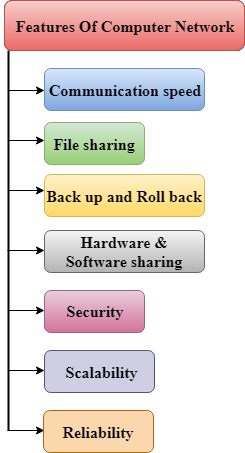
Computer Network BIT373CO

# 1. Network concepts, classification and components [7Hrs]

## a. Introduction, features and advantages of network, networking criteria

Computer network is defined as a set of interconnected autonomous systems that facilitate distributed processing of information. It results in better performance with high speed of processing.



* Communication speed

Network provides us to communicate over the network in a fast and efficient manner. For example, we can do video conferencing, email messaging, etc. over the internet. Therefore, the computer network is a great way to share our knowledge and ideas.

* File sharing

File sharing is one of the major advantages of the computer network. Computer network provides us to share the files with each other.

* Backup and Rollback is easy

Since the files are stored in the main server which is centrally located. Therefore, it is easy to take the back up from the main server.

* Software and Hardware sharing

We can install the applications on the main server, therefore, the user can access the applications centrally. So, we do not need to install the software on every machine. Similarly, hardware can also be shared.

* Security

Network allows security by ensuring that the user has the right to access certain files and applications.

* Scalability

Scalability means that we can add the new components on the network. Network must be scalable so that we can extend the network by adding new devices. But, it decreases the speed of the connection and data of the transmission speed also decreases, this increases the chances of error occurring. This problem can be overcome by using the routing or switching devices.

* Reliability

Computer networks can use the alternative source for the data communication in case of any hardware failure.

Advantages of Network:

These are main advantages of Computer Networks:

* Central Storage of Data –

Files can be stored on a central node (the file server) that can be shared and made available to each and every user in an organization.

* Anyone can connect to a computer network –

There is a negligible range of abilities required to connect to a modern computer network. The effortlessness of joining makes it workable for even youthful kids to start exploiting the data.

* Faster Problem solving –

Since an extensive procedure is disintegrated into a few littler procedures and each is taken care of by all the associated gadgets, an explicit issue can be settled in less time.

* Reliability –

Reliability implies backing up of information. Due to some reason equipment crash, and so on, the information gets undermined or inaccessible on one PC, another duplicate of similar information is accessible on another workstation for future use, which prompts smooth working and further handling without interruption.

* It is highly flexible –

This innovation is known to be truly adaptable, as it offers clients the chance to investigate everything about fundamental things, for example, programming without influencing their usefulness.

* Security through Authorization –

Security and protection of information is additionally settled through the system. As just the system clients are approved to get to specific records or applications, no other individual can crack the protection or security of information.

* It boosts storage capacity –

Since you will share data, records and assets to other individuals, you need to guarantee all information and substance are legitimately put away in the framework. With this systems administration innovation, you can do the majority of this with no issue, while having all the space you requirement for capacity.

Disadvantages of Network:

These are main disadvantages of Computer Networks:

* It lacks robustness –

If a PC system’s principle server separates, the whole framework would end up futile. Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill. To manage these issues, gigantic systems ought to have a ground-breaking PC to fill in as a document server to influence setting up and keeping up the system less demanding.

* It lacks independence –

PC organizing includes a procedure that is worked utilizing PCs, so individuals will depend on a greater amount of PC work, rather than applying an exertion for their jobs that needs to be done. Beside this, they will be subject to the primary document server, which implies that, in the event that it separates, the framework would end up futile, making clients inactive.

* Virus and Malware –

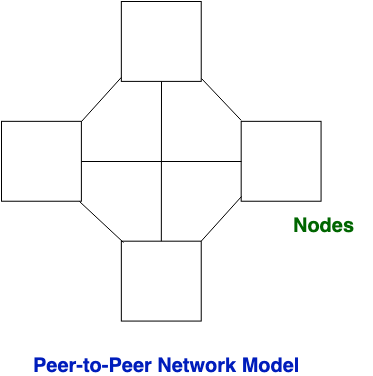
On the off chance that even one PC on a system gets contaminated with an infection, there is a possibility for alternate frameworks to get tainted as well. Infections can spread on a system effectively, in view of the between availability of different gadgets.4. Lack of Independence

* Cost of network –

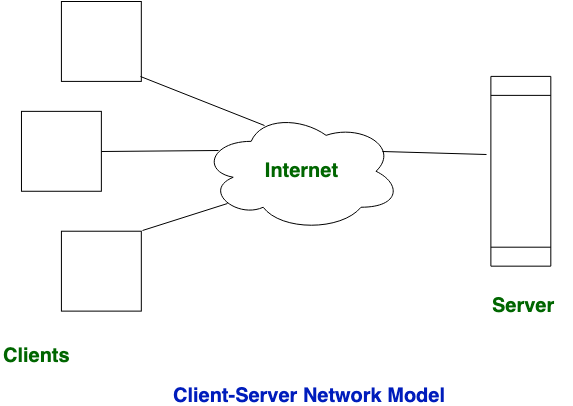
The expense of executing the system including cabling and equipment can be expensive.

## b. Types of network (LAN, MAN, WAN, Peer to Peer model, Client/Server model)

* 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 quite expensive and a single organization may not have its own it.
* WAN - Wide Area Network
  + A Wide Area Network (WAN) is a much larger network than LAN and MAN. It often covers multiple countries or continents. It is quite expensive and a single organization may not have its own it. Satellites are used to manage WAN.
* Peer to Peer model
  + This model does not differentiate the clients and the servers, In this each and every node is itself client and server. In Peer-to-Peer Network, Each and every node can do both request and response for the services.



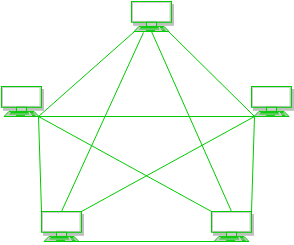
* Client/Server model
  + This model is a broadly used network model. In Client-Server Network, Clients and server are differentiated, Specific server and clients are present. In Client-Server Network, Centralized server is used to store the data because its management is centralized.In Client-Server Network, Server responds to the services which are requested by Client.



## c. LAN topologies (Bus, Ring, Star, Hybrid, etc)

a) Mesh Topology :

In mesh topology, every device is connected to another device via a particular channel.



Advantages of this topology :

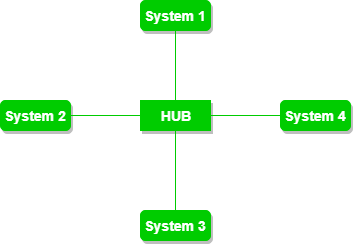
* It is robust.
* Fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
* Provides security and privacy.

Problems with this topology :

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

b) Star Topology :

In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Advantages of this topology :

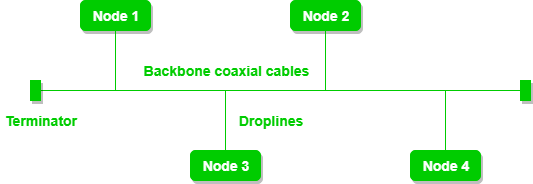
* If N devices are connected to each other in star topology, then the number of cables required to connect them is N. So, it is easy to set up.
* Each device requires only 1 port i.e. to connect to the hub.

Problems with this topology :

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

c) Bus Topology :

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



Advantages of this topology :

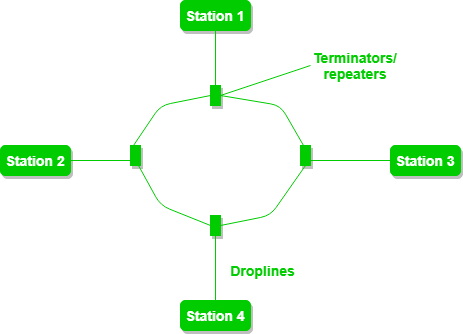
* If N devices are connected to each other in bus topology, then the number of cables required to connect them is 1 which is known as backbone cable and N drop lines are required.
* Cost of the cable is less as compared to other topologies, but it is used to build small networks.

Problems with this topology :

* If the common cable fails, then the whole system will crash down.
* If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in MAC layers known as Pure Aloha, Slotted Aloha, CSMA/CD etc.

d) Ring Topology :

In this topology, it forms a ring connecting devices with its exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.



Advantages of this topology :

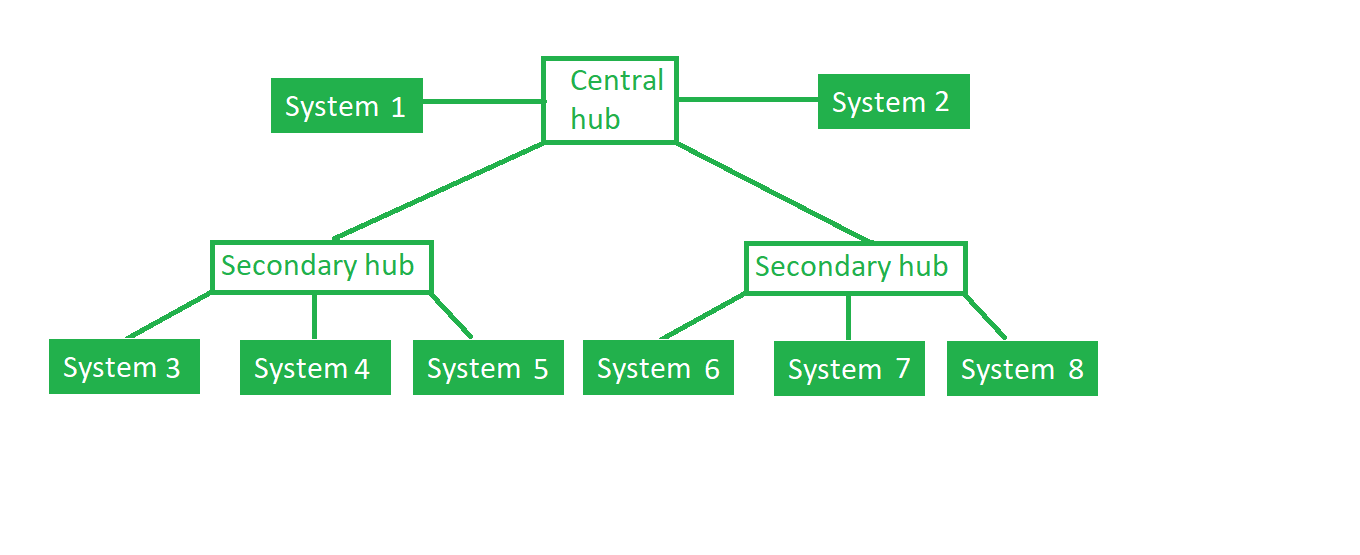
* The possibility of collision is minimum in this type of topology.
* Cheap to install and expand.

Problems with this topology :

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

e) Tree Topology :

This topology is the variation of Star topology. This topology has hierarchical flow of data.



Advantages of this topology :

* It allows more devices to be attached to a single central hub thus it increases the distance that is traveled by the signal to come to the devices.
* It allows the network to isolate and also prioritize from different computers.

Problems with this topology :

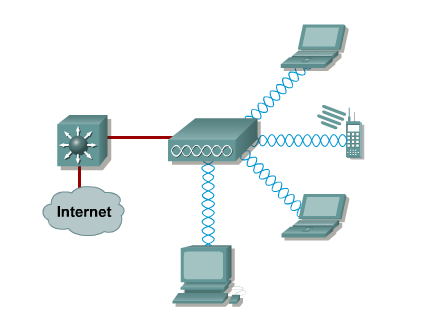
* If the central hub fails the entire system fails.
* The cost is high because of cabling.

## d. Wireless networks (Bluetooth, Wifi, WiMax, etc)

Wireless LAN (WLAN)/ WiFi (802.11)

Wireless LANs (WLAN) are similar to Ethernet networks in many ways. A WLAN is a shared network. The access point is a shared device and functions like a shared Ethernet hub. In the wireless cell, only one station can transmit at any time; all other stations listen. A station that wants to transmit must wait until the wireless media is not in use by another station. This transmission setup is similar to that of a coaxial cable or half-duplex Ethernet and an Ethernet hub. The average data rate per station is total bandwidth divided by the number of stations. The actual data throughput experienced by the wireless clients is even less because of wireless-specific issues.

In WLANs, data is transmitted over radio waves. WLAN signals use the same frequency for transmitting and receiving (half-duplex); therefore, a station cannot receive while it is transmitting. This is similar to coaxial cable Ethernet.



## e. Circuit switching, packet switching and message switching networks

Circuit Switching / Connection Oriented Internet-Working

1. Primarily designed for telephone lines which were not highbvc blessings;   
   Three phases: Connection Establishment, Data Transfer and Connection Termination.
2. During the connection establishment phase, a fixed path and required resources are reserved.
3. After connection setup, data is transferred. All data travel through the same path.
4. At the connection termination phase all reserved resources are freed.
5. It has the following advantages:

* Guaranteed Bandwidth: Resources are reserved beforehand.
* Low Overhead: No TCP or IP header needs to be sent.
* Simple Forwarding: No need to inspect the header to find the o/p port.

1. It has the following drawbacks:

* Wasted bandwidth: Reserved bandwidth means the link can't be used even if there is no traffic flowing.
* Blocked Connections: No new connections are set-up if the system can't reserve the resources.
* Connection set-up delay.

Packet Switching / Connectionless Interworking

1. Invented to overcome the drawbacks of Circuit Switching.
2. Here, data are divided into small chunks called packets and routed independently of others so different packets may take different paths.
3. It has the following benefits:

* Full use of available bandwidth.
* Devices of different speeds can communicate over the same link.
* High Availability: No waiting time for connection establishment.
* Redundancy: Packets can be routed via alternate router even if a link fails.

1. The main drawbacks are:

* Possible data loss or corruption due to congestion.
* Extra protocols are needed for reliable transfer.
* Long delay in case of high load.

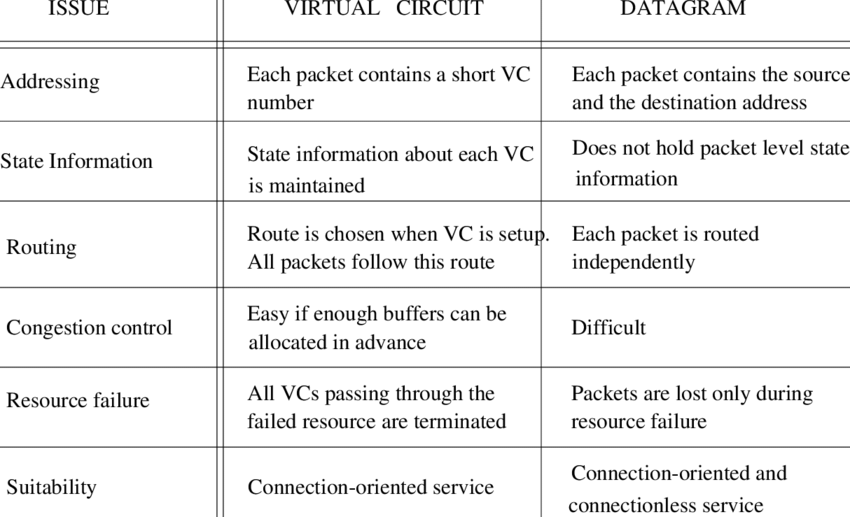
Packet switching are divided into two types:

1. Virtual Circuit Method

* In this method first a connection is established to the reserver resource (bandwidth) between the source, the intermediate paths and destination.
* Similar to circuit switching after the connection is established.
* All packets are then sent through this fixed path.
* Since all packets take the same path, packets arrive in order.

1. Datagram Method

* Here the individual packets are sent independently to each other.
* Packets may take different path and hence can arrive out of order

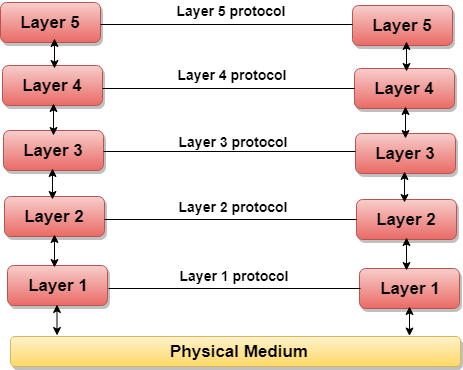
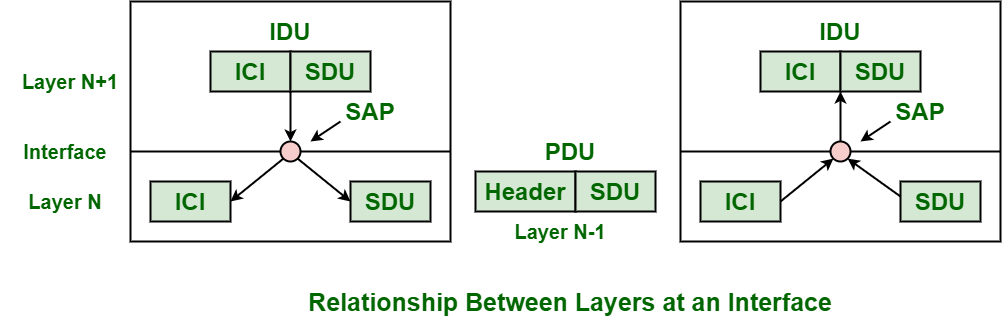


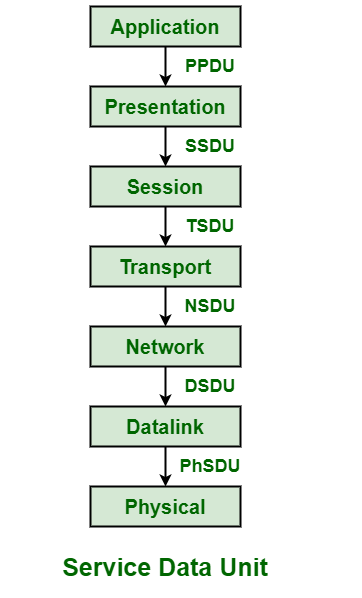
## f. Network components (NIC, bridge, repeater, Hub, Switch, Router, Gateway)

Computer network components are the major parts which are needed to install the software. Some important network components are NIC, switch, cable, hub, router, and modem. Depending on the type of network that we need to install, some network components can also be removed.

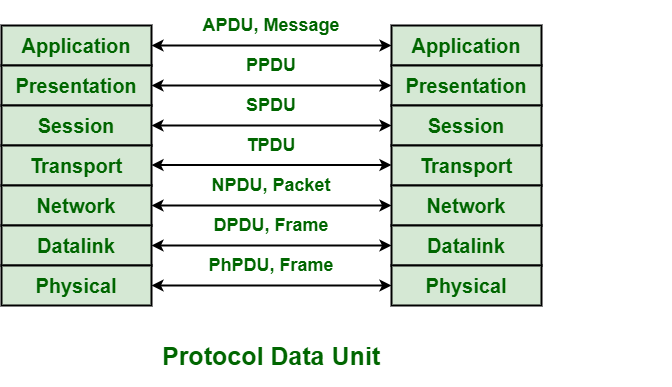
* NIC
  + NIC stands for network interface card.
  + NIC is a hardware component used to connect a computer with another computer onto a network
  + It can support a transfer rate of 10,100 to 1000 Mb/s.
  + The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).
* Bridge
  + A bridge operates at a data link layer.
  + A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.
* Repeater
  + A repeater operates at the physical layer.
  + Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.
  + It is a two port device.
* Hub
  + A Hub is a hardware device that divides the network connection among multiple devices.
  + When a computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.
  + The process used by the Hub consumes more bandwidth and limits the amount of communication.
* Switch
  + A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub.
  + A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination.
* Router
  + A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.
  + A router works in a Layer 3 (Network layer) of the OSI Reference model.
  + A router forwards the packet based on the information available in the routing table.
  + It determines the best path from the available paths for the transmission of the packet.
* Gateway
  + It is a passage to connect two networks together that may work upon different networking models.
  + They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.
  + Gateways are also called protocol converters and can operate at any network layer.

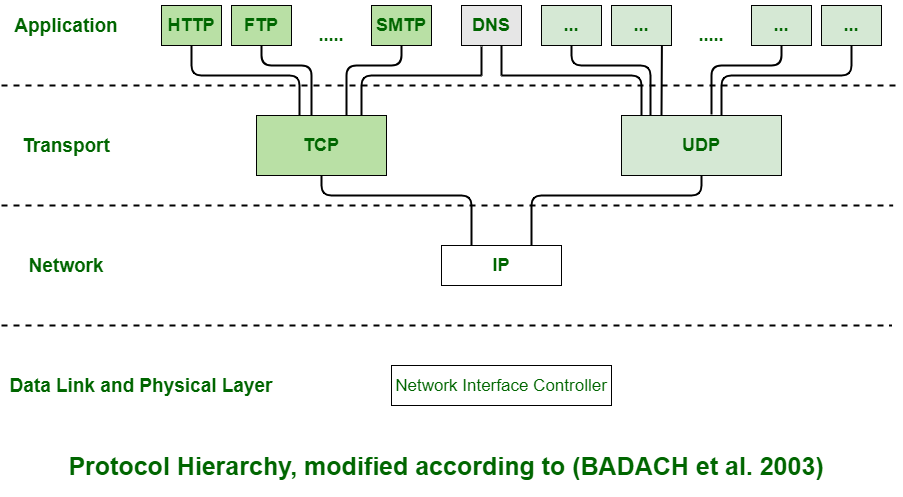
## g. Layered architecture, interfaces, services and protocol hierarchies.

* Layered architecture:
  + The main aim of the layered architecture is to divide the design into small pieces.
  + Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
  + It provides modularity and clear interfaces, i.e., provides interaction between subsystems.
  + It ensures the independence between layers by providing the services from lower to higher layers without defining how the services are implemented. Therefore, any modification in a layer will not affect the other layers.
  + The number of layers, functions, contents of each layer will vary from network to network. However, the purpose of each layer is to provide the service from lower to a higher layer and hiding the details from the layers of how the services are implemented.
  + The basic elements of layered architecture are services, protocols, and interfaces.
    - Service: It is a set of actions that a layer provides to the higher layer.
    - Protocol: It defines a set of rules that a layer uses to exchange the information with a peer entity. These rules mainly concern both the contents and order of the messages used.
    - Interface: It is a way through which the message is transferred from one layer to another layer.
  + In a layer n architecture, layer n on one machine will have a communication with the layer n on another machine and the rules used in a conversation are known as a layer-n protocol.
  + 
  + In case of layered architecture, no data is transferred from layer n of one machine to layer n of another machine. Instead, each layer passes the data to the layer immediately just below it, until the lowest layer is reached.
  + Below layer 1 is the physical medium through which the actual communication takes place.
  + In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.
  + The data is passed from the upper layer to lower layer through an interface. A Layered architecture provides a clean-cut interface so that minimum information is shared among different layers. It also ensures that the implementation of one layer can be easily replaced by another implementation.
  + A set of layers and protocols is known as network architecture.
* Interface and services:
  + Interfaces and Services is a process that generally provides and gives a common technique for each layer to communicate with each other. Standard terminology basically required for layered networks to request and aim for the services are provided.
  + Service is defined as a set of primitive operations. Services are provided by layer to each of layers above it.
  + Below is a diagram showing the relation between layers at an interface. In the diagram, layers N+1, N, and N-1 are involved and engaged in the process of communication among each other.
  + 
  + Components and its functions:
    - Service Data Unit (SDU):
      * SDU is a piece of information or data that is generally passed by layer just above current layer for transmission. Unit of data or information is passed down to a lower layer from an OSI (Open System Interconnection) layer or sublayer. Data is passed with a request to transmit data. SDU basically identifies or determines information that has been transferred among entities of peer layers that are not interpreted by supporting entities of lower-layer.

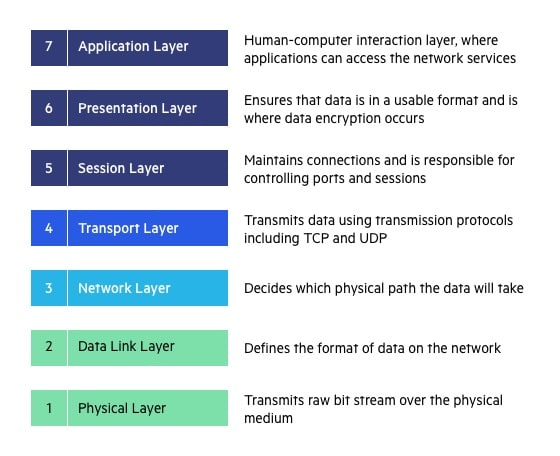


* + - Protocol Data Unit (PDU)
      * PDU is a single unit of information or data that is transmitted or transferred among entities of peer layers of a computer network. When application data is passed down to the protocol stack on its way to being transmitted all over network media, some protocols add information and data to it at each and every level. PDU is used to represent and describe data as it gets transferred from one layer of OSI model to another layer.



* + - Interface Data Unit (IDU)
      * IDU is used to have an agreed way of communication among two layers in a network layered architecture. It is passed from (N+1 to N).
    - Service Access Point (SAP)
      * SAP is generally used as an identifier label for endpoints of a network in OSI networking or model. It is a data structure and identifier also for a buffer area in memory of the system. It is a point in a layer of a layered architecture where a network is usually provided and where layer just above layer that provides service can probably have access to it.
    - Interface Control Information (ICI)
      * ICI is a temporary parameter that is passed between N and N-1 layers to include service functions among two layers.
* Protocol hierarchies:
  + Generally, Computer networks are composed of or contain a large number of pieces of hardware and software. To just simplify network design, various networks are organized and arranged as a stack of layers of hardware and software, one on top of another. The number, name, content, and function of each layer might vary and can be different from one network to another. The main purpose of each of the layers is just to offer and provide services to higher layers that are present. Each and every layer has some particular task or function. The networks are organized and arranged as different layers or levels simply to reduce and minimize complexity of design of network software.
  + 
  + Advantages :
    - The layers generally reduce complexity of communication between networks
    - It increases network lifetime.
    - It also uses energy efficiently.
    - It does not require overall knowledge and understanding of the network.

## h. ISO-OSI Reference model



OSI Model  
In the OSI reference model, there are seven layers. The purpose of each of the seven layers in the model is to carry out part of the communication process in a well-defined way. This is achieved in a hierarchical fashion; i.e. the higher layers request the services of the lower layers to carry out their functions. Data travels across the network and is passed from layer to layer until the lowest layer is reached. Actual physical communication takes place at the lowest layer and is passed up through the layers to the highest layer and from there to the user.

Layer 1: Physical Layer

The physical layer is mainly concerned with the transmission of data over a communications link, i.e. a telephone cable or LAN cable. The function of the Physical Layer is to provide ''mechanical, electrical, functional, and procedural means to activate a physical connection for bit transmission'' (ISO/IEC 7498: 1984). Basically, this means that the typical role of the physical layer is to Transform bits in a computer system into electromagnetic (or equivalent) signals for a particular transmission medium (wire, fiber, ether, etc.). Repeaters operate at this level.

Layer 2 : The Data Link Layer

This layer attempts to make the physical layer reliable for the transmission of data. It provides synchronization and error Detection control, which allows the upper layers to assume error-free transmission over the link. Data received from the Network Layer is formatted into frames and sent to the Physical Layer for transmission. Bridges and switches operate at this level and use the machine's MAC address to filter traffic.

Layer 3 : The Network Layer

The network layer relieves the higher layers of the routing, switching and signaling functions required to establish the necessary physical network links .It accepts data from layer 4 and selects the best route to transfer it between end systems. The computer communicates with the network at this layer to specify the destination address and to request network facilities such as priority. The IP protocol is used at this level for packet forwarding routing. Routers are used at this level. They use packet addresses to choose the optimum route across the network.

Layer 4 : The Transport Layer

The transport layer ensures reliable, cost effective, end to end transfer of data. Like the data link layer, the transport layer has error control functions. Whereas the data link layer was concerned with the traffic across physical links, the transport layer is concerned with traffic between the layers. This layer provides a data transfer service, which shields the upper layers from any concern with the detailed way in which data is transferred.

Layer 5 : The Session Layer

The Session Layer permits two parties to hold ongoing communications called a session across a network. It provides dialogue control, which is the setting up and monitoring of connections. If the lower four layers of the model are unreliable, the session layer will attempt to correct the faults and maintain the connection with the higher layers becoming aware of any problem. Thus the applications on either end of the session can exchange data or send packets to another for as long as the session lasts. The Session layer handles session setup, data or message exchanges, and teardown when the session ends. It also monitors session identification so only designated parties can participate and security services to control access to session information.

Layer 6 : The Presentation Layer

The presentation layer defines the format and representation of the data exchanged between users. Video displays and printers may use different data formats. Without this layer these different formats would require individual treatment. Data Encryption and compression, and Code and format conversions are some of the facilities offered by this layer. For outgoing messages, it converts data into a generic format that can survive the rigors of network transmission; for incoming messages, it converts data from its generic networked representation into a format that will make sense to the receiving application.

Layer 7 : The Application Layer

The Application Layer is the top layer of the reference model. It provides a set of interfaces to allow equipment and application programs to exchange information in the OSI environment. It is the source of all data to be transferred including services such as networked file transfer, message handling, and database query processing. Gateways work at this level.

**Similarity between OSI and TCP/IP model**

1. Both are the logical models.
2. Both define standards for networking.
3. Both provide a framework for creating and implementing networking standards and devices.
4. Both divide the network communication process in layers.
5. In both models, a single layer defines a particular functionality and sets standards for that functionality only.
6. Both models simplify troubleshooting processes by dividing complex functions into simpler components.

**Differentiate between OSI and TCP/IP model**

1. The OSI Layer model has seven layers while the TCP/IP model has four layers.
2. The OSI Layer model is no longer used while TCP/IP is still used in computer networking.
3. To define the functionality of upper layers, OSI uses three separate layers (application, presentation and session) while TCP/IP uses a single layer (application).
4. Just like upper layers, OSI uses two separate layers (Physical and Data link) to define the functionality of bottom layers while TCP/IP uses a single layer (Link) for the same.
5. To define the routing protocols and standards, OSI uses Network layer while TCP/IP uses Internet layer.
6. In comparison to TCP/IP model, OSI model is well documented and explains standards and protocols in more detail.

# 2. Data communication and services [8 Hrs]

## a. Concepts of data, signal, channel and circuits, channel speed and bandwidth, throughput, bit rate and baud rate, maximum data rate of a channel, propagation time, transmission time.

* Data:
  + Data is information processed or stored by a computer. This information may be in the form of text documents, images, audio clips, software programs, or other types of data.
* Signal:
  + Signals are the electric or electromagnetic impulses used to encode and transmit data.
* Channel and Circuits:
  + Physical medium like cables over which information is exchanged is called a channel. Transmission channels may be analog or digital. As the name suggests, analog channels transmit data using analog signals while digital channels transmit data using digital signals.
* Channel speed:
* Bandwidth:
  + Data transfer rates that can be supported by a network is called its bandwidth. It is measured in bits per second (bps). Modern day networks provide bandwidth in Kbps, Mbps and Gbps.
* Throughput:
  + Throughput is the actual speed with which data gets transferred over the network. Besides transmitting the actual data, network bandwidth is used for transmitting error messages, acknowledgement frames, etc.
* Bit rate:
  + bit rate is the number of bits that are conveyed or processed per unit of time.
* Baud rate:
  + The baud rate is the rate at which information is transferred in a communication channel.
* Maximum data rate of channel:
  + Data rate governs the speed of data transmission. A very important consideration in data communication is how fast we can send data, in bits per second, over a channel. Data rate depends upon 3 factors:
    - The bandwidth available
    - Number of levels in digital signal
    - The quality of the channel – level of noise
  + Two theoretical formulas were developed to calculate the data rate: one by Nyquist for a noiseless channel, another by Shannon for a noisy channel.
    - Noiseless Channel : Nyquist Bit Rate
      * For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate

| BitRate = 2 \* Bandwidth \* log2(L) |
| --- |

* + - * In the above equation, bandwidth is the bandwidth of the channel, L is the number of signal levels used to represent data, and BitRate is the bit rate in bits per second.

Bandwidth is a fixed quantity, so it cannot be changed. Hence, the data rate is directly proportional to the number of signal levels.

* + - Noisy Channel : Shannon Capacity
      * In reality, we cannot have a noiseless channel; the channel is always noisy. Shannon capacity is used, to determine the theoretical highest data rate for a noisy channel:

| Capacity = bandwidth \* log2(1 + SNR) |
| --- |

* + - * In the above equation, bandwidth is the bandwidth of the channel, SNR is the signal-to-noise ratio, and capacity is the capacity of the channel in bits per second.Bandwidth is a fixed quantity, so it cannot be changed. Hence, the channel capacity is directly proportional to the power of the signal, as SNR = (Power of signal) / (power of noise).The signal-to-noise ratio (S/N) is usually expressed in decibels (dB) given by the formula:

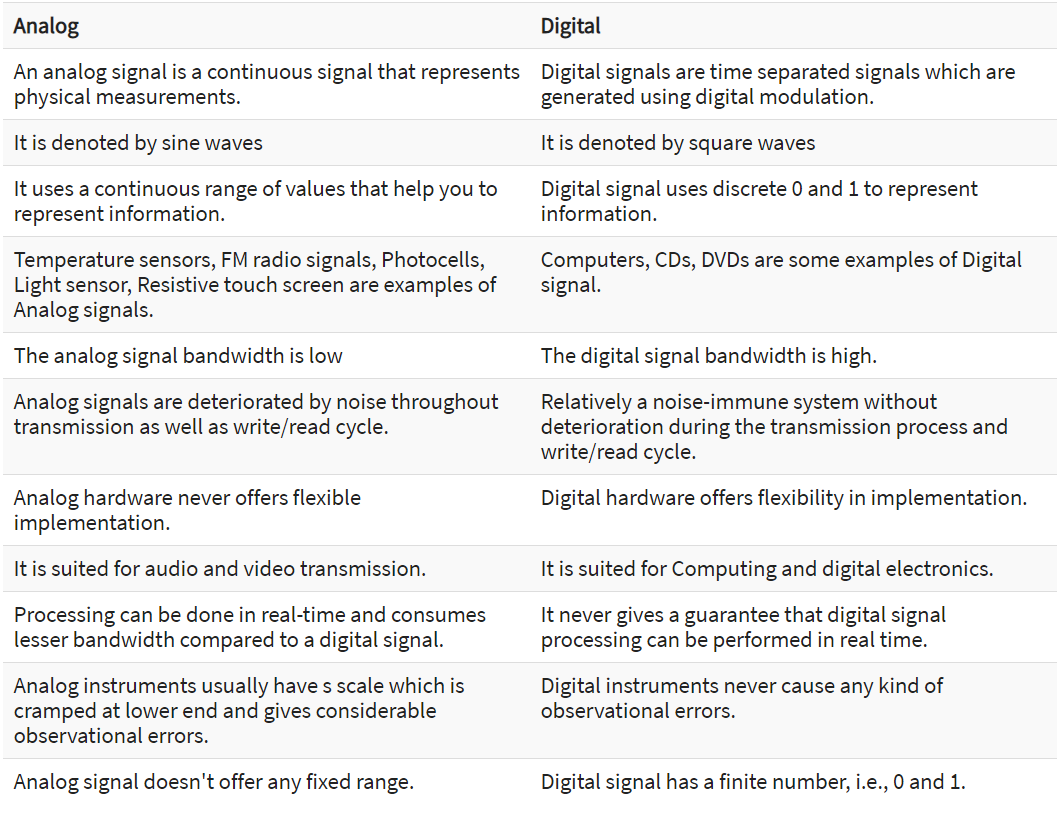
| 10 \* log10(S/N) |
| --- |

* Propagation time:
  + Propagation time The time required for a signal or wave to travel from one point of a transmission medium to another.
* Transmission time:
  + The transmission time is the amount of time from the beginning until the end of a message transmission.

## b. Analog and digital transmission

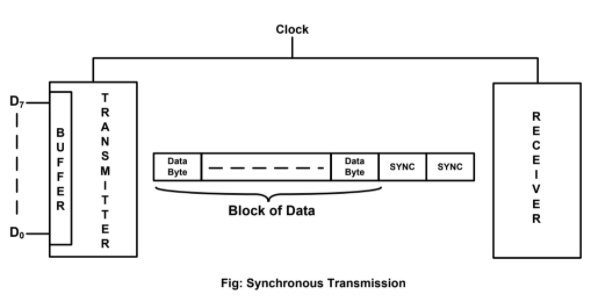
* Analog Transmission:
  + An analogue signal (otherwise known as a wave form) is characterised by being continuously variable along both amplitude and frequency. In the case of telephony, when we speak into a handset, our voice is converted into current, or voltage fluctuations. Those fluctuations in current are an analogue transmission of the actual voice pattern.
* Digital Transmission:
  + Digital signals are much simpler than analogue signals. Instead of a continuous waveform, analogue signals are made up of a series of pulses that represent either one bit or zero bits. Each computer system uses a coding scheme which defines what combinations of ones and zeros make up all the characters in the character set.

The data (ones and zeros) are carried throughout the network depending on whether it is an electrical or optical transmission system.



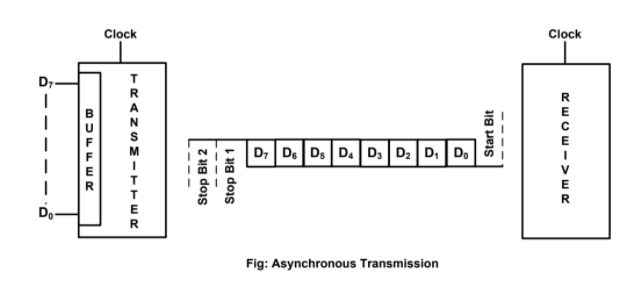
## c. Asynchronous and synchronous transmission

* Synchronous Transmission
  + The basic feature of synchronous data transmission is that the data is transmitted or received based on a clock signal and both the transmitter and receiver are synchronized with the common clock signal.
  + It is also called clock oriented transmission because all bytes of block are transmitted constantly. In this transmission, a block of data byte is transmitted along with the synchronization information.Usually, one or two SYNC character are used to indicate the start of each synchronous data stream as shown below:



At the receiver side, as soon as it matches one or two SYNC characters based on the number of SYNC characters used, the receiver starts interpreting the data. In synchronous transmission, the transmitting device needs to send data continuously to the receiving device. However, if data is not ready to be transmitted, the transmitter will send SYNC characters until the data is available.

* Asynchronous Transmission
  + In asynchronous data transmission, the transmitter and receiver need not to be synchronized with the common clock signal. It is also called character oriented transmission, because only one character is transmitted at a time. Each character carries a start bit and stop bits as synchronised information. Transmission begins with ont start but that is at logic 0, followed by required information byte, which is always transmitted with LSB first and finally the stop bits that are at logic 1. This formatting of data is known as Framing. Asynchronous data transmission is shown below with the framing information.



The asynchronous transmission is generally used in low speed transmission less than 20 Kbps, but asynchronous transmission transmits data greater than 20 kbps.

Each asynchronous serial data unit can be divided into equal time intervals called bit intervals. An 8-bit data will have 8 intervals. The format for asynchronous serial data contains the following information:

* A low START bit that indicated the beginning of the data to be transferred.
* 8 data bits, denoting the actual data being transferred
* An optional parity bit for either odd or even parity

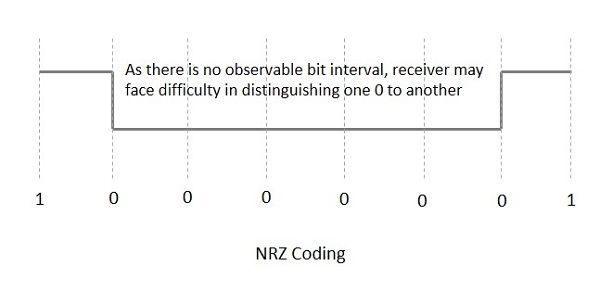
| S.NO | Synchronous Transmission | Asynchronous Transmission |
| --- | --- | --- |
| 1. | In Synchronous transmission, Data is sent in the form of blocks or frames. | In asynchronous transmission, Data is sent in form of byte or character. |
| 2. | Synchronous transmission is fast. | Asynchronous transmission is slow. |
| 3. | Synchronous transmission is costly. | Asynchronous transmission is economical. |
| 4. | In Synchronous transmission, the time interval of transmission is constant. | In asynchronous transmission, the time interval of transmission is not constant, it is random. |
| 5. | In Synchronous transmission, There is no gap present between data. | In asynchronous transmission, There is a present gap between data. |
| 6. | Efficient use of transmission lines is done in synchronous transmission. | While in asynchronous transmission, transmission line remains empty during gap in character transmission. |
| 7. | Synchronous transmission needs precisely synchronized clocks for the information of new bytes. | Asynchronous transmission have no need of synchronized clocks as parity bit is used in this transmission for information of new bytes. |

## d. Data encoding techniques

Encoding is the process of converting the data or a given sequence of characters, symbols, alphabets etc., into a specified format, for the secured transmission of data. Decoding is the reverse process of encoding which is to extract the information from the converted format.

The data encoding technique is divided into the following types, depending upon the type of data conversion.

* Analog data to Analog signals − The modulation techniques such as Amplitude Modulation, Frequency Modulation and Phase Modulation of analog signals, fall under this category.
* Analog data to Digital signals − This process can be termed as digitization, which is done by Pulse Code Modulation PCM. Hence, it is nothing but digital modulation. As we have already discussed, sampling and quantization are the important factors in this. Delta Modulation gives a better output than PCM.
* Digital data to Analog signals − The modulation techniques such as Amplitude Shift Keying ASK, Frequency Shift Keying FSK, Phase Shift Keying PSK, etc., fall under this category. These will be discussed in subsequent chapters.
* Digital data to Digital signals − These are in this section. There are several ways to map digital data to digital signals. Some of them are −
  + Non Return to Zero NRZ
    - NRZ Codes have 1 for High voltage level and 0 for Low voltage level. The main behavior of NRZ codes is that the voltage level remains constant during the bit interval. The end or start of a bit will not be indicated and it will maintain the same voltage state, if the value of the previous bit and the value of the present bit are the same.
    - The following figure explains the concept of NRZ coding.



If the above example is considered, as there is a long sequence of constant voltage levels and the clock synchronization may be lost due to the absence of bit intervals, it becomes difficult for the receiver to differentiate between 0 and 1.

* + NRZ - L NRZ–LEVEL
    - There is a change in the polarity of the signal, only when the incoming signal changes from 1 to 0 or from 0 to 1. It is the same as NRZ, however, the first bit of the input signal should have a change of polarity.
  + NRZ - I NRZ–INVERTED
    - If a 1 occurs at the incoming signal, then there occurs a transition at the beginning of the bit interval. For a 0 at the incoming signal, there is no transition at the beginning of the bit interval.
    - NRZ codes have a disadvantage that the synchronization of the transmitter clock with the receiver clock gets completely disturbed, when there is a string of 1s and 0s. Hence, a separate clock line needs to be provided.
* Bi-phase Encoding
  + The signal level is checked twice for every bit time, both initially and in the middle. Hence, the clock rate is double the data transfer rate and thus the modulation rate is also doubled. The clock is taken from the signal itself. The bandwidth required for this coding is greater.
  + There are two types of Bi-phase Encoding.
    - Bi-phase Manchester
      * In this type of coding, the transition is done at the middle of the bit-interval. The transition for the resultant pulse is from High to Low in the middle of the interval, for the input bit 1. While the transition is from Low to High for the input bit 0.
    - Differential Manchester
      * In this type of coding, there always occurs a transition in the middle of the bit interval. If there occurs a transition at the beginning of the bit interval, then the input bit is 0. If no transition occurs at the beginning of the bit interval, then the input bit is 1.
      * The following figure illustrates the waveforms of NRZ-L, NRZ-I, Bi-phase Manchester and Differential Manchester coding for different digital inputs.



## e. Multiplexing and demultiplexing

Multiplexing

1. Frequency Division Multiplexing (FDM)

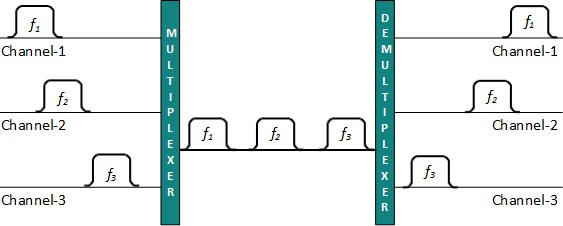
When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel. Each user can use the channel frequency independently and has exclusive access to it. All channels are divided such a way 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.

Advantages OF FDM

* Simple
* Inexpensive
* Popular with Radio, TV, Cable TV
* It is not sensitive to propagation delays.
* It allows maximum transmission link usage.

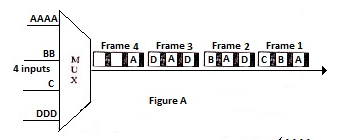
Disadvantages OF FDM

* In FDM there is a need for filters, which are very expensive and complicated to construct and design.
* Analog signal only has limited frequency range.
* Sometimes, it is necessary to use more complex linear amplifiers in FDM systems.



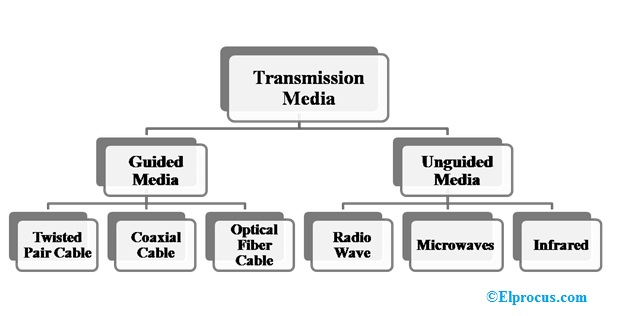
1. Time Division Multiplexing (TDM)

Time-division multiplexing (TDM) is a mechanism that allows multiple logical calls or streams to share the same physical circuit, providing an equal amount of time for each conversation. Instead of sharing a portion of the bandwidth as in FDM, here in TDM time is shared. Example: telephone system



## f. Transmission media

A communication channel that is used to carry the data from the transmitter to the receiver through the electromagnetic signals. The main function of this is to carry the data in the bits form through the Local Area Network (LAN). In data communication, it works like a physical path between the sender & the receiver. For instance, in a copper cable network the bits in the form of electrical signals whereas in a fiber network, the bits are available in the form of light pulses. The quality, as well as characteristics of data transmission, can be determined from the characteristics of medium & signal. The properties of different transmission media are delay, bandwidth, maintenance, cost, and easy installation.



## g. Guided: coaxial, twisted-pair, fiber-optic; unguided: radio, microwaves, infrared, VSAT

Guided Media:

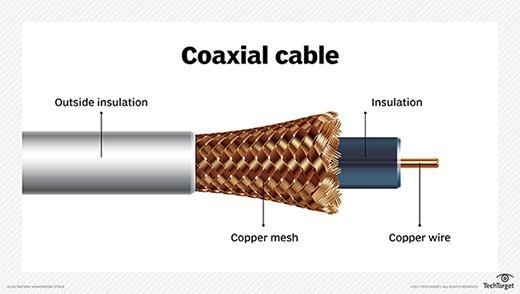
This kind of transmission media is also known as wired otherwise bounded media. In this type, the signals can be transmitted directly & restricted in a thin path through physical links.

The main features of guided media mainly include secure, high-speed, and used in small distances. This kind of media is classified into three types which are discussed below.

1. Coaxial Cable

This cable contains an external plastic cover and it includes two parallel conductors where each conductor includes a separate protection cover. This cable is used to transmit data in two modes like baseband mode as well as broadband mode. This cable is widely used in cable TVs & analog TV networks.

The advantages of the coaxial cable include high bandwidth, noise immunity is good, low cost and simple to install. The disadvantage of this cable is, the failure of cable can disturb the whole network



1. Twisted Pair Cable

It includes two separately protected conductor wires. Normally, some pairs of cables are packaged jointly in a protective cover. This is the most frequently used type of transmission media and it is available in two types.

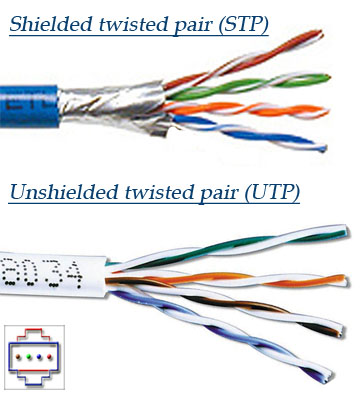
* UTP (Unshielded Twisted Pair)

This UTP cable has the capacity to block interference. It doesn’t depend on a physical guard and is used in telephonic applications. The advantage of UTP is a low cost, very simple to install, and high speed. The disadvantages of UTP is liability to exterior interference, transmitted in fewer distances, and less capacity.

* STP (Shielded Twisted Pair)

STP cable includes a particular jacket for blocking outside interference. It is used in rapid data rate Ethernet, in voice & data channels of telephone lines.

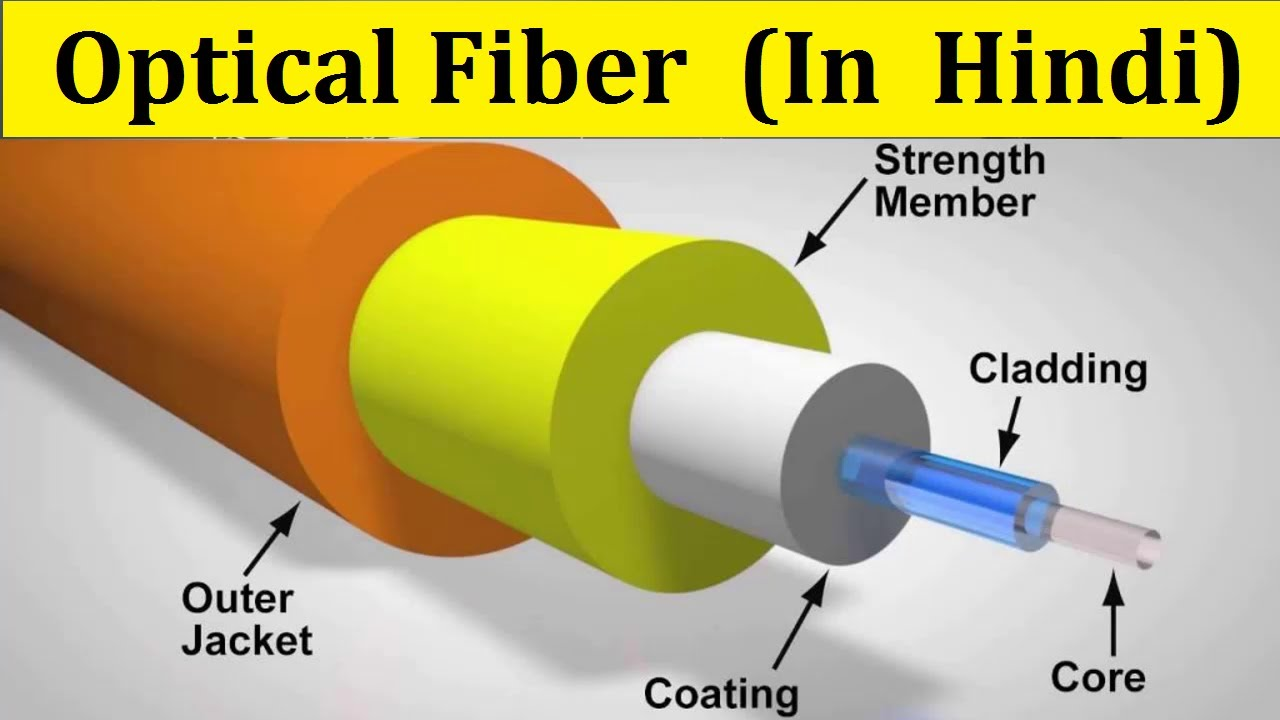
The main advantages of STP cable mainly include good speed, and removes crosstalk. The main disadvantages are hard to manufacture as well as install, It is expensive and bulky also



1. Optical Fibre Cable

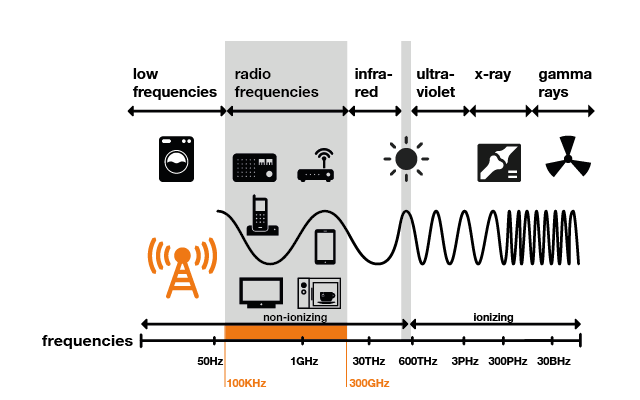
This cable uses the notion of light reflected through a core that is made with plastic or glass. The core is enclosed with less thick plastic or glass and it is known as the cladding, used for large volume data transmission.

The main advantages of this cable include lightweight, capacity & bandwidth will be increased, signal attenuation is less, etc. The disadvantages are high cost, fragile, installation & maintenance is difficult and unidirectional.



Unguided Media:

It is also known as unbounded otherwise wireless transmission media. It doesn’t require any physical medium to transmit electromagnetic signals. The main features of this media are less secure, the signal can be transmitted through air, and applicable for large distances. There are three types of unguided media which are discussed below.



1. Radio Waves

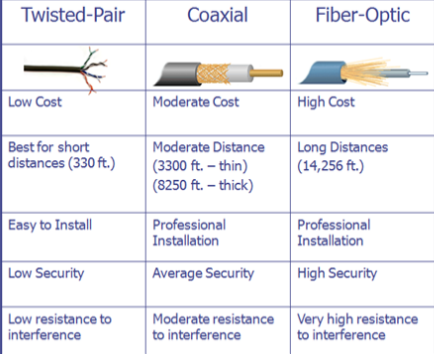
These waves are very easy to produce as well as penetrate through buildings. In this, the transmitting & receiving antennas no need to align. The frequency range of these waves ranges from 3 kHz to 1GHz. These waves are used in AM & Fm radios for transmission. These waves are classified into two types namely Terrestrial & Satellite.

1. Microwaves

It is a sightline transmission which means the transmitting & receiving antennas need to align correctly with each other. The distance which is covered through the signal can be directly proportional to the antenna’s height. The frequency range of microwaves ranges from 1GHz to 300GHz. These are extensively used in TV distribution & mobile phone communication

1. Infrared Waves

Infrared (IR) waves are used in extremely small distance communication as they cannot go through obstacles. So it stops intrusion between systems. The range of frequency of these waves is 300GHz to 400THz. These waves are used in TV remotes, keyboards, wireless mouse, printer, etc.



| Basis | Radiowave | Microwave | Infrared wave |
| --- | --- | --- | --- |
| Direction | These are omni-directional in nature. | These are unidirectional in nature. | These are unidirectional in nature. |
| Penetration | At low frequency, they can penetrate through solid objects and walls but high frequency they bounce off the obstacle. | At low frequency, they can penetrate through solid objects and walls. at high frequency, they cannot penetrate. | They cannot penetrate through any solid object and walls. |
| Frequency range | Frequency range: 3 KHz to 1GHz. | Frequency range: 1 GHz to 300 GHz. | Frequency range: 300 GHz to 400 GHz. |
| Security | These offer poor security. | These offer medium security. | These offer high security. |
| Attenuation | Attenuation is high. | Attenuation is variable. | Attenuation is low. |
| Government Licence | Some frequencies in the radio waves require a government license to use these. | Some frequencies in the microwaves require a government license to use these. | There is no need for a government license to use these waves. |
| Usage Cost | Setup and usage Cost is moderate. | Setup and usage Cost is high. | Usage Cost is very less. |
| Communication | These are used in long distance communication. | These are used in long distance communication. | These are not used in long distance communication. |

## h. Transmission errors, error detection and correction codes; detection methods (VRC, LRC, CRC, Checksum)

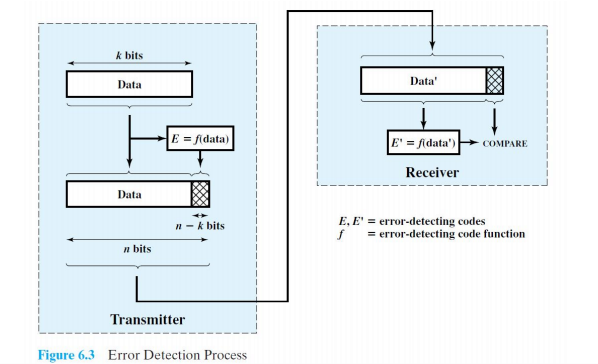
Error Detection

The contents of a frame may be altered during transmission due to noise, signal attenuation or other.

The error detection techniques allow for the detection of these transmission errors.

The most popular of these are

The types of error detection are:



Parity Check / Vertical Redundancy Check

The simplest error-detecting scheme is to append a parity bit to the end of a block of data. In the Parity Check error detection scheme, a parity bit is added to the end of a block of data. The value of the bit is selected so that the character has an even number of 1s (even parity) or an odd number of 1s (odd parity). For odd parity check, the receiver examines the received character and if the total number of 1s is odd, then it assumes that no error has occurred. If any one bit (or any odd number of bits) is erroneously inverted during transmission, then the receiver will detect an error.

However,if two (or any even number) of bits are inverted due to error, an undetected error occurs. Typically, even parity is used for synchronous transmission and odd parity for asynchronous transmission. The use of the parity bit is not foolproof, as noise impulses are often long enough to destroy more than one bit, particularly at high data rates.



if even parity is used and the number of 1s is even then one bit with value 0 is added. This way the number of 1s remains even.If the number of 1s is odd, to make it even a bit with value 1 is added.

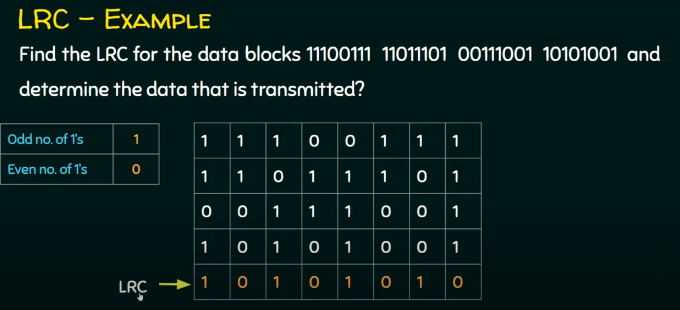
Types of VRC:

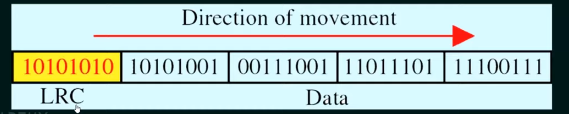
Even parity – an even number of bits are 1 Even parity – data: 10010001, parity bit 1

Odd parity – an odd number of bits are 1 Odd parity – data: 10010111, parity bit 0

LRC (Longitudinal Redundancy Check)

In LRC, a block of bits is organized in rows and columns aka Two Dimensional Parity. The parity bit is calculated for each column and sent along with the data. The block of parity acts as the redundant bits.

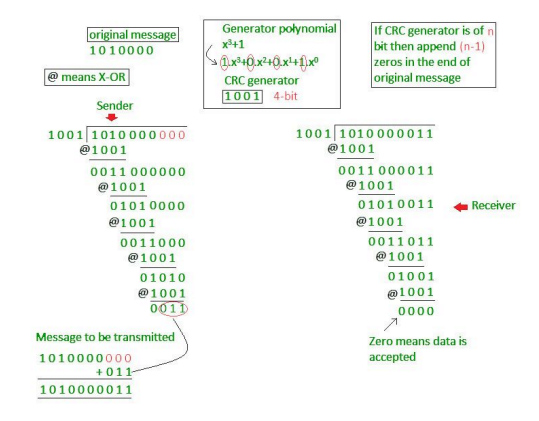




Cyclic Redundancy Check (CRC)

One of the most common, and one of the most powerful, error-detecting codes is the cyclic redundancy check (CRC).

Given a k-bit block of bits, or message, the transmitter generates a sequence, known as a frame check sequence (FCS), such that the resulting frame, consisting of n bits,n is exactly divisible by some predetermined number. The receiver then divides the incoming frame by that number and, if there is no remainder, assumes there was no error.



Checksum

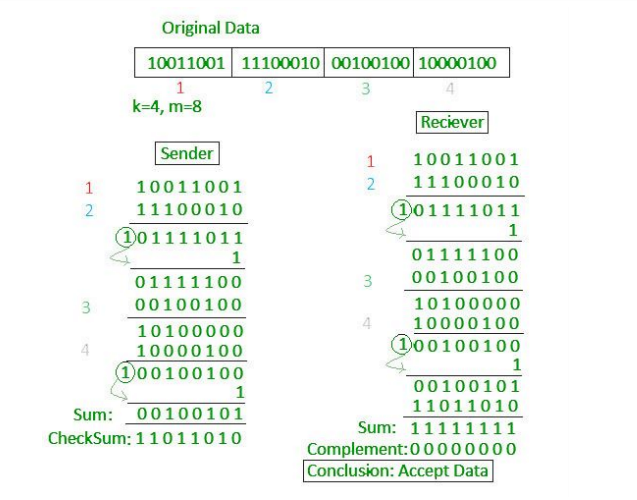
● In the checksum error detection scheme, the data is divided into k segments each of m bits.

● In the sender’s end the segments are added using 1’s complement arithmetic to get the sum. The sum is complemented to get the checksum.

● The checksum segment is sent along with the data segments.

● At the receiver’s end, all received segments are added using 1’s complement arithmetic to get the sum. The sum is complemented.

● If the result is zero, the received data is accepted; otherwise discarded.



# 3. Data link layer [8 Hrs]

## a. Data link layer design issues

* Services provided to the network layer –

The data link layer acts as a service interface to the network layer. The principal service is transferring data from the network layer on the sending machine to the network layer on the destination machine. This transfer also takes place via DLL (Dynamic Link Library).

* + Unacknowledged connectionless service - Doesn’t send any acknowledgement.
  + Acknowledged connectionless service
  + Acknowledge connection oriented service.
* Frame synchronization –

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

* Flow control –

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

* Error control –

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

## b. Media access control. MAC address

The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card. Functions are –

(i) To perform the control of access to media.

(ii) It performs the unique addressing to stations directly connected to LAN.

(iii) Detection of errors.

Mac Address

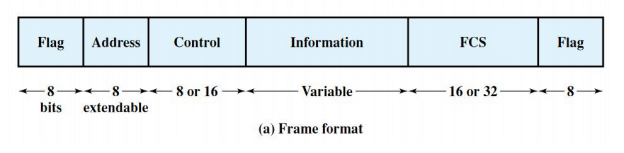
MAC address or media access control address is a unique identifier allotted to a network interface controller (NIC) of a device. It is used as a network address for data transmission within a network segment like Ethernet, Wi-Fi, and Bluetooth.

MAC address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard-coded in the network interface card (NIC). A MAC address comprises six groups of two hexadecimal digits, separated by hyphens, colons, or no separators. An example of a MAC address is 00:0A:89:5B:F0:11.

## c. Farming methods

Frame Structure

Figure 7.7 depicts the structure of the HDLC frame. The flag, address, and control fields that precede the information field are known as a header. The FCS andflag fields following the data field are referred to as a trailer.



● Flag Fields: Flag fields delimit the frame at both ends with the unique pattern 01111110.

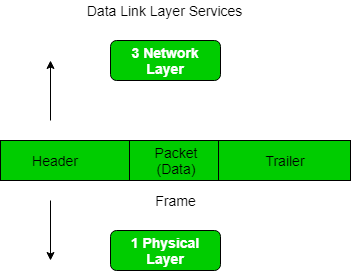
● Address Field: The address field identifies the secondary station that transmitted or is to receive the frame.

● Control Field: Used to identify the type of data contained in the frame. (eg. Ack)

● Information Field: Contains data

● Frame Check Sequence Field: The frame check sequence (FCS) is an error-detecting code

Frames are the units of digital transmission particularly in computer networks and telecommunications. Frames are comparable to the packets of energy called photons in case of light energy. Framing is a function of DLL which provides a way for a sender to transmit a set of fits that are meaningful to the receiver. Framing is a point-to-point connection between two computers or devices consisting of a wire in which data is transmitted as a stream of bits. However, these bits must be framed into discernible blocks of information.



Problems in Framing –

* Detecting start of the frame: When a frame is transmitted, every station must be able to detect it. Station detect frames by looking out for special sequence of bits that marks the beginning of the frame i.e. SFD (Starting Frame Delimiter).
* How do stations detect a frame: Every station listens to links for SFD patterns through a sequential circuit. If SFD is detected, a sequential circuit alerts the station. Station checks destination address to accept or reject frames.
* Detecting end of frame: When to stop reading the frame.

Types of frames.

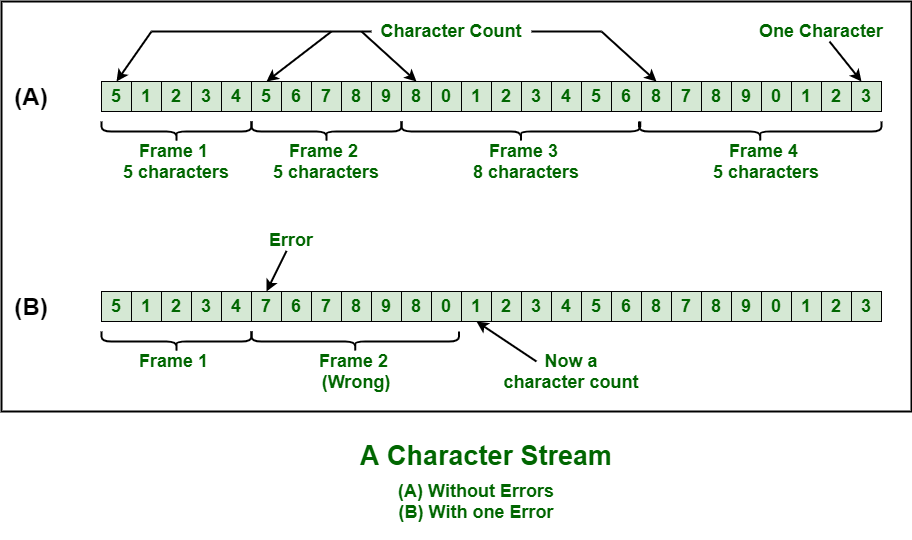
* Fixed length - The frame is of fixed size and there is no need to provide boundaries to the frame, length of the frame itself acts as a delimiter. Data bit is fixed.

* Variable length - In this there is a need to define the end of frame as well as beginning of the next frame to distinguish. Data bit is variable.

Four methods can be used to mark the start and end of each frame.

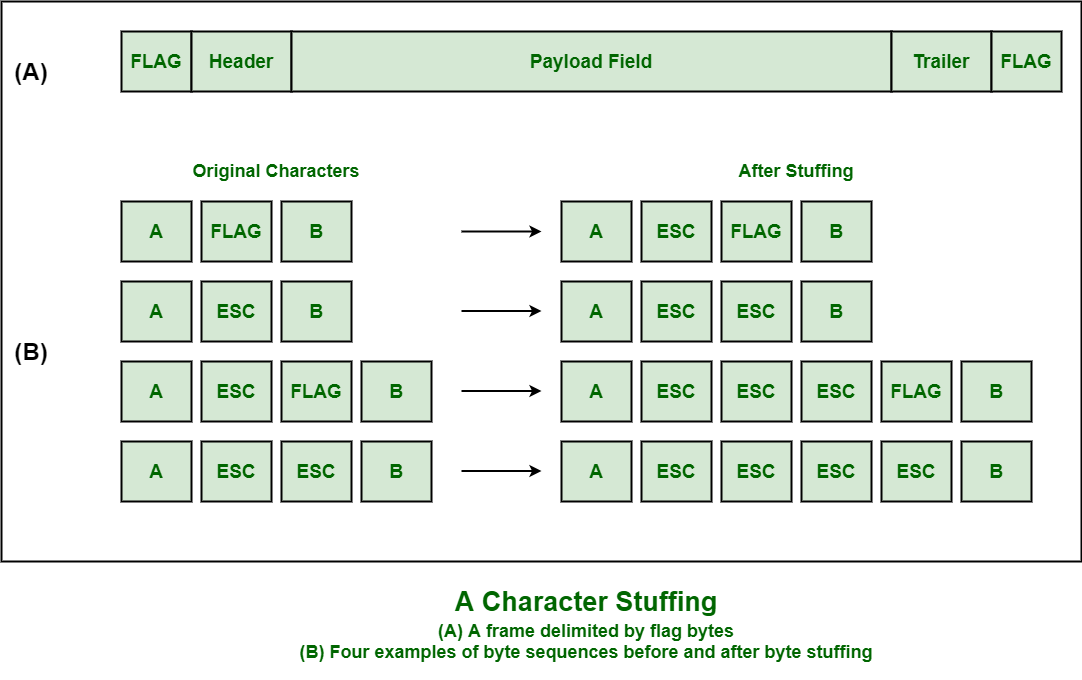
* Character count

This method is rarely used and is generally required to count the total number of characters that are present in the frame. This can be done by using a field in the header. Character count method ensures data link layer at the receiver or destination about the total number of characters that follow, and about where the frame ends.

There is disadvantage also of using this method i.e., if anyhow character count is disturbed or distorted by an error occurring during transmission, then destination or receiver might lose synchronization. The destination or receiver might also be not able to locate or identify the beginning of the next frame.

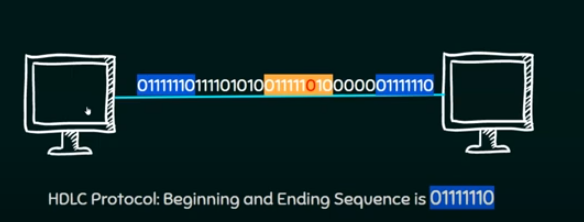
* Byte stuffing/ Character stuffing

In byte stuffing, a special byte that is basically known as ESC (Escape Character) that has a predefined pattern is generally added to the data section of the data stream or frame when there is a message or character that has the same pattern as that of flag byte.



* Bit stuffing

The beginning and end of each frame a specific bit pattern. For example, if the flag byte is 0111110 then, if it finds 5 consecutive bits inside the data bit then it adds one 0 after it.



* Physical layer coding violation

Encoding violation is a method that is used only for networks in which encoding in physical medium includes some sort of redundancy. In order to operate a division between frames in Data Link Layer this approach exploits the redundancy in Physical Layer Encoding that represents data as

00 error

01 low

10 high

11 error

So error codes 00 and 11 can be used as escapes to separate between DL frames thus violating physical layer encoding.

## d. Error control (detection and correction)

Error control refers to mechanisms to detect and correct errors that occur in the transmission of frames. Two types of errors:

Lost frame: A frame fails to arrive at the other side. For example, a noise burst may damage a frame to the extent that the receiver is not aware that a frame has been transmitted.

Damaged frame: A recognizable frame does arrive, but some of the bits are in error (have been altered during 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

The most common techniques for error control are:

• Error detection:Error detection can be done through Parity bit, CheckSum, Cyclic Redundancy Check(CRC)

• Positive acknowledgment: The destination returns a positive acknowledgment (ACK) to successfully received, error-free frames.

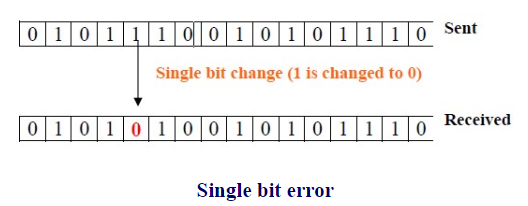
• Retransmission after timeout:The source retransmits a frame that has not been acknowledged after a predetermined amount of time.

• Negative acknowledgment and retransmission: The destination returns a negative acknowledgment (NACK) to frames in which an error is detected. The source retransmits such frames.

These errors can be divided into two types :

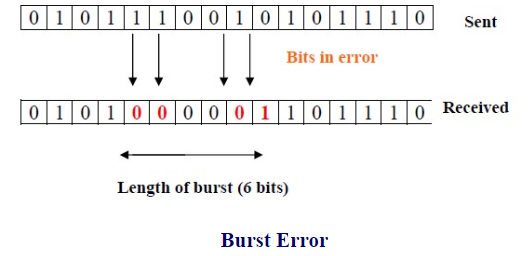
1. Single-bit error

The term single-bit error means that only one bit of a given data unit (such as a byte, character, or data unit) is changed from 1 to 0 or from 0 to 1. Single bit errors are the least likely type of errors in serial data transmission. However, a single-bit error can happen if we are having a parallel data transmission.



2. Burst error.

The term burst error means that two or more bits in the data unit have changed from 0 to 1 or vice-versa. Note that burst error doesn’t necessarily mean that error occurs in consecutive bits. The length of the burst error is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not be corrupted. Burst errors are mostly likely to happen in serial transmission.



Error Correction

The techniques that we have discussed so far can detect errors, but do not correct them. Error Correction can be handled in two ways. One is when an error is discovered; the receiver can have the sender retransmit the entire data unit. This is known as backward error correction. In the other, the receiver can use an error-correcting code, which automatically corrects certain errors. This is known as forward error correction. In theory it is possible to correct any number of errors atomically. Error-correcting codes are more sophisticated than error detecting codes and require more redundant bits. The number of bits required to correct multiple-bit or burst error is so high that in most of the cases it is inefficient to do so. For this reason, most error correction is limited to one, two or at the most three-bit errors.

One of the most widely used single bit error correction codes is the hamming code.

Steps:

1. Find no of parity bits(p) to use using formula

2^p >= m + p +1 Where m = no message bits.

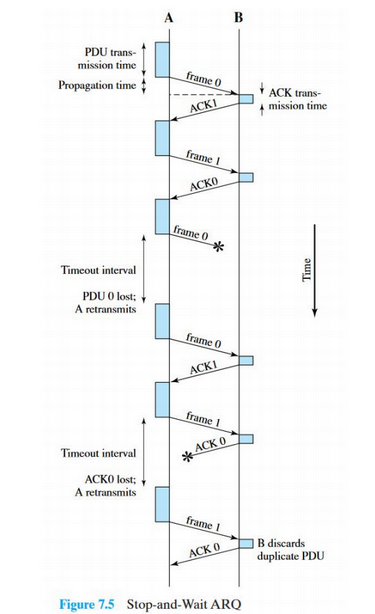
## e. Flow control, sliding window protocol

Flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from over running a slow receiver. Flow control is the management of data flow between computers or devices or between nodes in a network so that the data can be handled at an efficient pace. Too much data arriving before a device can handle it causes data overflow, meaning the data is either lost or must be retransmitted.

Three versions of ARQ have been standardized:

Stop-and-Wait ARQ

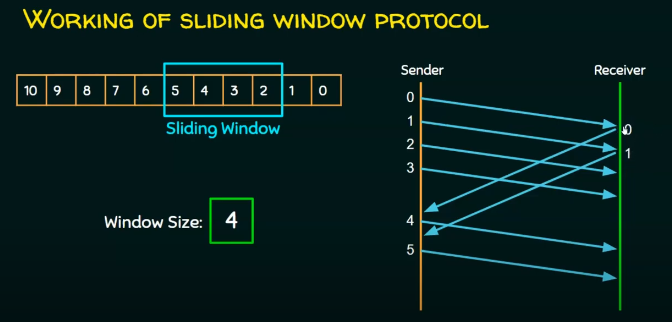
The simplest form of flow control, known as stop-and-wait flow control, works as follows. A source entity transmits a frame. After the destination entity receives the frame, it indicates its willingness to accept another frame by sending back an acknowledgment to the frame just received. The source must wait until it receives the acknowledgment before sending the next frame. The destination can thus stop the flow of data simply by withholding acknowledgment.



Sliding Windows Protocols

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol). In this technique, each frame is sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number. Types of sliding window protocol are as follows:

* Go-Back-N ARQ
* Selective Repeat ARQ



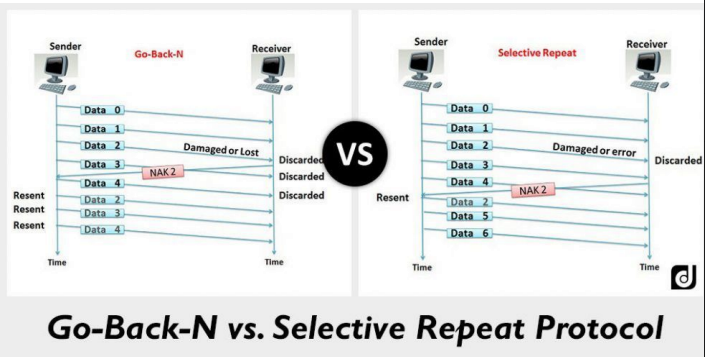
Go back N (GBN)

Let us take an example where the source is sending some packets to the destination as shown in figure. Here the receiver receives packet no 0 and pkt 1. But the packet no 2 is lost during transmission. The sender keeps sending other packets (packet no 3 and 4), but since the

receiver did not receive the packet no 2 it sends an NACK2 (negative ack) indicating that it didn’t receive the packet no 2. The receiver will discard packet 3 and packet 4 even though it received them just fine. The sender upon receiving the NACK2, will again start sending packet from pkt 2 as shown in figure.

Selective Repeat (SR)

The problem with GBN is that even though valid packets 3 and 4 were received they get discarded because the previous packet 2 was not received. The SR packet solves this by storing the received packet 3 and 4 in its buffer and sending NACK2 to request only the lost packet 2. When packet 2 is received the sender resumes sending packet from pkt 5.



## f. Data link layer protocols: HDLC, SLIP, and PPP

The most important data link control protocol is HDLC. Not only is HDLC widely used, but it is the basis for many other important data link control protocols, which use the same or similar formats and the same mechanisms as employed in HDLC.

A high-level data link control defines rules for transmitting data between network points. Data in an HDLC is organized into units called frames and is sent across networks to specified destinations. HDLC also manages the pace at which data is transmitted. HDLC is commonly used in the open systems interconnection (OSI) model's layer 2.

HDLC frames are transmitted over synchronous links or asynchronous links. This is done using a frame delimiter or flag, which contains a unique sequence of bits that are not visible inside a frame. HDLC provides both connection-oriented and connectionless service.

There are three types of stations:

1. Primary station

Sends command and accepts responses (the controlling node).

2. Secondary station

Accepts commands and sends responses (the controlled node).

3. Combined station

Sends or accepts commands and responses (this type appears in what is called balanced configurations, such as LAPB).

The two link configurations are:

1. Unbalanced configuration:

Consists of one primary and one or more secondary stations and supports both full-duplex and half-duplex transmission.

2. Balanced configuration:

Consists of two combined stations and supports both full-duplex and half-duplex transmission

The three data transfer modes are:

1. Normal response mode (NRM):

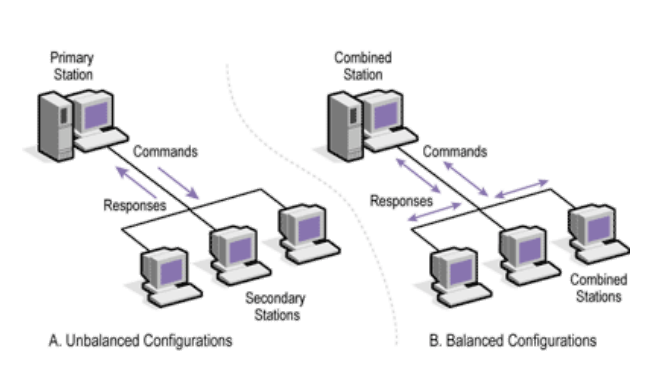
Used with an unbalanced configuration. The primary may initiate data transfer to a secondary, but a secondary may only transmit data in response to a command from the primary.

2. Asynchronous balanced mode (ABM):

Used with a balanced configuration.Either combined station may initiate transmission without receiving permission from the other combined station.

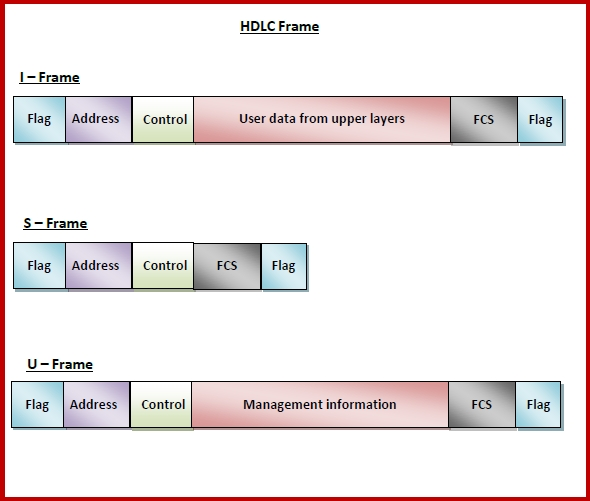
3. Asynchronous response mode (ARM):

Used with an unbalanced configuration. The secondary may initiate transmission without explicit permission of the primary. The primary still retains responsibility for the line, including initialization, error recovery, and logical disconnection.



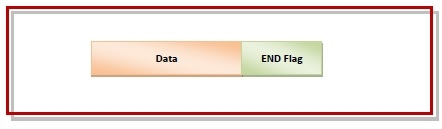
There are three types of HDLC frames. The type of frame is determined by the control field of the frame −

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



Serial Line Internet Protocol (SLIP) is a simple protocol that works with TCP/IP for communication over serial ports and routers. They provide communications between machines that were previously configured for direct communication with each other.

SLIP frame has a very simple format, consisting of payload and a flag that acts as an end delimiter. The flag is generally a special character equivalent to decimal 192. If this flag is present in the data, then an escape sequence precedes it, so that the receiver does not consider it as the end of the frame



Advantages of SLIP

* It has a very small overhead. So, it is suitable for usage in microcontrollers.
* It reuses the existing dial-up connections and telephone lines.
* It supports the most widely used protocol, Internet Protocol (IP). So, there is ease of deployment.

Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds. Since it is a data link layer protocol, data is transmitted in frames. It is also known as RFC 1661.

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

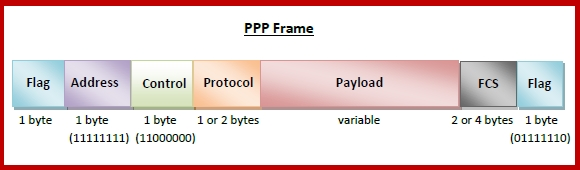
* Defining the frame format of the data to be transmitted.
* Defining the procedure of establishing link between two points and exchange of data.
* Stating the method of encapsulation of network layer data in the frame.
* Stating authentication rules of the communicating devices.
* Providing address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

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

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

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

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



Byte Stuffing in PPP Frame − Byte stuffing is used as PPP payload field whenever the flag sequence appears in the message, so that the receiver does not consider it as the end of the frame. The escape byte, 01111101, is stuffed before every byte that contains the same byte as the flag byte or the escape byte. The receiver on receiving the message removes the escape byte before passing it onto the network layer.

## 

## g. ALOHA, CSMA/CD, FDDI, Token ring, Token bus and IEEE802.3, 802.4, 802.5

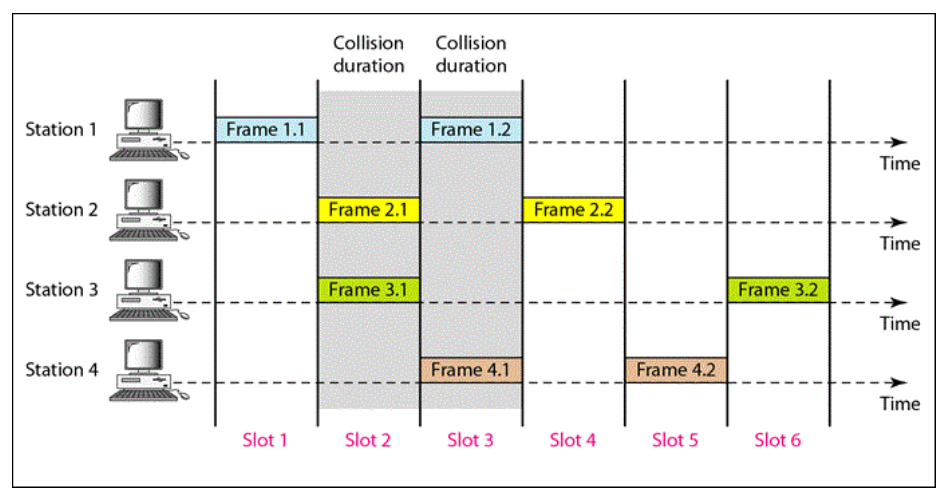
1. Pure ALOHA

The original ALOHA protocol is called pure ALOHA. This is a simple, but elegant protocol. The idea is that each station sends a frame whenever it has a frame to send. However, since there is only one channel to share, there is the possibility of collision between frames from different stations. The pure ALOHA protocol relies on acknowledgments from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgement. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame. A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again. Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions. We call this time the back-off time. Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames. After a maximum number of retransmission attempts Kmax' a station must give up and try later. The efficiency is 18%.

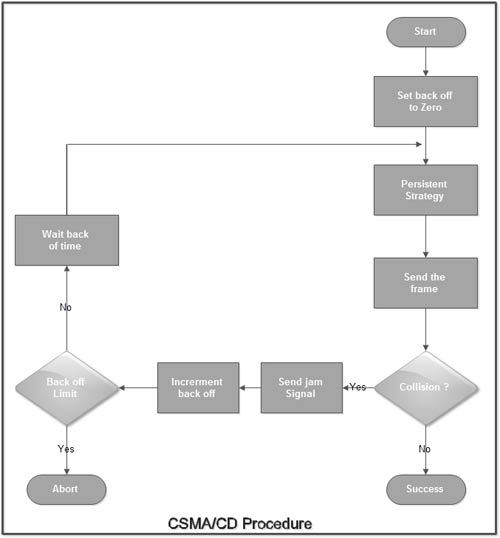


1. Slotted ALOHA

Pure ALOHA has a vulnerable time of 2 x Tfr . This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished. Slotted ALOHA was invented to improve the efficiency of pure ALOHA. In slotted ALOHA we divide the time into slots and force the station to send only at the beginning of the time slot. Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finished sending its frame. Of course, there is still the possibility of collision if two stations try to send at the beginning of the same time slot. However, the vulnerable time is now reduced to one-half, the efficiency is at 36%.



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



The algorithm of CSMA/CD is:

* When a frame is ready, the transmitting station checks whether the channel is idle or busy.
* If the channel is busy, the station waits until the channel becomes idle.
* If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision.
* If a collision is detected, the station starts the collision resolution algorithm.
* The station resets the retransmission counters and completes frame transmission.

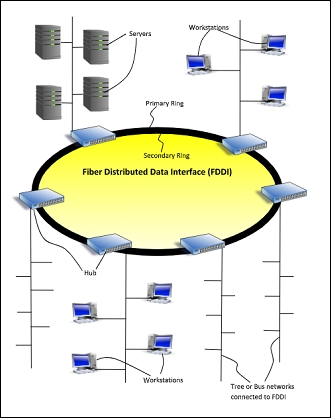
The algorithm of Collision Resolution is:

* The station continues transmission of the current frame for a specified time along with a jam signal, to ensure that all the other stations detect collision.
* The station increments the retransmission counter.
* If the maximum number of retransmission attempts is reached, then the station aborts transmission.
* Otherwise, the station waits for a backoff period which is generally a function of the number of collisions and restarts the main algorithm.

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

Features

* FDDI uses optical fiber as its physical medium.
* It operates in the physical and medium access control (MAC layer) of the Open Systems Interconnection (OSI) network model.
* It provides a high data rate of 100 Mbps and can support thousands of users.
* It is used in LANs up to 200 kilometers for long distance voice and multimedia communication.
* It uses ring based token passing mechanism and is derived from IEEE 802.4 token bus standard.
* It contains two token rings, a primary ring for data and token transmission and a secondary ring that provides backup if the primary ring fails.
* FDDI technology can also be used as a backbone for a wide area network (WAN).



The fields of an FDDI frame are −

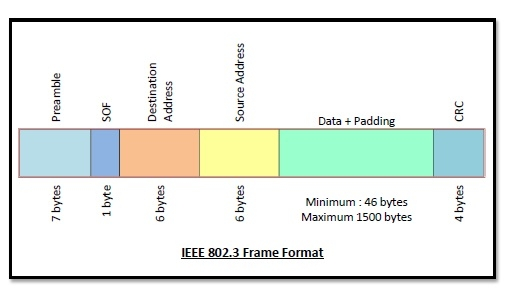
* Preamble: 1 byte for synchronization.
* Start Delimiter: 1 byte that marks the beginning of the frame.
* Frame Control: 1 byte that specifies whether this is a data frame or control frame.
* Destination Address: 2-6 bytes that specifies address of destination station.
* Source Address: 2-6 bytes that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

## 

IEEE 802.3 is a set of standards and protocols that define Ethernet-based networks. Ethernet technologies are primarily used in LANs, though they can also be used in MANs and even WANs. IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks.

The main fields of a frame of classic Ethernet are -

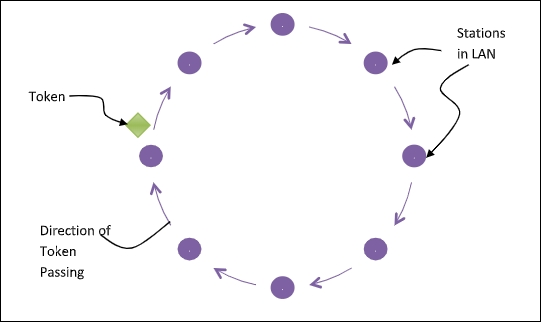
* Preamble: It is a 7 bytes starting field that provides alert and timing pulse for transmission.
* Start of Frame Delimiter: It is a 1 byte field that contains an alternating pattern of ones and zeros ending with two ones.
* Destination Address: It is a 6 byte field containing physical address of destination stations.
* Source Address: It is a 6 byte field containing the physical address of the sending station.
* Length: It is a 7 bytes field that stores the number of bytes in the data field.
* Data: This is a variable sized field carrying the data from the upper layers. The maximum size of the data field is 1500 bytes.
* Padding: This is added to the data to bring its length to the minimum requirement of 46 bytes.
* CRC: CRC stands for cyclic redundancy check. It contains the error detection information.



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

Token Passing Mechanism in Token Ring

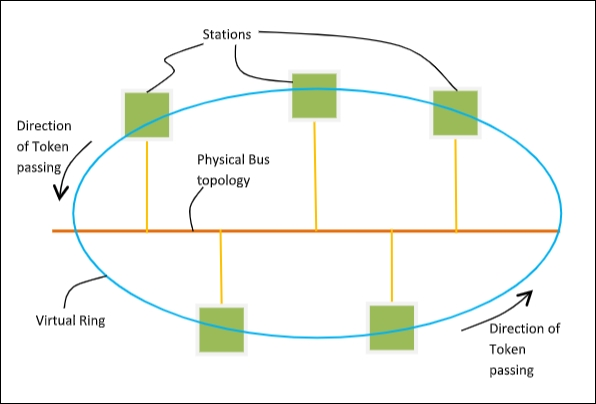
If a station has a frame to transmit when it receives a token, it sends the frame and then passes the token to the next station; otherwise it simply passes the token to the next station. Passing the token means receiving the token from the preceding station and transmitting to the successor station.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



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

Token Passing Mechanism in Token Bus

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



The frame format is given by the following diagram −

#same as FDDI frame format

| S.NO | TOKEN BUS Network | TOKEN RING Network |
| --- | --- | --- |
| 1. | In the token bus network the token is passed along a virtual ring. | While in the token ring network the token is passed over a physical ring. |
| 2. | The token bus network is simply designed for the large factories. | While the token ring network is designed for the offices. |
| 3. | The token bus network is defined by the IEEE 802.4 standard. | While the token ring network is defined by the IEEE 802.5 standard. |
| 4. | Token bus network provides better bandwidth. | While the token ring network does not provide better bandwidth as compared to token bus. |
| 5. | In the token bus network, Bus topology is used. | While in the token ring network, Star topology is used. |
| 6. | The maximum time it takes to reach the last station in a token bus network cannot be calculated. | While the maximum time to reach the last station in the token ring network can be calculated. |

# 4. Network layer [8 Hrs]

## a. Network layer design issues

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.

## b. IP based networking (Mobile-IP, Subnet Mask, Private and Public address IP address, IPv4 addressing, Subnetting, VLSM, CIDO, Supernetting, multicasting, broadcasting, IPv6)

Mobile-IP

Mobile IP is a communication protocol (created by extending Internet Protocol, IP) that allows the users to move from one network to another with the same IP address. It ensures that the communication will continue without user’s sessions or connections being dropped.

Terminologies:

Mobile Node (MN):

It is the hand-held communication device that the user carries e.g. Cell phone.

Home Network:

It is a network to which the mobile node originally belongs to as per its assigned IP address (home address).

Home Agent (HA):

It is a router in home network to which the mobile node was originally connected

Home Address:

It is the permanent IP address assigned to the mobile node (within its home network).

Foreign Network:

It is the current network to which the mobile node is visiting (away from its home network).

Foreign Agent (FA):

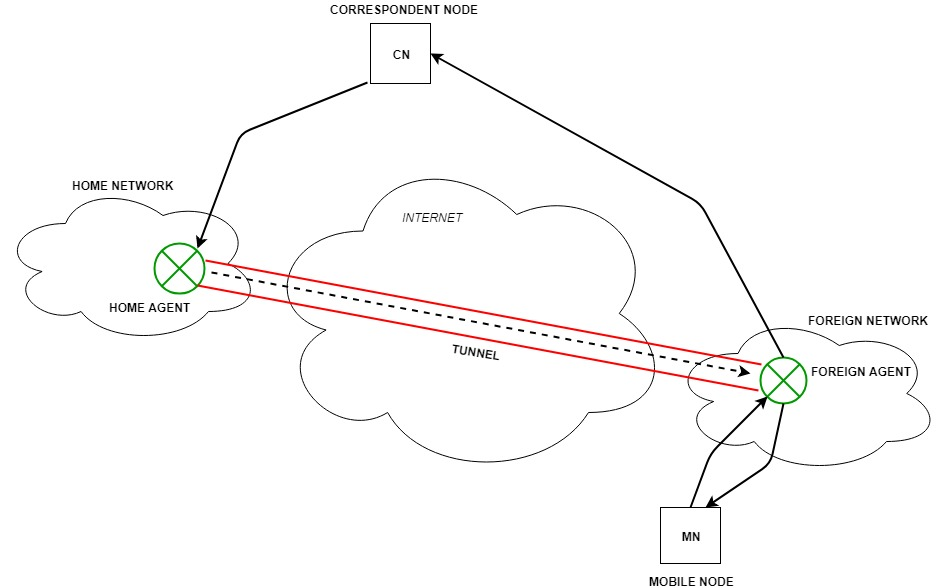
It is a router in foreign network to which a mobile node is currently connected. The packets from the home agent are sent to the foreign agent which delivers it to the mobile node.

Correspondent Node (CN):

It is a device on the internet communicating to the mobile node.

Care of Address (COA):

It is the temporary address used by a mobile node while it is moving away from its home network.



Process of Mobile IP

1. Agent Discovery

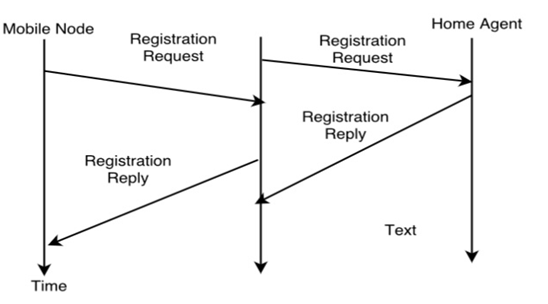
During the agent discovery phase the HA and FA advertise their services on the network by using the ICMP router discovery protocol (IROP).

Mobile IP defines two methods: agent advertisement and agent solicitation which are in fact router discovery methods plus extensions.

* Agent advertisement: For the first method, FA and HA advertise their presence periodically using special agent advertisement messages. These message advertisements can be seen as a beacon broadcast into the subnet. For this advertisement internet control message protocol (ICMP) messages according to RFC 1256, are used with some mobility extensions.
* Agent solicitation: If no agent advertisements are present or the inter arrival time is too high, and an MN has not received a COA, the mobile node must send agent solicitations. These solicitations are again based on RFC 1256 for router solicitations.

1. Registration

The main purpose of the registration is to inform the home agent of the current location for correct forwarding of packets.



Registration can be done in two ways depending on the location of the COA.

* If the COA is at the FA, the MN sends its registration request containing the COA to the FA which is forwarding the request to the HA. The HA now set up a mobility binding containing the mobile node's home IP address and the current COA.

Additionally, the mobility biding contains the lifetime of the registration which is negotiated during the registration process. Registration expires automatically after the lifetime and is deleted; so a mobile node should register before expiration. After setting up the mobility binding, the HA sends a reply message back to the FA which forwards it to the MN.

* If the COA is co-located, registration can be very simple. The mobile node may send the request directly to the HA and vice versa. This by the way is also the registration procedure for MNs returning to their home network.

1. Tunneling

A tunnel is used to establish a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets which are entering in a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunneling, i.e., sending a packet through a tunnel is achieved with the help of encapsulation.

Tunneling is also known as "port forwarding" is the transmission and data intended for use only within a private, usually corporate network through a public network.

Subnet Mask

A subnet mask is a 32-bit number created by setting host bits to all 0s and setting network bits to all 1s. In this way, the subnet mask separates the IP address into the network and host addresses.

The “255” address is always assigned to a broadcast address, and the “0” address is always assigned to a network address. Neither can be assigned to hosts, as they are reserved for these special purposes.

A subnet mask of 255.255.255.0 allows for close to 256 unique hosts within the network (since not all 256 IP addresses can be used).

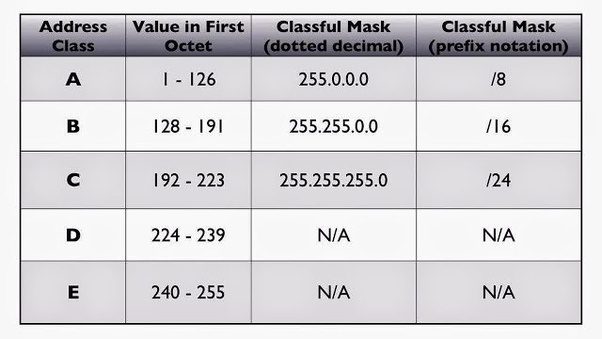
Private IP Address

Blocks of IP addresses that are set aside for internal private use for computers not directly connected to the Internet. These IP addresses are not supposed to be routed through the Internet, and most service providers will block the attempt to do so. These IP addresses are used for internal use by companies or home networks that need to use TCP/IP but do not want to be directly visible on the Internet. Eg. 192.168.0.0/16, 10.0.0.0/8, 172.16.0.0/12

Public IP Address

Blocks of IP addresses that are used to access the public network (eg internet). The public IP addresses are generally available through the ISP to systems that need to be accessed through the internet. Eg. If you have a website or email server then you need to assign those systems a public address so that users are able to access them. A system also needs an public ip address to access the internet.

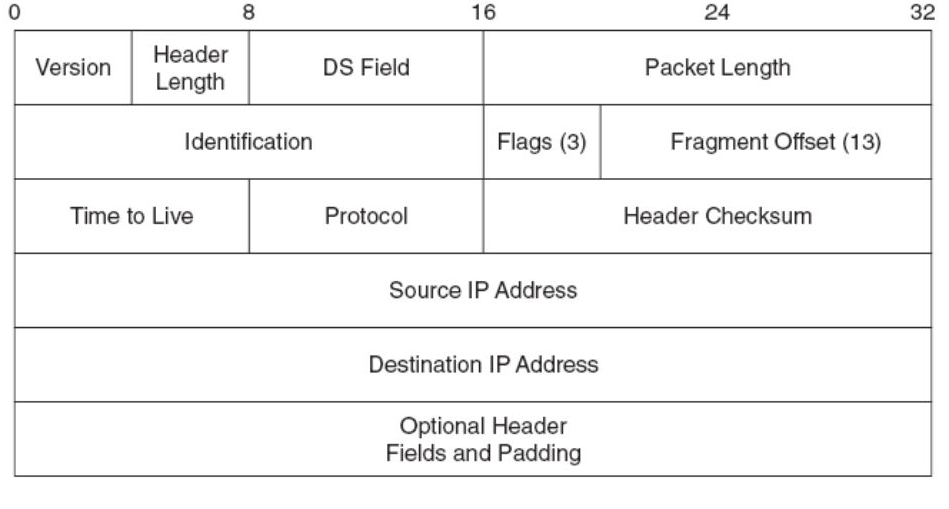
IP addresses are divided into 5 classes. Different classes have different host and network bits.



IPv4 addressing

IPv4 is the most widely used Internet protocol across the internet today. Internet protocols are mostly responsible for addressing and forwarding of data on the Internet.

The network layer packet, also referred to as datagram, plays a central role in communication across the internet. The basic format of the IPv4 datagram is shown below :

IPv4 Fields

Version:- The first header field in an IP packet is the four-bit version field. The Version field indicates the format of the internet header. Version identifies the IP version to which the packet belongs. This four-bit field is set to binary 0100 to indicate version 4 (IPv4) or binary 0110 to indicate version 6 (IPv6).

Header length or Internet Header Length (IHL) :- The second field (4 bits) is the Internet Header Length (IHL), this field specifies the size of the header.

Type of Service(ToS):- now known as Differentiated Services Code Point (DSCP). The TOS field is used to carry information to provide quality of service features. An example is Voice over IP (VoIP) that is used for interactive data voice exchange.

Total Length:- This 16-bit field defines the entire datagram size, including header and data, in bytes.

Identification, Flags, Fragment Offset:- These three fields are used to fragment and reassemble large IP datagram.

Time To Live (TTL):-It is of 8 bit field. This field specifies the maximum no of hops ( Routers ) the packet can travel before it is dropped.

Protocol:-This field defines the protocol used in the data portion of the IP datagram. Eg. TCP, UDP etc.

Header Checksum:- The 16-bit checksum field is used for error-checking of the header. At each hop, the checksum of the header must be compared to the value of this field. If a header checksum is found to be mismatched, then the packet is discarded.

Source address:- Sets the source IP address.

Destination address:- An IPv4 address indicating the receiver of the packet.

Options and Padding :- Used to specify additional header fields if needed. They must be multiple of 32 bits.

Subnetting

Subnetting is the practice of dividing a network into two or smaller networks. It increases routing efficiency, which helps to enhance the security of the network and reduces the size of the broadcast domain.

IP Subnetting designates high-order bits from the host as part of the network prefix. This method divides a network into smaller subnets.

It also helps you to reduce the size of the routing tables, which is stored in routers. This method also helps you to extend the existing IP address base & restructures the IP address.

Advantage of Subnetting

* Subnetting allows us to break a single large network in smaller networks. Small networks are easy to manage.
* Subnetting reduces network traffic by allowing only the broadcast traffic which is relevant to the subnet.
* By reducing unnecessary traffic, Subnetting improves overall performance of the network.
* By blocking a subnet’ traffic in subnet, Subnetting increases security of the network.
* Subnetting reduces the requirement of IP range.

Disadvantage of Subnetting

* Different subnets need an intermediate device known as a router to communicate with each other.
* Since each subnet uses its own network address and broadcast address, more subnets mean more wastage of IP addresses.
* Subnetting adds complexity to the network. An experienced network administrator is required to manage the subnetted network.

VLSM

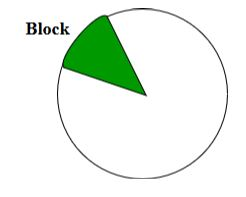
VLSM stands for Variable Length Subnet Mask where the subnet design uses more than one mask in the same network which means more than one mask is used for different subnets of a single class A, B, C or a network.

Variable-Length Subnet Masking (VLSM) amounts to "subnetting subnets," which means that VLSM allows network engineers to divide an IP address space into a hierarchy of subnets of different sizes, making it possible to create subnets with very different host counts without wasting large numbers of addresses.

A subnet mask defines the size of the subnet (the number of host addresses in the subnet). Fixed-Length Subnet Masking (FLSM) creates subnets all the same size. But where some subnets will have many hosts and some have few, FLSM results in some subnets having many orphaned addresses, or some sets of hosts being too big to fit into a subnet. Where VLSM is enabled, a large subnet can be divided into a set of smaller sub-subnets, which can be used to handle smaller sets of hosts.

* Subnets are variable in size.
* Subnets have a variable number of hosts.
* Subnets use different subnet masks.
* It is complex in configuration and administration.
* It wastes minimum IP addresses.
* It is also known as classless Subnetting.
* It supports only classless routing protocols.

CIDO  
In order to reduce the wastage of IP addresses a new concept of Classless Inter-Domain Routing is introduced. Nowadays IANA is using this technique to provide the IP addresses. Whenever any user asks for IP addresses, IANA is going to assign that many IP addresses to the User.



Representation: It is also a 32-bit address, which includes a special number which represents the number of bits that are present in the Block Id.

a . b . c . d / n

Where n is the number of bits that are present in Block Id / Network Id.

Example:

20.10.50.100/20

Rules for forming CIDR Blocks:

1. All IP addresses must be contiguous.
2. Block size must be the power of 2 (2n).

If the size of the block is the power of 2, then it will be easy to divide the Network. Finding out the Block Id is very easy if the block size is of the power of 2.

Example:

If the Block size is 25 then, Host Id will contain 5 bits and Network will contain 32 – 5 = 27 bits.

1. First IP address of the Block must be evenly divisible by the size of the block. In simple words, the least significant part should always start with zeroes in Host Id. Since all the least significant bits of Host Id are zero, then we can use it as a Block Id part.

Supernetting

Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.

Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

More specifically,

* When multiple networks are combined to form a bigger network, it is termed as super-netting
* Super netting is used in route aggregation to reduce the size of routing tables and routing table updates

There are some points which should be kept in mind while supernetting:

1. All the Networks should be contiguous.
2. The block size of every network should be equal and must be in the form of 2n.
3. First Network id should be exactly divisible by whole size of supernet

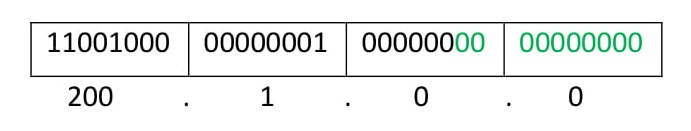
Conditions:

1. Contiguous: You can easily see that all networks are contiguous all having size 256 hosts.

Range of first Network from 200.1.0.0 to 200.1.0.255. If you add 1 in the last IP address of the first network that is 200.1.0.255 + 0.0.0.1, you will get the next network id that is 200.1.1.0. Similarly, check that all networks are contiguous.

1. Equal size of all networks: As all networks are of class C, so all of them have a size of 256 which in turn equal to 28.
2. First IP address exactly divisible by total size: When a binary number is divided by 2n then last n bits are the remainder. Hence in order to prove that first IP address is exactly divisible by the size of Supernet Network. You can check that if last n v=bits are 0 or not.

In given example first IP is 200.1.0.0 and whole size of supernet is 4\*28 = 210. If the last 10 bits of the first IP address are zero then IP will be divisible.



Last 10 bits of the first IP address are zero (highlighted by green color). So the 3rd condition is also satisfied.

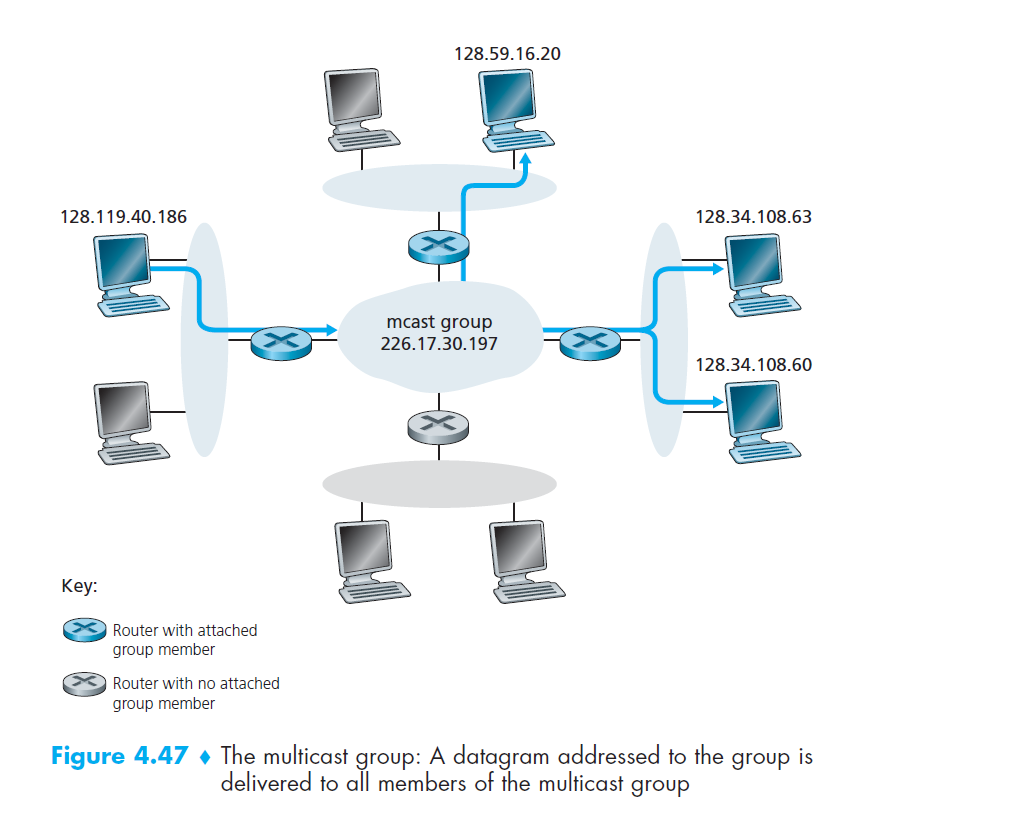
Therefore, you can join all these 4 networks and can make a Supernet. New Supernet Id will be 200.1.0.0.

Multicasting

Multicast service, in which a multicast packet is delivered to only a subset of

network nodes. A number of emerging network applications require the delivery of packets from one or more senders to a group of receivers. These applications include bulk data transfer (for example, the transfer of a software upgrade from the software developer to users needing the upgrade), streaming continuous media (for example, the transfer of the audio, video, and text of a live lecture to a set of distributed lecture participants), shared data applications (for example, a whiteboard or teleconferencing application that is shared among many distributed participants), data feeds (for example, stock quotes), Web cache updating, and interactive gaming (for example, distributed interactive virtual environments or multiplayer games).

On the Internet, if we need to send a message to multiple pc ( a group) then to identify these groups of pc a single identifier is used. This single identifier is a class D multicast IP address. The group of receivers associated with a class D address is referred to as a multicast group. The multicast group abstraction is illustrated in Figure 4.47. Here, four hosts (shown in shaded color) are associated with the multicast group address of 226.17.30.197 and will receive all datagrams addressed to that multicast address.



Broadcasting

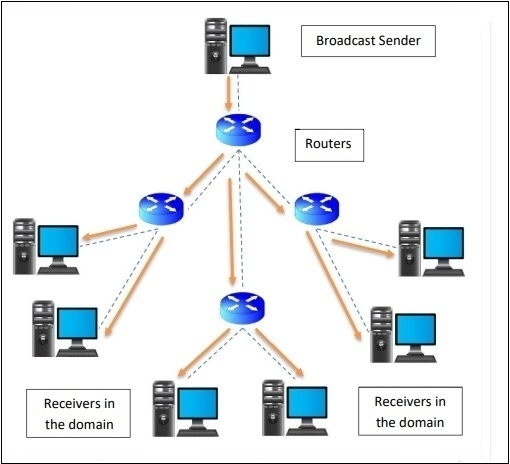
Broadcasting in a computer network is a group communication, where a sender sends data to receivers simultaneously. This is an all − to − all communication model where each sending device transmits data to all other devices in the network domain.

The ways of operation of broadcasting may be −

A high level operation in a program, like broadcasting in Message Passing Interface.

A low level networking operation, like broadcasting on Ethernet.

Broadcasting is shown in the following figure −



Advantages of Broadcasting

Broadcast helps to attain economies of scale when a common data stream needs to be delivered to all, by minimizing the communication and processing overhead. It ensures better utilization of resources and faster delivery in comparison to several unicast communication.

Disadvantages of Broadcasting

Broadcasting cannot accommodate a very large amount of devices. Also it does not allow personalisation of the messages according to the individual preferences of the devices.

IPv6

The exhaustion of the IPv4 address space has forced the technology world to look for newer solutions to the addressing scheme. Since IPv4 IP addresses use 32-bit addresses, there are a possible ~4.2 billion (2^32) possible IP addresses. Have we used them all up? No, but there are some address ranges that can’t be used for technical/legacy reasons. Even if those technical/legacy reasons could be overcome, the IPv4 address space is still very constrained for a quickly growing Internet. In April 2010, the Regional Internet Registries (the “authorities”) said that only 8% of the IPv4 addresses are unallocated and the remaining are expected to run within years.

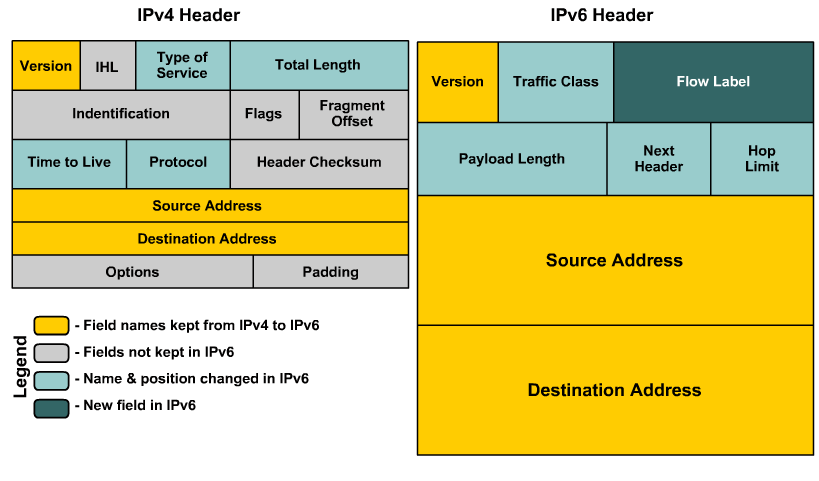
The main incentives to move to IPv6 are:

-IPv6 gives us 128 bits for address space that is (2^128) unique addresses.

-IPv6 has built-in features for mobility.

-IPv6 has built-in support for IPSec.

-IPv6 supports for smooth transition from IPv4



The following list describes the function of each header field.

Version – 4-bit Version number of Internet Protocol = 6.

Traffic Class – 8-bit traffic class field. The nodes that originate a packet must identify different classes or different priorities of IPv6 packets. The nodes use the Traffic Class field in the IPv6 header to make this identification. The routers that forward the packets also use the Traffic Class field for the same purpose.

Flow Label – 20-bit field. The IPv6 routers must handle the packets belonging to the same flow in a similar fashion. All packets that belong to the same flow must be sent with the same source address, same destination address.

Payload Length – The 16-bit payload length field contains the length of the data field in octets/bits following the IPv6 packet header. The 16-bit Payload length field puts an upper limit on the maximum packet payload to 64 kilobytes.

Next Header – 8-bit selector. Identifies the type of header that immediately follows the IPv6 header. wing the IPv6 header and located at the beginning of the data field (payload) of the IPv6 packet. This field usually specifies the transport layer protocol used by a packet's payload. The two most common kinds of Next Headers are TCP (6) and UDP (17), but many other headers are also possible. Similar to the Protocol field in IPv4.

Hop Limit – 8-bit integer. This field specifies the maximum no of hops ( Routers ) the packet can travel before it is dropped.

Source Address – 128 bits. The address of the initial sender of the packet.

Destination Address – 128 bits. The address of the intended recipient of the packet.

## c. Concept of routing (Static and dynamic routing)

## Static Routing/Non-Adaptive Routing

A static routing table is created, maintained, and updated by a network administrator, manually. A static route to every network must be configured on every router for full connectivity. This provides a granular level of control over routing, but quickly becomes impractical on large networks. Routers will not share static routes with each other, thus reducing CPU/RAM overhead and saving bandwidth. However, static routing is not fault-tolerant, as any change to the routing infrastructure (such as a link going down, or a new network added) requires manual intervention. Routers operating in a purely static environment cannot seamlessly choose a better route if a link becomes unavailable.

Advantages of Static Routing

• Minimal CPU/Memory overhead

• No bandwidth overhead (updates are not shared between routers)

• Granular control on how traffic is routed

Disadvantages of Static Routing

• Infrastructure changes must be manually adjusted

• No “dynamic” fault tolerance if a link goes down

• Impractical on large network

## Dynamic Routing/Adaptive Routing

A dynamic routing table is created, maintained, and updated by a routing protocol running on the router. Examples of routing protocols include RIP (Routing Information Protocol) and OSPF (Open Shortest Path First).Routers do share dynamic routing information with each other, which increases CPU, RAM, and bandwidth usage. However, routing protocols are capable of dynamically choosing a different (or better) path when there is a change to the routing infrastructure.

Advantages of Dynamic Routing

• Simpler to configure on larger networks

• Will dynamically choose a different (or better)

Disadvantages of Dynamic Routing

• Updates are shared between routers, thus consuming bandwidth

• Routing protocols put additional load on router CPU/RAM

• The choice of the “best route” is in the hands of the routing protocol, and not the network administrator.

## d. Routing algorithm (Shortest-path, Flooding, Flow-based, Distance-vector, Link-state)

Shortest-path  
Shortest path routing refers to the process of finding paths through a network that have a minimum of distance or other cost metric.

Basics of Dijkstra's Algorithm

* Dijkstra's Algorithm basically starts at the node that you choose (the source node) and it analyzes the graph to find the shortest path between that node and all the other nodes in the graph.
* The algorithm keeps track of the currently known shortest distance from each node to the source node and it updates these values if it finds a shorter path.
* Once the algorithm has found the shortest path between the source node and another node, that node is marked as "visited" and added to the path.
* The process continues until all the nodes in the graph have been added to the path. This way, we have a path that connects the source node to all other nodes following the shortest path possible to reach each node.

Flooding

When a routing algorithm is implemented, each router must make decisions

based on local knowledge, not the complete picture of the network. A simple

local technique is flooding, in which every incoming packet is sent out on every

outgoing line except the one it arrived on.

Flooding obviously generates vast numbers of duplicate packets, in fact, an

infinite number unless some measures are taken to damp the process. One such

measure is to have a hop counter contained in the header of each packet that is

decremented at each hop, with the packet being discarded when the counter

reaches zero. Ideally, the hop counter should be initialized to the length of the

path from source to destination. If the sender does not know how long the path is,

it can initialize the counter to the worst case, namely, the full diameter of the network.

Flooding with a hop count can produce an exponential number of duplicate

packets as the hop count grows and routers duplicate packets they have seen before.

A better technique for damming the flood is to have routers keep track of

which packets have been flooded, to avoid sending them out a second time. One

way to achieve this goal is to have the source router put a sequence number in

each packet it receives from its hosts. Each router then needs a list per source

router telling which sequence numbers originating at that source have already

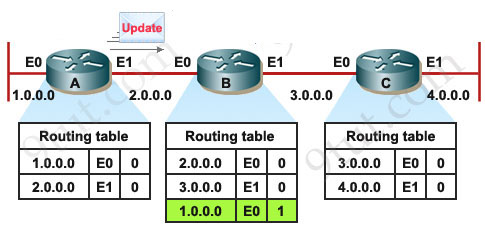
been seen. If an incoming packet is on the list, it is not flooded.

Flow Control

Flow routing is a network routing technology that takes variations in the flow of data into account to increase routing efficiency. The increased efficiency helps avoid excessive latency and jitter for streaming data, such as VoIP (voice over IP) or video. Rather than routing individual packets, a flow router observes and evaluates flows to gather statistics, including source, destination, amount of traffic "in flight," and stream duration.

Distance-Vector

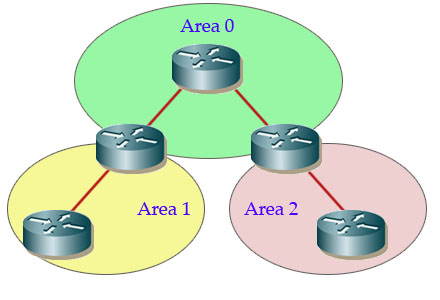
A distance-vector routing protocol begins by advertising directly-connected networks to its neighbors. These updates are sent regularly (RIP – every 30 seconds; IGRP – every 90 seconds). Neighbors will add the routes from these updates to their own routing tables. Each neighbor trusts this information completely, and will forward their full routing table (connected and learned routes) to every other neighbor. Thus, routers fully (and blindly) rely on neighbors for route information, a concept known as routing by rumor. There are several disadvantages to this behavior. Because routing information is propagated from neighbor to neighbor via periodic updates, distance-vector protocols suffer from slow convergence. This, in addition to blind faith of neighbor updates, results in distance-vector protocols being highly susceptible to routing loops. Distance-vector protocols utilize some form of distance to calculate a route’s metric. RIP uses hop count as its distance metric.



Link-State

Link-state routing protocols were developed to alleviate the convergence and loop issues of distance-vector protocols. Link-state protocols maintain three separate tables: Link-state protocols do not “route by rumor.” Instead, routers send updates advertising the state of their links (a link is a directly-connected network). All routers know the state of all existing links within their area, and store this information in a topology table. All routers within an area have identical topology tables. The best route to each link (network) is stored in the routing (or shortest- path) table. If the state of a link changes, such as a router interface failing, an advertisement containing only this link-state change will be sent to all routers within that area. Each router will adjust its topology table accordingly, and will calculate a new best route if required. By maintaining a consistent topology table among all routers within an area, link-state protocols can converge very quickly and are immune to routing loops. Additionally, because updates are sent only during a link-state change, and contain only the change (and not the full table), link-state protocols are less bandwidth intensive than distance-vector protocols. However, the three link-state tables utilize more RAM and CPU on the router itself. Link-state protocols utilize some form of cost, usually based on bandwidth, to calculate a route’s metric. The Dijkstra formula is used to determine the shortest path.

Eg: OSPF, IS-IS



| **BASIS FOR COMPARISON** | **DISTANCE VECTOR ROUTING** | **LINK STATE ROUTING** |
| --- | --- | --- |
| Algorithm | Bellman ford | Dijkstra |
| Network view | Topology information from the neighbour point of view | Complete information on the network topology |
| Best path calculation | Based on the least number of hops | Based on the cost |
| Updates | Full routing table | Link state updates |
| Updates frequency | Periodic updates | Triggered updates |
| CPU and memory | Low utilisation | Intensive |
| Simplicity | High simplicity | Requires a trained network administrator |
| Convergence time | Moderate | Fast |
| Updates | On broadcast | On multicast |
| Hierarchical structure | No | Yes |
| Intermediate Nodes | No | Yes |

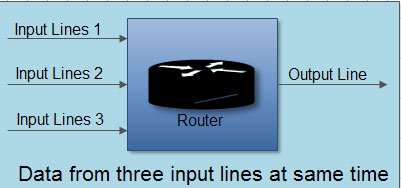
## e. Congestion control and prevention, Leaky-bucket algorithm, Token-bucket algorithm

Congestion Control

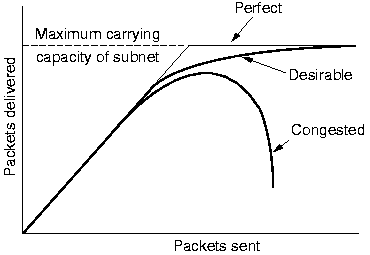
When the no. of packets being transmitted through a link becomes high (generally 80% of capacity), then the performance of the n/w decreases i.e. packets are dropped, this state is called congestion.

Common causes

In a packet switched network each intermediate device takes traffic in its i/p port, buffers it before transmitting out of the o/p port. If the density of incoming traffic is high there may not be enough buffer space to store the incoming traffic leading to packet drops.Even a large buffer space cannot solve the problem since it introduces delay, leading to timeout and retransmission. The slow processing of the intermediate devices. Low network line bandwidth leading to bottleneck.



Effects of Congestion

Ideally the n/w should be able to send data at the full capacity, giving 100% throughput as shown by the ideal curve in fig. 1.But practically, the congestion causes the throughput to decline sharply when the n/w is 80% saturated as shown by uncontrolled curve. The use of congestion control algorithms can prevent this sharp decline in performances and send data efficiently at close to 80% of the n/w capacity as shown by the controlled curve. 

## 

## 

## 

## 

Leaky Bucket Algorithm

It is used to shape bursty rate traffic into fixed rate traffic.

Its working can be compared with a tap with a bursty flow of water. If the water is collected in a bucket with a hole at the bottom for a continuous drainage of water.

Its working as follows as illustrated in the figure below:

1. A host sent data of bursty nature.

2. This data is kept in a storage buffer by the OS or the NIC.

3. This stored data is then sent out to n/w at a uniform rate.

But it has two major disadvantages

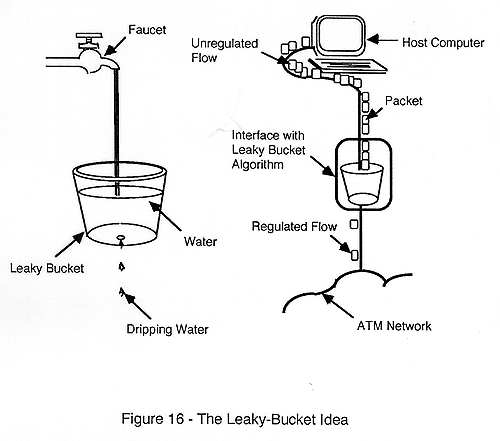
1. Traffic is lost when the bucket is full.

2. The o/p rate is fixed even if there is no congestion.

Algorithm;

The following is an algorithm for variable-length packets:

1. Initialize a counter to n at the tick of the clock.
2. If n is greater than the size of the packet, send the packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size.
3. Reset the counter and go to step 1.



Token Bucket Algorithm

Token buckets were introduced to address the two major drawbacks of leaky buckets i.e. loss of traffic when the bucket is full and fixed o/p rate even in case of no congestion.

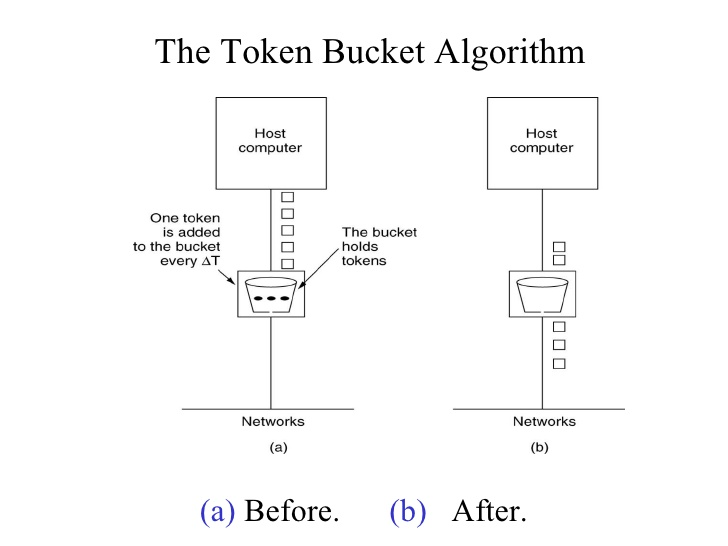
This algorithm works as follow

1. At every tick (or time interval) a token is added in the bucket.

2. Let us say there are 3 tokens at the bucket at a given time when the host sends a bursty data containing 5 packets as shown in figure 1. below.

3. Since the bucket has 3 tokens it can send 3 packets immediately as shown in figure 2 below.

4. The rest of the data are sent at subsequent ticks.



Differentiate between Leaky bucket and Token bucket algorithm

| Leaky Bucket | Token Bucket |
| --- | --- |
| When the host has to send a packet , the packet is thrown in a bucket. | In this leaky bucket holds tokens generated at regular intervals of time. |
| Bucket leaks at constant rate | Bucket has maximum capacity. |
| Bursty traffic is converted into uniform traffic by a leaky bucket. | If there is a ready packet , a token is removed from the Bucket and the packet is sent. |
| In practice bucket is a finite queue outputs at finite rate | If there is no token in the bucket, the packet can not be sent. |

## 

## 

## 

## 

## 

## 

## 

## f. Internetworking, Tunneling and routing, ATM internetworking, Mobile routing schemes

Internetworking

Any interconnection among or between public, private, commercial, industrial, or governmental computer networks may also be defined as an internetwork or “Internetworking“.

1. Extranet – It’s a network of the internetwork that’s restricted in scope to one organization or entity however that additionally has restricted connections to the networks of one or a lot of different sometimes, however not essential. It's the very lowest level of Internetworking, usually enforced in an exceedingly personal area. Associate degree extranet may additionally be classified as a Man, WAN, or different form of network however it cannot encompass one local area network i.e. it should have a minimum of one reference to associate degree external network.
2. Intranet – This associate degree computer network could be a set of interconnected networks, which exploits the Internet Protocol and uses IP-based tools akin to web browsers and FTP tools, that’s underneath the management of one body entity. That body entity closes the computer network to the remainder of the planet and permits solely specific users. Most typically, this network is the internal network of a corporation or different enterprise. An outsized computer network can usually have its own internet server to supply users with browseable data.
3. Internet – A selected Internetworking, consisting of a worldwide interconnection of governmental, academic, public, and personal networks based mostly upon the Advanced analysis comes Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense additionally home to the World Wide Web (WWW) and cited as the ‘Internet’ to differentiate from all different generic Internetworks. Participants within the web, or their service suppliers, use IP Addresses obtained from address registries that management assignments.

Challenges of Internetworking:

* The initial challenge lies when we are trying to connect numerous systems to support communication between disparate technologies. For example, Totally different sites might use different kinds of media, or they could operate at variable speeds.
* Another essential thought is reliable service that should be maintained in an internetwork. Individual users and whole organizations depend upon consistent, reliable access to network resources.
* Network management should give centralized support associate degreed troubleshooting capabilities in an internetwork. Configuration, security, performance, and different problems should be adequately addressed for the internetwork to perform swimmingly.
* Flexibility, the ultimate concern, is important for network enlargement and new applications and services, among different factors.

Tunneling and routing

Tunnels are a method for transporting data across a network using protocols that are not supported by that network. Tunneling works by encapsulating packets: wrapping packets inside of other packets. (Packets are small pieces of data that can be re-assembled at their destination into a larger file.)

Tunneling is often used in virtual private networks (VPNs). It can also set up efficient and secure connections between networks, enable the usage of unsupported network protocols, and in some cases allow users to bypass firewalls.

ATM internetworking

Mobile routing schemes

## g. Network layer protocols: IP, NAT, ICMP, IGMP, RIP, ARP, RARP, OSPF, IGRP, EIGRP, BGP

IP:

An IP address is a unique identifier assigned to a device or domain that connects to the Internet. Each IP address is a series of characters, such as '192.168.1.1'. Via DNS resolvers, which translate human-readable domain names into IP addresses, users are able to access websites without memorizing this complex series of characters. Each IP packet will contain both the IP address of the device or domain sending the packet and the IP address of the intended recipient, much like how both the destination address and the return address are included on a piece of mail.

Network Address Translation (NAT)

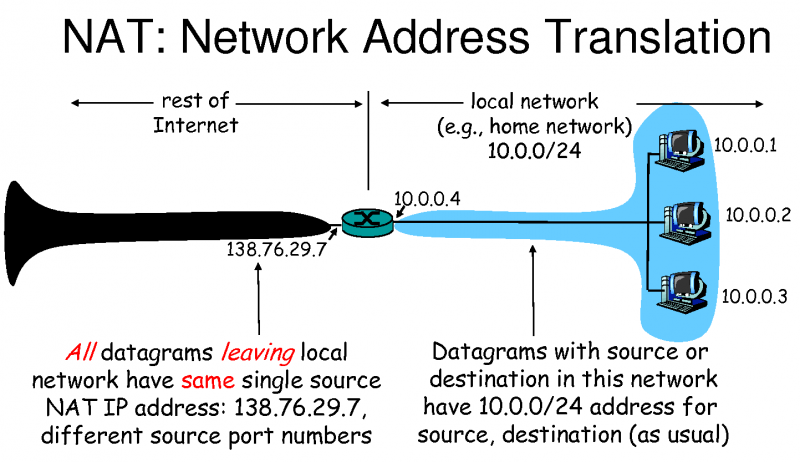
A Network address translation is a process by which an address can be changed into another address. For example an IPv4 address can be translated to IPv6 address.One of the most widely used implementations ofNAT is the conversion of private IP address to public IP address. Since a LAN in an organization uses a private address it cannot access the internet; as a system needs to havean public address to access the internet. But aNAT router converts the private address of theLAN computer to a public address thus allowing for communication with the Internet.

Every computer on the internet has an IP address, e.g., 177.77.10.10. A website has to have a public IP address. So, you can look up www.google.com or yahoo, or any other site.

But, there are only so many IP addresses, and there are lots and lots of computers, phones, playstations, TVs, etc... that need an IP. So, someone, somewhere along the way had the idea of private IPs. Private IPs are in certain ranges. 192.168.X.Y is one such range. Those IPs can only be used for private networks.

Private IPs are valid just on your network. Say you have 3 computers at home connected to a router. Those computers will have private IP addresses. The computers on your network can see each other, but no one outside your network can see those computers, because they don't have public IPs. Your router on the other hand gets a public IP address, and anyone in the world can see your router. So, all of the equipment in your house communicates to outside web sites using that public IP of the router.

This is where NAT comes in. Your computer tries to reach google.com. So, it sends the request out, and your router gets the request. Your router sees that your computer (192.168.1.2) wants to talk to Google. So, your router takes the message you sent, and sends it on itself, pretending that it sent the original messages from <Router's Public IP>. Google replies back, and your router passes the response from google back to your personal computer. That's NAT.



ICMP

The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. Commonly, the ICMP protocol is used on network devices, such as routers.

RIP

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol which has AD value 120 and works on the application layer of OSI model. RIP uses port number 520.

ARP

ARP stands for Address Resolution Protocol. Its functionality is to translate IP address to physical address.

RARP

RARP stands for Reverse Address Resolution Protocol. IT is a protocol based on computer networking which is employed by a client computer to request its IP address from a gateway server’s Address Resolution Protocol table or cache. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.

OSPF

OSPF stands for Open Shortest Path First. Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First.

IGRP

IGRP stands for Interior Gateway Routing Protocol. Interior Gateway Routing Protocol is the routing protocol. It is also a distance vector routing protocol. In this, Bellman ford algorithm is used. The least hop count in IGRP is 255.

EIGRP

EIGRP stands for Enhanced Interior Gateway Routing Protocol. It is a routing protocol like the Interior Gateway Routing Protocol. It is the link state routing protocol as well as vector routing protocol. The main difference between the IGRP and EIGRP is that, Interior Gateway Routing Protocol is Classful routing technique, while Enhanced Interior Gateway Routing Protocol is a classless routing technique.

BGP

BGP stands for Border Gateway Protocol. Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISPs which are different ASes.

The protocol can connect together any internetwork of autonomous system using an arbitrary topology. The only requirement is that each AS have at least one router that is able to run BGP and that is router connect to at least one another AS’s BGP router. BGP’s main function is to exchange network reach-ability information with other BGP systems. Border Gateway Protocol constructs an autonomous systems’ graph based on the information exchanged between BGP routers.

# 5. Transport layer [5 Hrs]

## a. Transport layer design issues

End-to-end delivery of the entire message, addressing, reliable delivery, flow (congestion control) and error control.

Two different types of protocol.

* UDP ( User datagram Protocol) - Connectionless and unreliable.
* TCP (Transport Control Protocol) - Connection oriented and reliable.

Issues in designing transport Layer protocol.

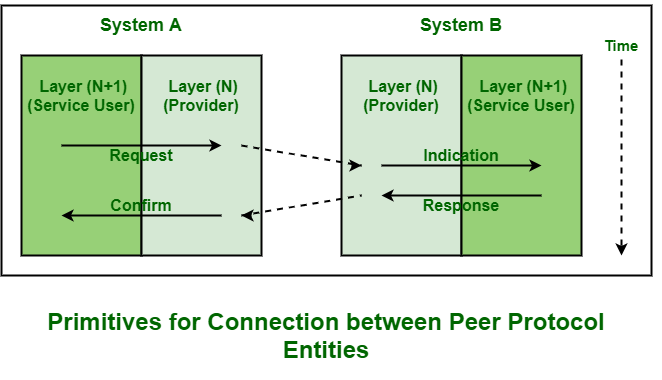
* Induced traffic - Large amount of induced traffic which may affect transport protocol. It will hamper the throughput.
* Power and Bandwidth Constraints - The available resources should be used efficiently.
* Throughput unfairness - If you give the channel unfair advantages. So, it should provide a fair share of throughput across contending flows.
* Interpretation of congestion - That arises when two or more stations who are out of range of each other transmit simultaneously to a common recipient. It will affect the transport layer protocol performance.
* Dynamic Topology - Mobility of nodes, intermediate path in the nodes may move cause delay in package.

## b. Service primitive, QoS

A primitive simply means Operations. A Service is specified by a set of primitives that are available and given to users or other various entities to access the service. All these primitives simply tell the service to perform some action or to report on action that is taken by a peer entity.

Classification of Service Primitives :

* Request - It represents an entity that wants or requests service to perform some action or do some work (requesting for connection to a remote computer).
* Indication - It represents an entity that is to be informed about an event (receiver just has received a request for connection).
* Response - It represents an entity that is responding to an event (receiver is simply sending the permission or allowing to connect).
* Confirm - It represents an entity that acknowledges the response to earlier requests that have come back (sender just acknowledges the permission to get connected to the remote host).



In the above diagram, these four primitives work as following :

* Request –

This primitive is transferred or sent to Layer N by Layer (N+1) to just request for service.

* Indication –

This primitive is returned by Layer N to Layer (N+1) to just advise of activation of service that is being requested or of action that is initiated by the service of Layer N.

* Response –

This primitive is simply provided by Layer (N+1) in reply to indication primitive. It might acknowledge or complete action that is previously invoked by indication primitive.

* Confirm –

This primitive is returned by the Nth layer to the requesting (N+1)st layer to simply acknowledge or complete action that is previously invoked by request primitive.

Some of the Service Primitives need parameters. These are given below :

* Connect. Request –

The initiating entity does this Connect.Request. It just specifies and determines the machine that we want to get connected to, type of service that is being desired, and maximum size of packet or message that is used on connection.

* Connect. Indication –

The receiver gets this Connect.Indication. It just specifies caller’s identity service that we want to use like FTP and Telnet, etc., and maximum size of packets that are exchanged.

* Connect. Response –

It just specifies whether or not it wants to accept or simply reject the connection that is being requested.

* Connect. Confirm –

It just finds out or determines what happened using the entity that is issuing the initial Connect. Request.

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

Need for QoS –

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

QoS Specification –

QoS requirements can be specified as:

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

There are two types of QoS Solutions:

* Stateless Solutions –

Routers maintain no fine grained state about traffic, one positive factor of it is that it is scalable and robust. But it has weak services as there is no guarantee about the kind of delay or performance in a particular application which we have to encounter.

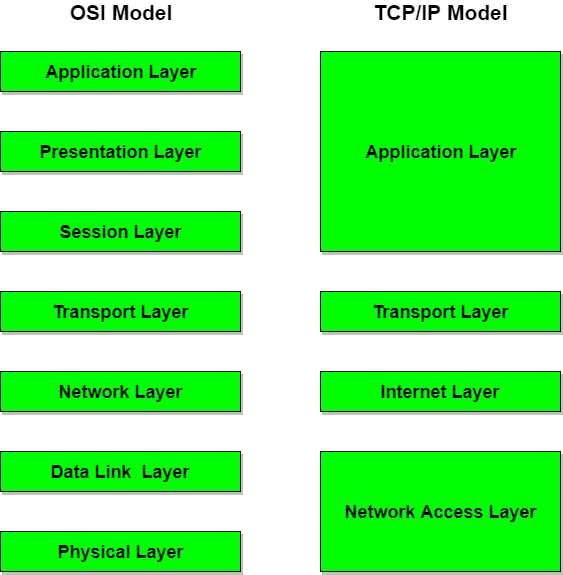
* Stateful Solutions –

Routers maintain per flow state as flow is very important in providing the Quality-of-Service i.e. providing powerful services such as guaranteed services and high resource utilization, provides protection and is much less scalable and robust.

## c. Connection-oriented and connectionless networks

| S.NO | Connection-oriented Service | Connectionless Service |
| --- | --- | --- |
| 1. | Connection-oriented service is related to the telephone system. | Connection-less service is related to the postal system. |
| 2. | Connection-oriented service is preferred by long and steady communication. | Connection-less Service is preferred by bursty communication. |
| 3. | Connection-oriented Service is necessary. | Connection-less Service is not compulsory. |
| 4. | Connection-oriented Service is feasible. | Connection-less Service is not feasible. |
| 5. | In connection-oriented Service, Congestion is not possible. | In connection-less Service, Congestion is possible. |
| 6. | Connection-oriented Service gives the guarantee of reliability. | Connection-less Service does not give the guarantee of reliability. |
| 7. | In connection-oriented Service, Packets follow the same route. | In connection-less Service, Packets do not follow the same route. |
| 8. | Connection-oriented Services requires a bandwidth of high range. | Connection-less Service requires a bandwidth of low range. |

## d. Transport layer protocols: TCP and UDP



Layer 1: Network Layer

The network access layer is responsible for exchanging data between a host and the network and for delivering data between two devices on the same network. Node physical addresses are used to accomplish delivery on the local network. Functions performed at this level include encapsulation of IP datagrams(i.e. the packet format defined by Internet Protocol.) into the frames transmitted by the network, and the mapping of IP addresses into the physical addresses used by the network. The TCP/IP Network Access Layer can encompass the function of all three lower layers of the OSI reference model (Network Layer, Data Link Layer, and Physical Layer.)

Layer 2 : Internet Layer

The internet layer is responsible for sending source packets from any network on the internetwork and have them arrive at their destination regardless of the path they took. The Internet Protocol (IP) is used in this layer and it provides the packet delivery service on which the TCP/IP is based. The IP protocol implements a system of logical host addresses called IP addresses. The IP addresses are used by the internet and higher layers to identify devices and to perform internetwork routing.

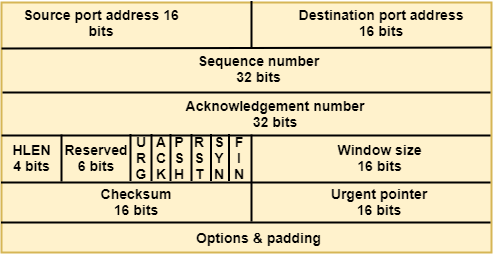
Layer 3: Transport Layer

The transport layer is responsible for the reliability, flow control, and error correction of data being sent across the network.Its main protocol is called the transmission control protocol (TCP). TCP provides reliable data delivery service with end-to-end error detection and correction.User Datagram Protocol (UDP) is another protocol used which provides slow-overhead, connectionless datagram delivery service.UDP is unreliable but enhances network throughput when error correction is not required at the host-to-host-layer. Both protocols deliver data between the Application Layer and the Internet Layer. The users may choose either best suited to their means.

Layer 4 : Application Layer

The application layer is responsible for handling high-level protocols, issues of representation, encoding and dialog control. This layer is broadly equivalent to the application, presentation and session layers of the OSI model. It gives an application access to the communication environment. Examples of protocols found at this layer are Telnet, FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol), HTTP (HyperText Transfer Protocol) and SMTP (Simple Mail Transfer Protocol).

TCP Segment Format



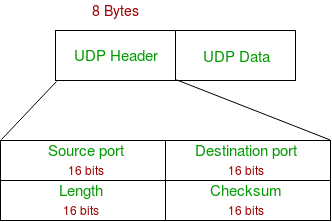
* Source port address: It is used to define the address of the application program in a source computer. It is a 16-bit field.
* Destination port address: It is used to define the address of the application program in a destination computer. It is a 16-bit field.
* Sequence number: A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.
* Acknowledgement number: A 32-field acknowledgement number acknowledges the data from other communicating devices. If the ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
* Header Length (HLEN): It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
* Reserved: It is a six-bit field which is reserved for future use.
* Control bits: Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

There are total six types of flags in control field:

* URG: The URG field indicates that the data in a segment is urgent.
* ACK: When the ACK field is set, then it validates the acknowledgement number.
* PSH: The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput.
* RST: The reset bit is used to reset the TCP connection when there is any confusion in the sequence numbers.
* SYN: The SYN field is used to synchronize the sequence numbers in three types of segments: connection request, connection confirmation ( with the ACK bit set ), and confirmation acknowledgement.
* FIN: The FIN field is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments: termination request, termination confirmation, and acknowledgement of termination confirmation.
* Window Size: The window is a 16-bit field that defines the size of the window.
* Checksum: The checksum is a 16-bit field used in error detection.
* Urgent pointer: If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.
* Options and padding: It defines the optional fields that convey the additional information to the receiver.

User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as the UDP/IP suite. Unlike TCP, it is unreliable and connectionless protocol. So, there is no need to establish connection prior to data transfer. UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also saves bandwidth. User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

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



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

| Basis for Comparison | TCP | UDP |
| --- | --- | --- |
| Definition | TCP establishes a virtual circuit before transmitting the data. | UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not. |
| Connection Type | It is a Connection-Oriented protocol | It is a Connectionless protocol |
| Speed | slow | high |
| Reliability | It is a reliable protocol. | It is an unreliable protocol. |
| Header size | 20 bytes | 8 bytes |
| acknowledgement | It waits for the acknowledgement of data and has the ability to resend the lost packets. | It neither takes the acknowledgement, nor it retransmits the damaged frame. |

## e. Elements of transport layer

Transport <> Data Link

Addressing

Establishing a connection

Releasing a connection

Flow control and buffering

Multiplexing

Crash recovery

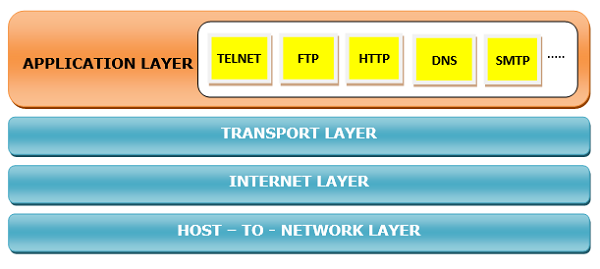
# 6. Application layer [5 Hrs]

## a. Application layer and its function

The application layer is the highest abstraction layer of the TCP/IP model that provides the interfaces and protocols needed by the users. It combines the functionalities of the session layer, the presentation layer and the application layer of the OSI model.

The functions of the application layer are −

* It facilitates the user to use the services of the network.
* It is used to develop network-based applications.
* It provides user services like user login, naming network devices, formatting messages, and e-mails, transfer of files etc.
* It is also concerned with error handling and recovery of the message as a whole.



## b. Electronic mail: SMTP

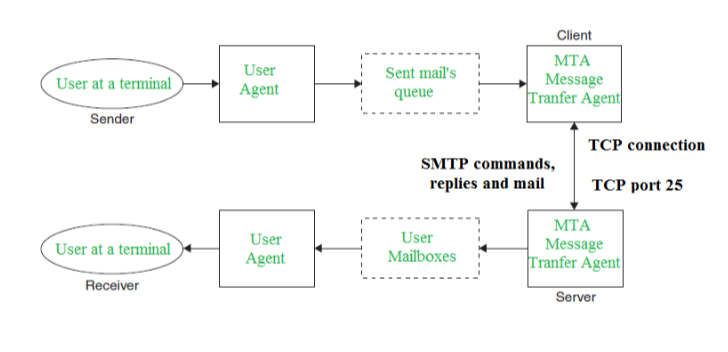
SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver’s side.

SMTP Fundamentals

SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port (25). After successfully establishing the TCP connection the client process sends the mail instantly.

Model of SMTP system

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



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

* User agent (UA)
* Local MTA

Some SMTP Commands:

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

## c. File transfer: FTP, Telnet

FTP

File Transfer Protocol (FTP) [TCP Port 20,11]

FTP refers to a network protocol responsible for transferring files from one computer to another over a TCP computer network or the Internet. Transferring files from a client computer to a server computer is called "uploading" and transferring from a server to a client is "downloading".

FTP uses one connection for commands and the other for sending and receiving data. FTP has a standard port number on which the FTP server "listens" for connections. The standard port number used by FTP servers is 21 and is used only for sending commands. Since port 21 is used exclusively for sending commands, this port is referred to as a command port. For example, to get a list of folders and files present on the FTP server, the FTP Client issues a "LIST" command. The FTP server then sends a list of all folders and files back to the FTP Client.

Some common ftp commands are

Cd: Change the directory on the remote computer.

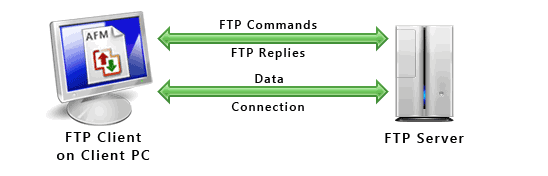
Close: Close the connection to the remote computer.

Del: Delete files from the remote computer.

Rmdir: Remove a directory on the remote host

Bye (or quit): Close the connection to the remote computer and exit FTP.

So what about the internet connection used to send and receive data? The port that is used for transferring data is referred to as a data port. The port used for sending data is port 20.



## d. Dynamic host configuration protocol (DHCP)

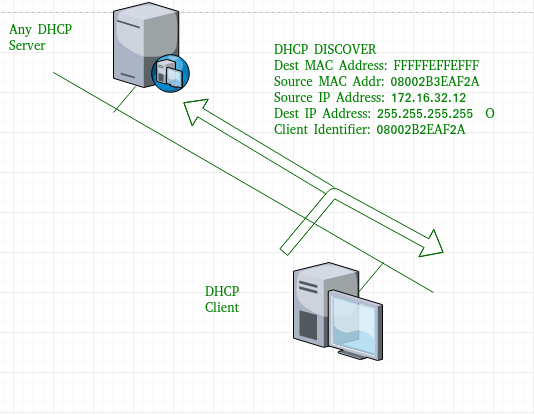
Dynamic Host Configuration Protocol(DHCP) is an application layer protocol which is used to provide:

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

DHCP is based on a client-server model and based on discovery, offer, request, and ACK.

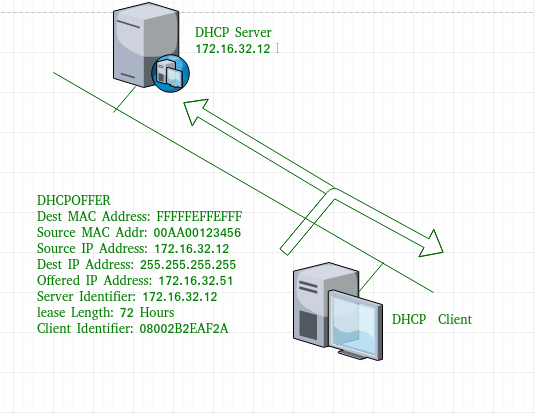
The DHCP port number for the server is 67 and for the client is 68. It is a Client server protocol which uses UDP services. IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called DORA process, but there are 8 DHCP messages in the process. These message are given below:

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



As shown in the figure, source MAC address (client PC) is 08002B2EAF2A, destination MAC address(server) is FFFFFFFFFFFF, source IP address is 0.0.0.0(because PC has no IP address till now) and destination IP address is 255.255.255.255 (IP address used for broadcasting). As the discovery message is broadcast to find out the DHCP server or servers in the network therefore broadcast IP address and MAC address is used.

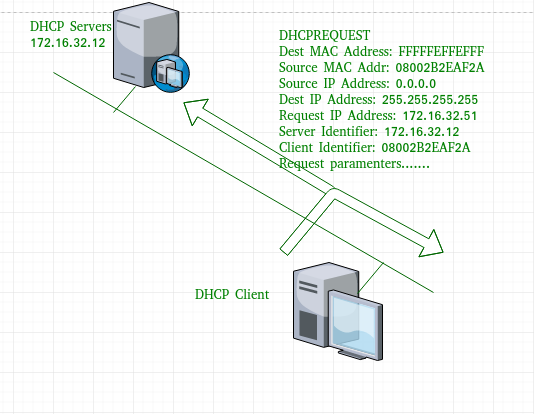
1. DHCP offer message
   * The server will respond to the host in this message specifying the unleashed IP address and other TCP configuration information. This message is broadcasted by the server. Size of the message is 342 bytes. If there are more than one DHCP servers present in the network then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



Now, for the offer message, source IP address is 172.16.32.12 (server’s IP address in the example), destination IP address is 255.255.255.255 (broadcast IP address) ,source MAC address is 00AA00123456, destination MAC address is FFFFFFFFFFFF. Here, the offer message is broadcast by the DHCP server therefore destination IP address is broadcast IP address and destination MAC address is FFFFFFFFFFFF and the source IP address is server IP address and MAC address is server MAC address.

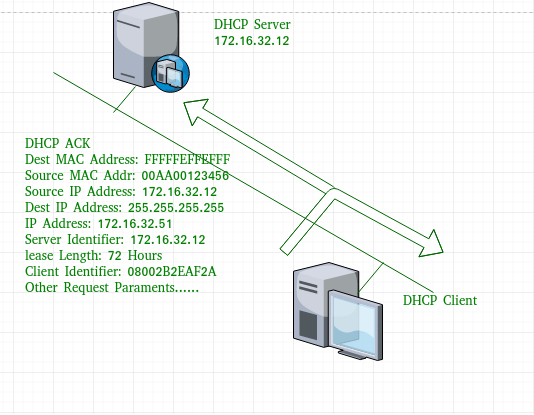
Also the server has provided the offered IP address 192.16.32.51 and lease time of 72 hours(after this time the entry of the host will be erased from the server automatically) . Also the client identifier is PC MAC address (08002B2EAF2A) for all the messages.

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



Now, the request message is broadcast by the client PC therefore source IP address is 0.0.0.0(as the client has no IP right now) and destination IP address is 255.255.255.255 (broadcast IP address) and source MAC address is 08002B2EAF2A (PC MAC address) and destination MAC address is FFFFFFFFFFFF.

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



Now the server will make an entry of the client host with the offered IP address and lease time. This IP address will not be provided by the server to any other host. The destination MAC address is FFFFFFFFFFFF and the destination IP address is 255.255.255.255 and the source IP address is 172.16.32.12 and the source MAC address is 00AA00123456 (server MAC address).

1. DHCP negative acknowledgement message
   * Whenever a DHCP server receives a request for an IP address that is invalid according to the scopes that it is configured with, it sends the DHCP Nak message to the client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to client.
2. DHCP decline
   * If DHCP client determines the offered configuration parameters are different or invalid, it sends DHCP decline message to the server .When there is a reply to the gratuitous ARP by any host to the client, the client sends DHCP decline message to the server showing the offered IP address is already in use.
3. DHCP release
   * A DHCP client sends a DHCP release packet to the server to release the IP address and cancel any remaining lease time.
4. DHCP inform
   * If a client address has obtained IP address manually then the client uses a DHCP inform to obtain other local configuration parameters, such as domain name. In reply to the dhcp inform message, DHCP server generates DHCP ack message with local configuration suitable for the client without allocating a new IP address. This DHCP back message is unicast to the client.

## e. DNS, HTTP, WWW, SNMP

Domain Name System (DNS) [TCP/UDP Port 53]

DNS or Domain Name System is an application that allows us to find the ip address of a domain name.Let us say that we want to access www.abc.com from our browser then, the chain of events to get the IP address for www.abc.com are

First your computer queries the name server (DNS server) it is set up to use. This is the recursive name server shown above.

The name server doesn’t know the IP address for www.abc.com, so it will start the following chain of queries before it can report back the IP address to your computer (the numbers below correspond to the numbers in the image).

1. Query the Internet root servers to get the name servers for the .com TLD.

2. Query the .com TLD name servers to get the authoritative name servers for abc.com.

3. Query the authoritative name servers for abc.com to finally get the IP address for the host www.abc.com, then return that IP address to your computer.

4. Done! Now that your computer has the IP address for www.abc.com, it can access that host.

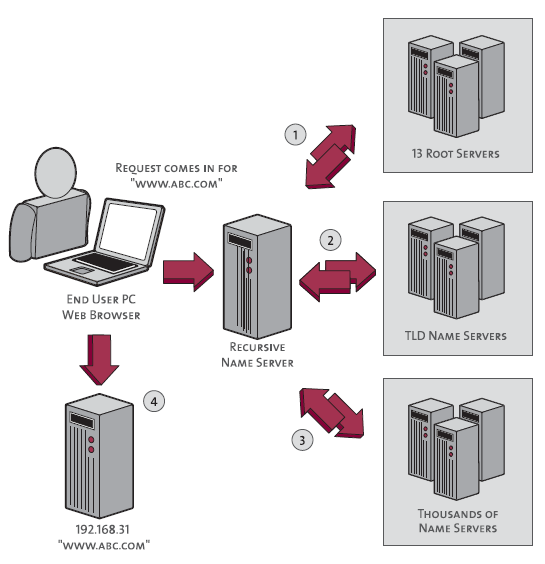
The basic records provided by DNS are:

A (Address): Host IP addresses.

CNAME (Canonical Name): Defines a host alias.

MX (Mail Exchange): Identifies where to send mail for a given domain name.

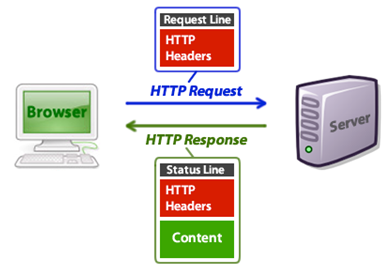
NS (Name Server): Identifies a domain's name servers



HyperText Transfer Protocol (HTTP)

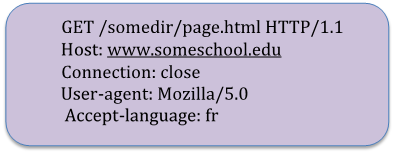
It's a protocol by which hypertext (that is, the content of a web page) is transferred between a web server and your machine.

Whenever a web client (web browser) needs to get a web object from a web server, it needs to send a GET request for that object. The GET request is included in the HTTP header. After receiving the request the server sends the HTTP response message requested object if available.



## HTTP Message Format

1. The web client makes a request for an object with a GET Request in the HTTP header. The basic structure of HTTP GET is as follow;



The first line of an HTTP request message is called the request line; the subsequent lines are called the header lines. The request line has three fields: the method field, the URL field, and the HTTP version field. The method field can take on several different values, including GET, POST, HEAD, PUT, and DELETE. The browser is requesting the object /somedir/page.html. And the browser is requesting using HTTP version 1.1.

The header line Host: www.someschool.edu specifies the host on which the object resides. The Connection:close header line tells the browser not to implement persistent connection. The User-agent Mozilla/5.0 tells that the request is made using Mozilla browser version 5.0. The last line tells the preferred language.

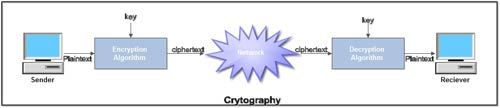
Http Cookies

A cookie is a small file that is stored on a user pc by the web server. The HTTP cookie is there to remember helpful information on that page or website. If you put items into your shopping cart on Amazon you are adding information of those items to a cookie that is stored so if you leave and come back you still have those stored in your shopping cart page. They are also common for letting each page know if the user is logged in, and to which account they are logged in with.

# 7. Network security [4 Hrs]

## a. Cryptography, digital signature

Cryptography is a technique to provide message confidentiality. The term cryptography is a Greek word which means “secret writing”. It is an art and science of transforming messages so as to make them secure and immune to attacks. Cryptography involves the process of encryption and decryption. This process is depicted.



• The terminology used in cryptography is given below:

1. Plaintext. The original message or data that is fed into the algorithm as input is called plaintext.

2. Encryption algorithm. The encryption algorithm is the algorithm that performs various substitutions and transformations on the plaintext. Encryption is the process of changing plaintext into cipher text.

3. Ciphertext. Ciphertext is the encrypted form of the message. It is the scrambled message produced as output. It depends upon the plaintext and the key.

4. Decryption algorithm. The process of changing Ciphertext into plaintext is known as decryption. Decryption algorithm is essentially the encryption algorithm run in reverse. It takes the Ciphertext and the key and produces the original plaintext.

5. Key. It also acts as input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key. Thus a key is a number or a set of numbers that the algorithm uses to perform encryption and decryption.

Features Of Cryptography are as follows:

* Confidentiality:

Information can only be accessed by the person for whom it is intended and no other person except him can access it.

* Integrity:

Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

* Non-repudiation:

The creator/sender of information cannot deny his or her intention to send information at a later stage.

* Authentication:

The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography:

In general there are three types Of cryptography:

* Symmetric Key Cryptography:

It is an encryption system where the sender and receiver of messages use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange keys in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

* Hash Functions:

There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

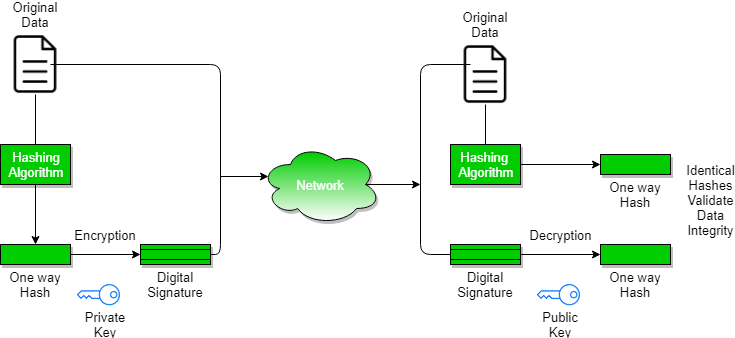
* Asymmetric Key Cryptography:

Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

The steps followed in creating digital signature are :

* Message digest is computed by applying a hash function on the message and then message digest is encrypted using the private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)).
* Digital signature is then transmitted with the message.(message + digital signature is transmitted)
* Receiver decrypts the digital signature using the public key of sender.(This assures authenticity,as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender’s public key).
* The receiver now has the message digest.
* The receiver can compute the message digest from the message (actual message is sent with the digital signature).
* The message digest computed by the receiver and the message digest (got by decryption on digital signature) need to be the same for ensuring integrity.



Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver’s identity to the sender.

A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder.

## b. Firewalls

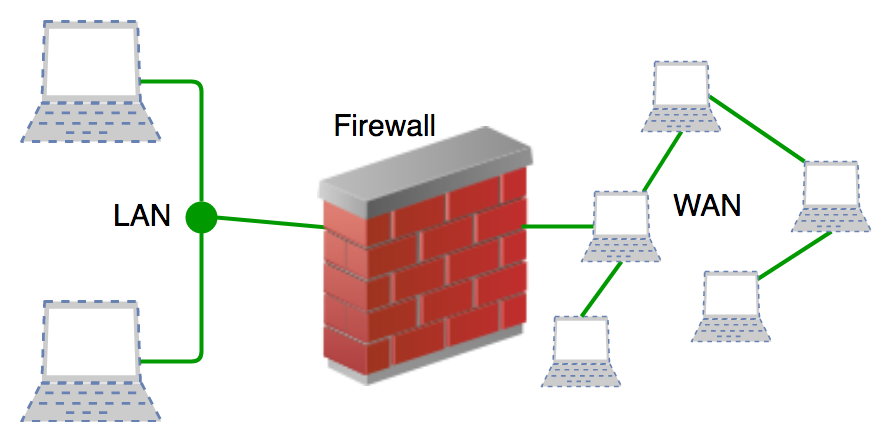
A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic

Reject : block the traffic but reply with an “unreachable error”

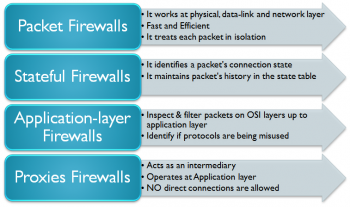
Drop : block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted networks, such as the Internet.



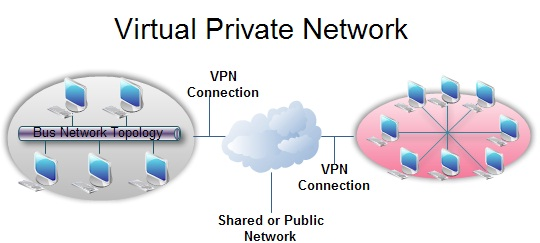
Firewalls are generally of two types: Host-based and Network-based.

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



## c. Virtual private network

VPN means that it is a private point-to-point connection between two machines or networks over a shared or public network such as the internet. A Virtual Private Network is a combination of software and hardware. VPN (Virtual Private Network) technology can be used in organizations to extend its safe encrypted connection over less secure internet to connect remote users, branch offices, and partner private, internal networks. VPN turns the Internet into a simulated private WAN. A VPN client uses TCP/IP protocol, that is called tunneling protocols, to make a virtual call to a VPN server.



The benefits of VPN are as follows:

• Security: The VPN should protect data while it’s travelling on the public network. If intruders attempt to capture data, they should be unable to read or use it.

• Reliability: Employees and remote offices should be able to connect to VPN. The virtual network should provide the same quality of connection for each user even when it is handling the maximum number of simultaneous connections.

• Cost Savings: Its operational cost is less as it transfers the support burden to the service providers.

• It reduces the long-distance telephone charges.

• It cut technical support.

• It eliminates the need for expensive private or leased lines.

• Its management is straightforward.

• Scalability: growth is flexible, i.e., we can easily add new locations to the VPN.

• It is efficient with broadband technology.

• By using VPN, the equipment cost is also reduced.

The difficulties of VPN are as follows:

• For VPN networks to establish, we require an in-depth understanding of the public network security issues.

• VPNs need to accommodate complicated protocols other than IP.

• There is a shortage of standardisation. The product from different vendors may or may not work well together.

• The reliability and performance of an Internet-based private network depend on uncontrollable external factors, which is not under an organisation’s direct control.

Virtual Private Network (VPN) is basically of 2 types:

* Remote Access VPN:

Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both. An employee of a company, while he/she is out of station, uses a VPN to connect to his/her company’s private network and remotely access files and resources on the private network. Private users or home users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users aware of Internet security also use VPN services to enhance their Internet security and privacy.

* Site to Site VPN:

A Site-to-Site VPN is also called a Router-to-Router VPN and is commonly used in large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

* + Intranet based VPN: When several offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.
  + Extranet based VPN: When companies use Site-to-site VPN type to connect to the office of another company, it is called Extranet based VPN.

# Reference Link

* <https://www.youtube.com/watch?v=VwN91x5i25g&list=PLBlnK6fEyqRgMCUAG0XRw78UA8qnv6jEx>
* <https://ecomputernotes.com/computernetworkingnotes/communication-networks/error-control>
* <https://www.geeksforgeeks.org/types-of-virtual-private-network-vpn-and-its-protocols/>
* <https://www.geeksforgeeks.org/service-primitives/#:~:text=A%20primitive%20simply%20means%20Operations,is%20taken%20by%20peer%20entity>.
* <https://www.youtube.com/watch?v=fUCBrd4zLeU>
* <https://www.youtube.com/watch?v=UwERCzJv-y8&list=PLBlnK6fEyqRgMCUAG0XRw78UA8qnv6jEx&index=45>
* <https://www.geeksforgeeks.org/tcp-ip-model/>
* <https://www.geeksforgeeks.org/user-datagram-protocol-udp/>
* <https://www.geeksforgeeks.org/introduction-of-mac-address-in-computer-network/>
* <https://www.educba.com/firewall-uses/>