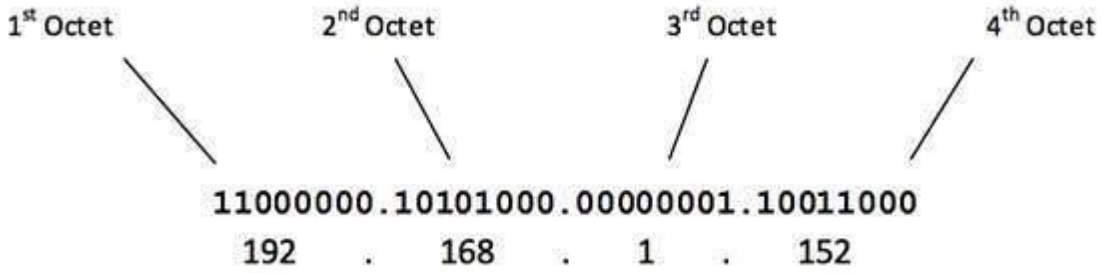
- **Destination IP address:** 32 bits IP address of the receiver

- **Option:** Optional information such as source route. Due to the presence of options, the size of the datagram header can be of variable length (20 bytes to 60 bytes).

Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address.

Internet Corporation for Assigned Names and Numbers is responsible for assigning IP addresses.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address −



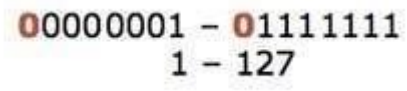
The number of networks and the number of hosts per class can be derived by this formula −

Number of networks	= 2^network_bits
Number of Hosts/Network	= 2^host_bits − 2

When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.



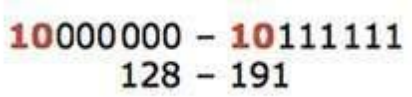
Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).

Class A IP address format is thus: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B Address

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.



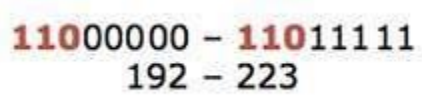
Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses.

Class B IP address format is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

Class C Address

The first octet of Class C IP address has its first 3 bits set to 110, that is −



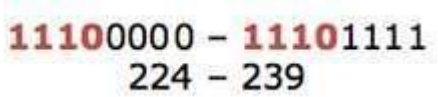
Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

Class C gives 2097152 (2^{21}) Network addresses and 254 (2^8-2) Host addresses.

Class C IP address format is: **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH

Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of −



Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E Address

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.