**Computer Network (CST-102)**

**Part 2**

**By Dr. Ramamani Tripathy**

Networking devices

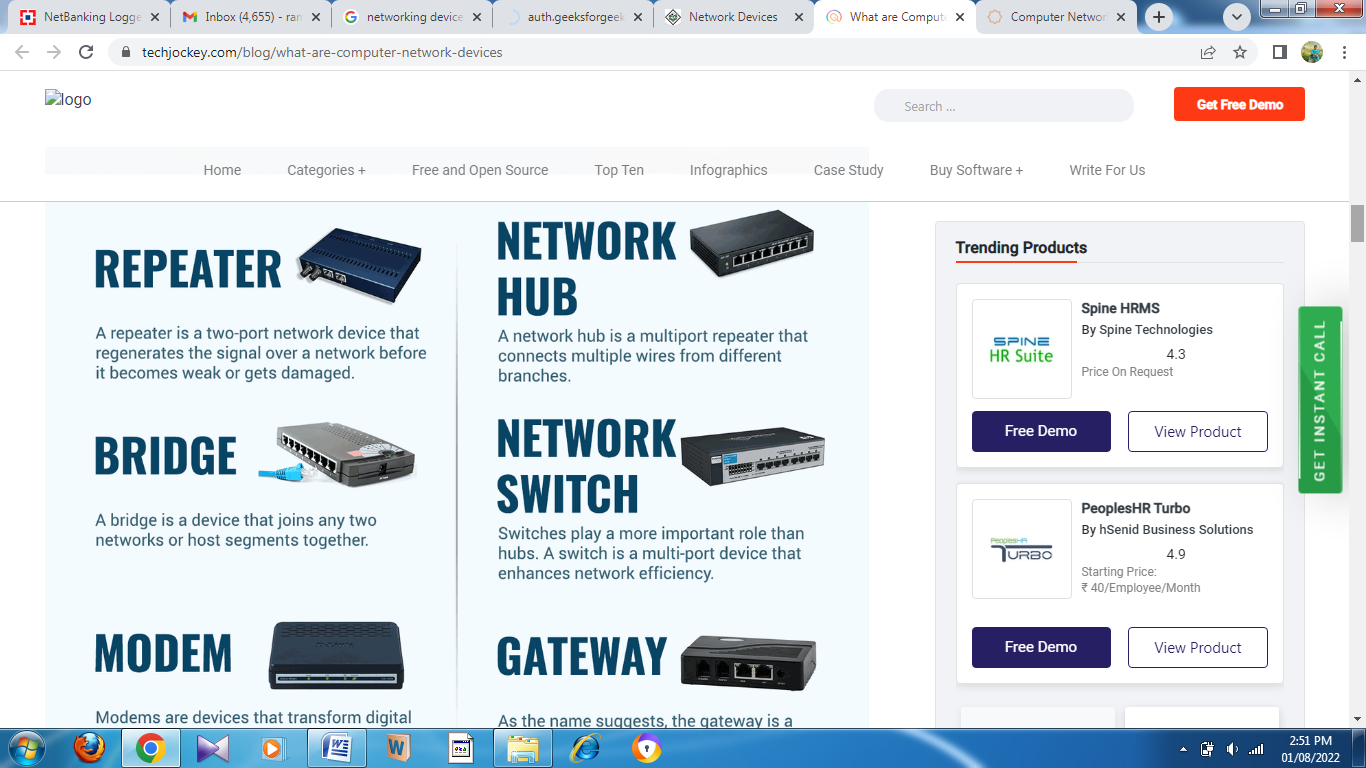
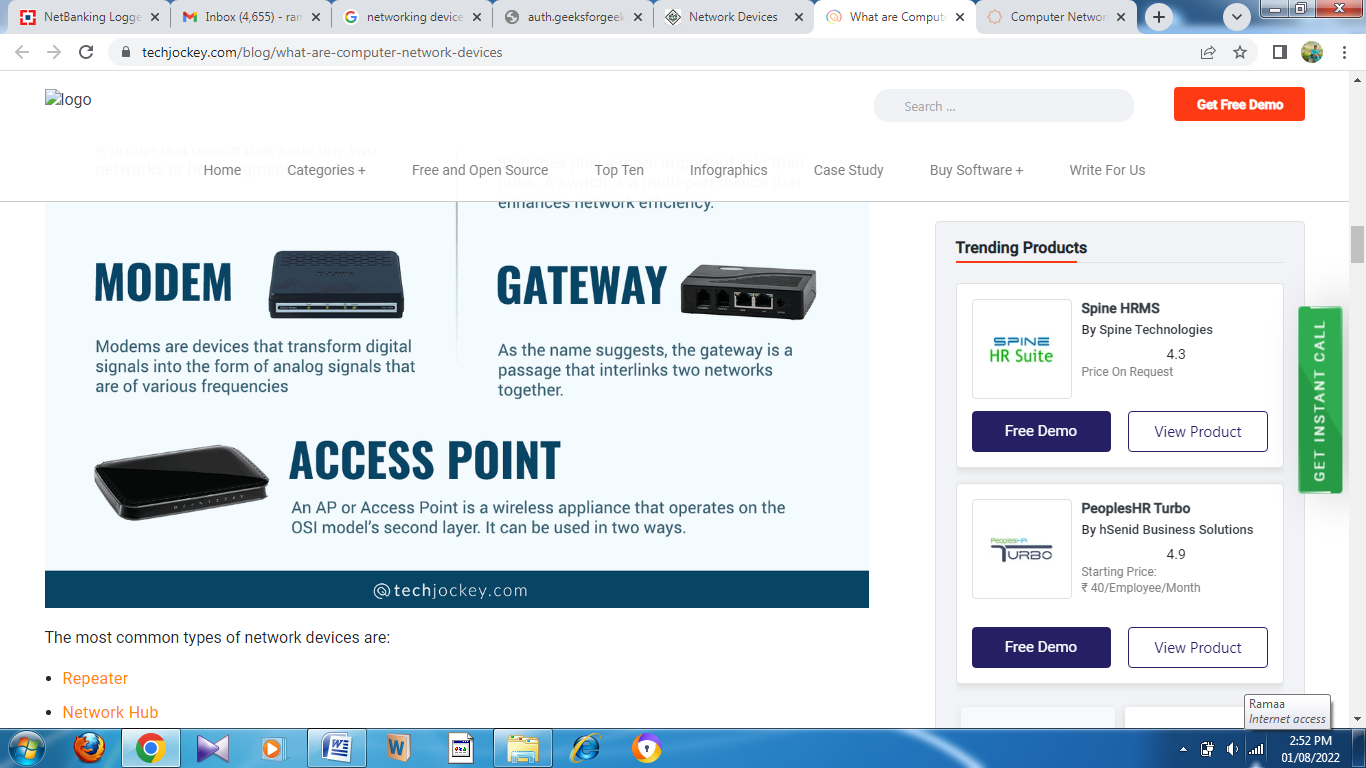
Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called **network devices**. These devices transfer data in a fast, secure and correct way over same or different networks. Network devices may be inter-network or intra-network. Some devices are installed on the device, like NIC card or RJ45 connector, whereas some are part of the network, like router, switch, etc.

**Purpose of Networking Devices**

When there are a large number of devices in a network, too many data packets get transmitted over the same network path. This can lead to congestion and degradation in performance.

The purpose of networking devices is to enable smooth communication between different hardware connected to a network. Addition of a network device helps in hassle free sharing of network resources between different systems.

While computer network devices like hubs send network data to all connected devices, intelligent network devices like routers not only have a fixed source and destination system but they also choose the most efficient route to transmit data.



### Repeater

t It extends the length of the signal and allows it to transmit over the same network. In other words, it simply copies the signal bit by bit and re-generates at its original strength by operating at the physical layer.

### Network Hub

A network hub is a multiport repeater that connects multiple wires from different branches. It is used to transfer important data and communicate among diverse network hosts.

Hub transfers the data as packets through a computer network. When the data processing is done from one host to another network hub, it gets transmitted to all the connected ports.

### Bridge

A bridge is a device that joins any two networks or host segments together. Its primary function in a networking architecture is to store and relay frames among the various connected segments.

They transfer frames using the MAC or the Media Access Control. It can also prevent data crossing if the MAC addresses are wrong. Besides, it also links different physical LANs together to form a bigger logical LAN.

### Network Switch

Switches play a more important role than hubs. A switch is a multi-port device that enhances network efficiency. It provides limited routing information about nodes in the internal network and allows systems to connect.

Network switches can read the hardware address of incoming data packets and transmit them to the applicable destination. A multilayer switch is a high-performance device that supports routing protocols like routers.

### Modem

Modems are devices that transform digital signals into the form of analog signals that are of various frequencies. Then it sends the analog signals to receivers.

Afterward, receiver modems reverse the process and send a digital signal to linked devices like phones and laptops. Telephone companies and cable operators sometimes use modems as the end terminals to identify residential and business customers.

### Gateway

As the name suggests, the gateway is a passage that interlinks two networks together. It works as the messenger agent that takes data from one system, interprets it, and transfers it to another system. Gateways are also called protocol converters, and they can operate at various network layers.

### Access Point

First, as a regular wired network for wireless devices. Second, like a router for transferring data between different access points.

The AP has various ports to expand the network’s size, firewall capabilities, and DHCP service. As a result, we have access points that act as a switch, DHCP server, router, and firewall.

# Switching techniques

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

**Classification Of Switching Techniques**

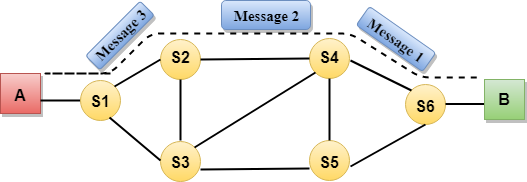


## Circuit Switching

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

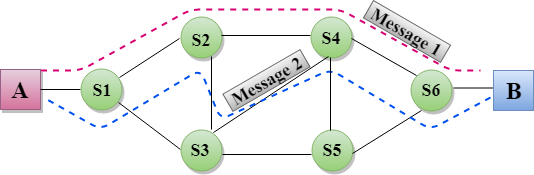
**Communication through circuit switching has 3 phases:**

* Circuit establishment
* Data transfer
* Circuit Disconnect



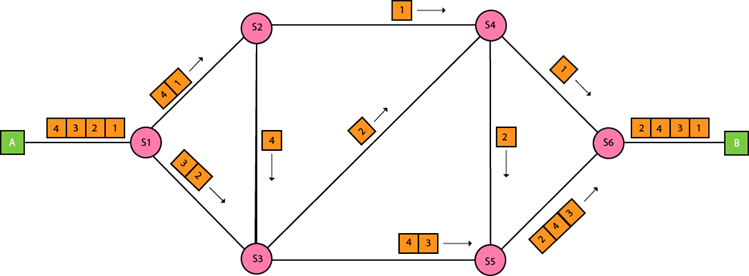
## Message Switching

* Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
* In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
* The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
* Message switches are programmed in such a way so that they can provide the most efficient routes.
* Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
* Message switching treats each message as an independent entity.



## Packet Switching

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



## Approaches Of Packet Switching:

There are two approaches to Packet Switching:

### Datagram Packet switching:

* It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
* The packets are reassembled at the receiving end in correct order.
* In Datagram Packet Switching technique, the path is not fixed.
* Intermediate nodes take the routing decisions to forward the packets.
* Datagram Packet Switching is also known as connectionless switching.

### Virtual Circuit Switching

* Virtual Circuit Switching is also known as connection-oriented switching.
* In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
* Call request and call accept packets are used to establish the connection between sender and receiver.
* In this case, the path is fixed for the duration of a logical connection.

## Differences b/w Datagram approach and Virtual Circuit approach

|  |  |
| --- | --- |
| Datagram approach | Virtual Circuit approach |
| Node takes routing decisions to forward the packets. | Node does not take any routing decision. |
| Congestion cannot occur as all the packets travel in different directions. | Congestion can occur when the node is busy, and it does not allow other packets to pass through. |
| It is more flexible as all the packets are treated as an independent entity. | It is not very flexible. |

# Error Detection

**Error**  
A condition when the receiver’s information does not match with the sender’s information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.

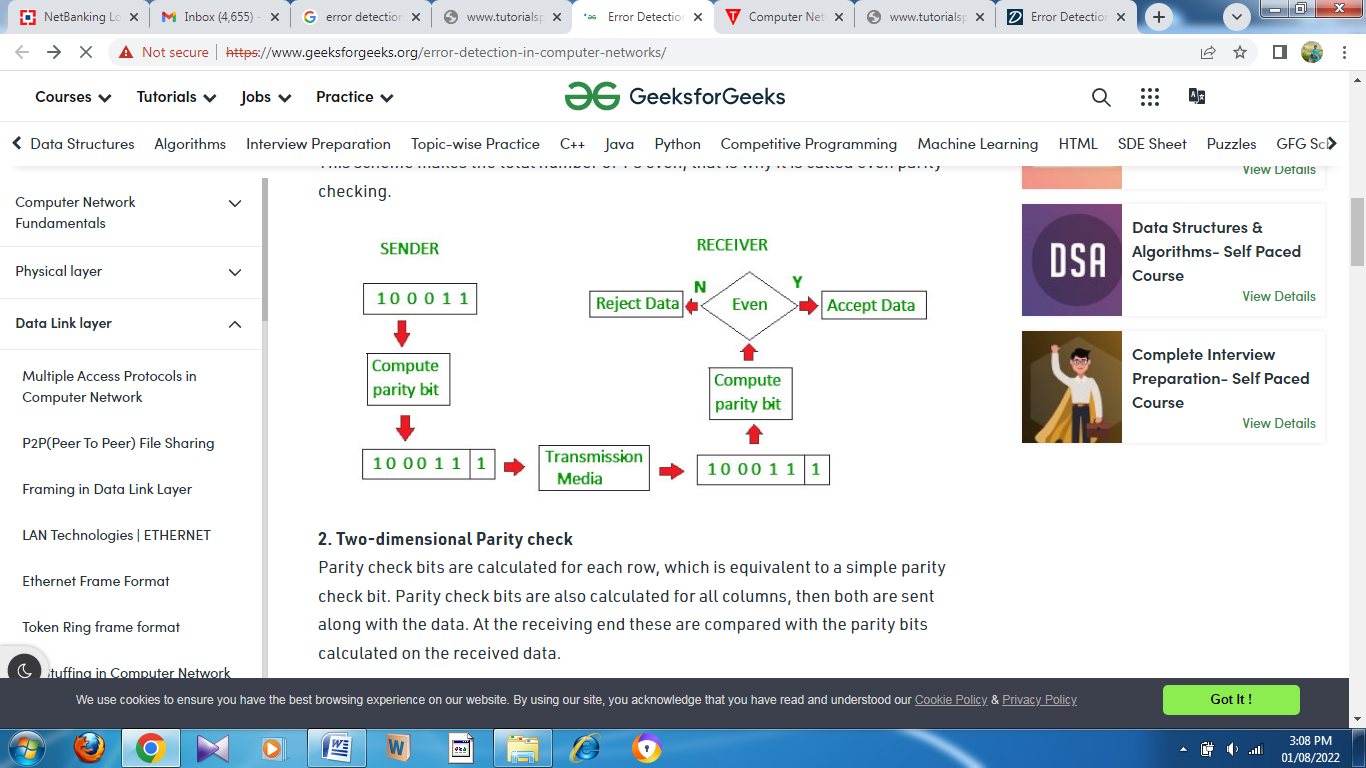
Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors.

Some popular techniques for error detection are:  
1. Simple Parity check  
2. Two-dimensional Parity check  
3. Checksum  
4. Cyclic redundancy check

**1. Simple Parity check**  
Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

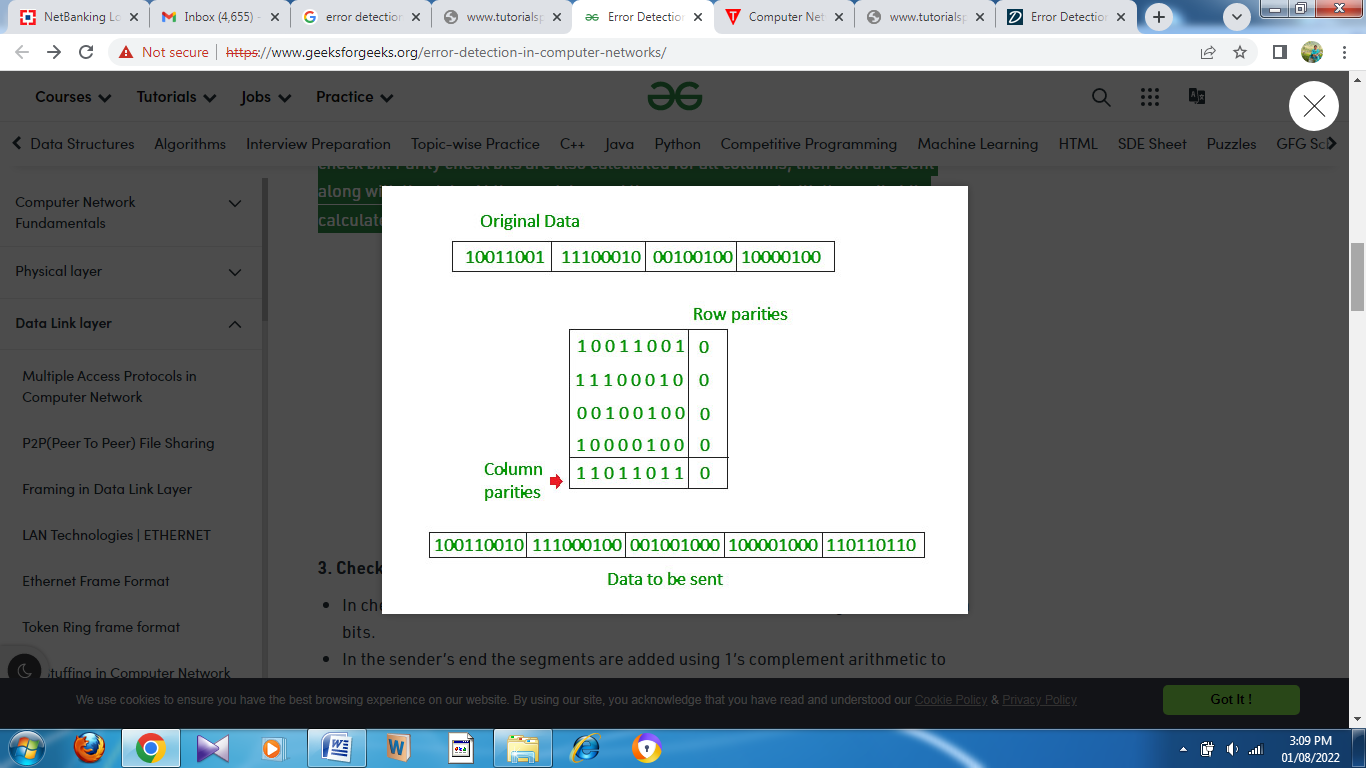
* 1 is added to the block if it contains odd number of 1’s, and
* 0 is added if it contains even number of 1’s

This scheme makes the total number of 1’s even, that is why it is called even parity checking.



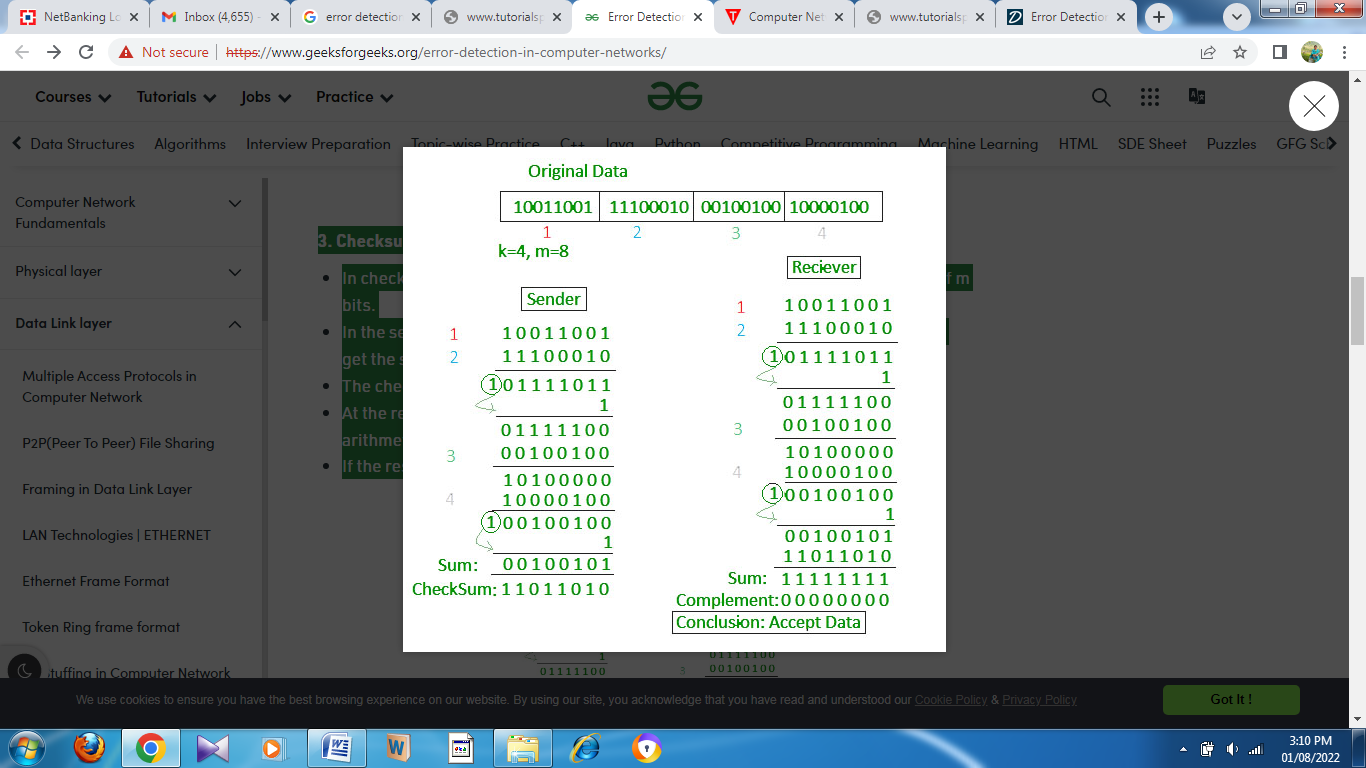
**2.Two-dimensionalParitycheck**

Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.



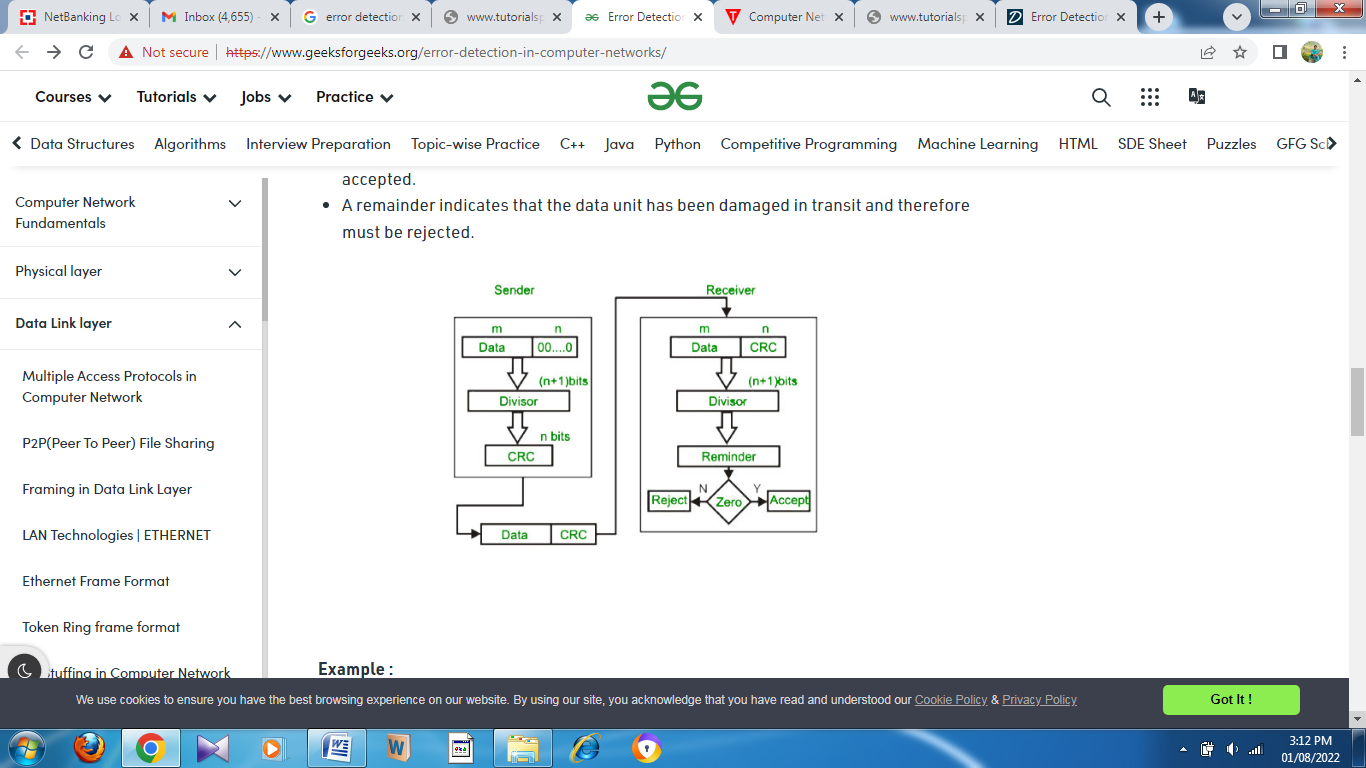
**3. Checksum**

* In 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.

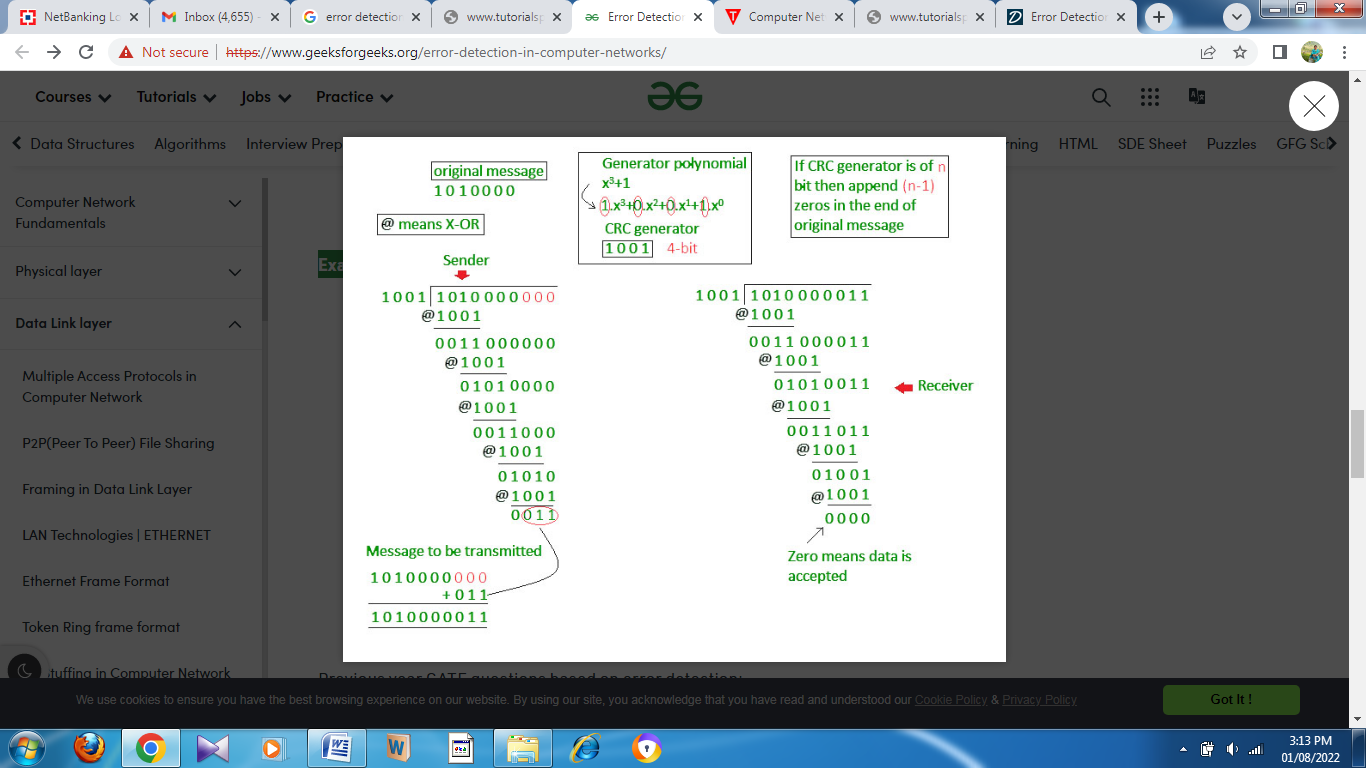


**4. Cyclic redundancy check (CRC)**

* Unlike checksum scheme, which is based on addition, CRC is based on binary division.
* In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
* At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
* A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.



**Example :**



# MAC Address

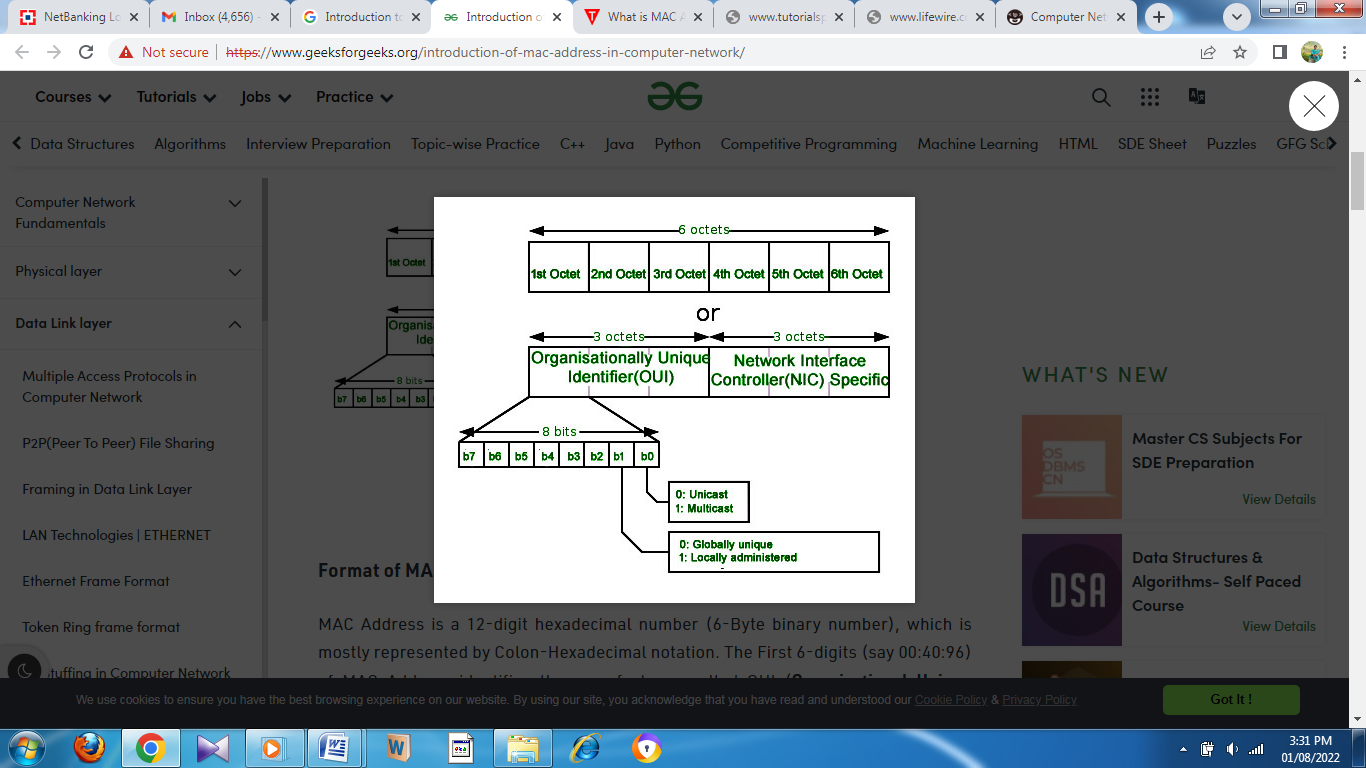
In order to communicate or transfer the data from one computer to another computer, we need some address. In Computer Network various types of addresses are introduced; each works at a different layer. Media Access Control Address is a physical address that works at the Data Link Layer. In this article, we will discuss about addressing DLL, which is MAC Address.

### Media Access Control (MAC) Address –

MAC Addresses are unique **48-bits** hardware number of a computer, which is embedded into a network card (known as a **Network Interface Card**) during the time of manufacturing. MAC Address is also known as the **Physical Address** of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers –

1. Logical Link Control(LLC) Sublayer
2. Media Access Control(MAC) Sublayer

MAC address is used by the Media Access Control (MAC) sublayer of the Data-Link Layer. MAC Address is worldwide unique since millions of network devices exist and we need to uniquely identify each.



### Format of MAC Address –

MAC Address is a 12-digit hexadecimal number (6-Byte binary number), which is mostly represented by Colon-Hexadecimal notation. The First 6-digits (say 00:40:96) of MAC Address identifies the manufacturer, called OUI (**Organizational Unique Identifier**). IEEE [Registration Authority Committee](http://standards.ieee.org/develop/regauth/index.html) assigns these MAC prefixes to its registered vendors.

Here are [some OUI](http://standards-oui.ieee.org/oui/oui.txt) of well-known manufacturers :

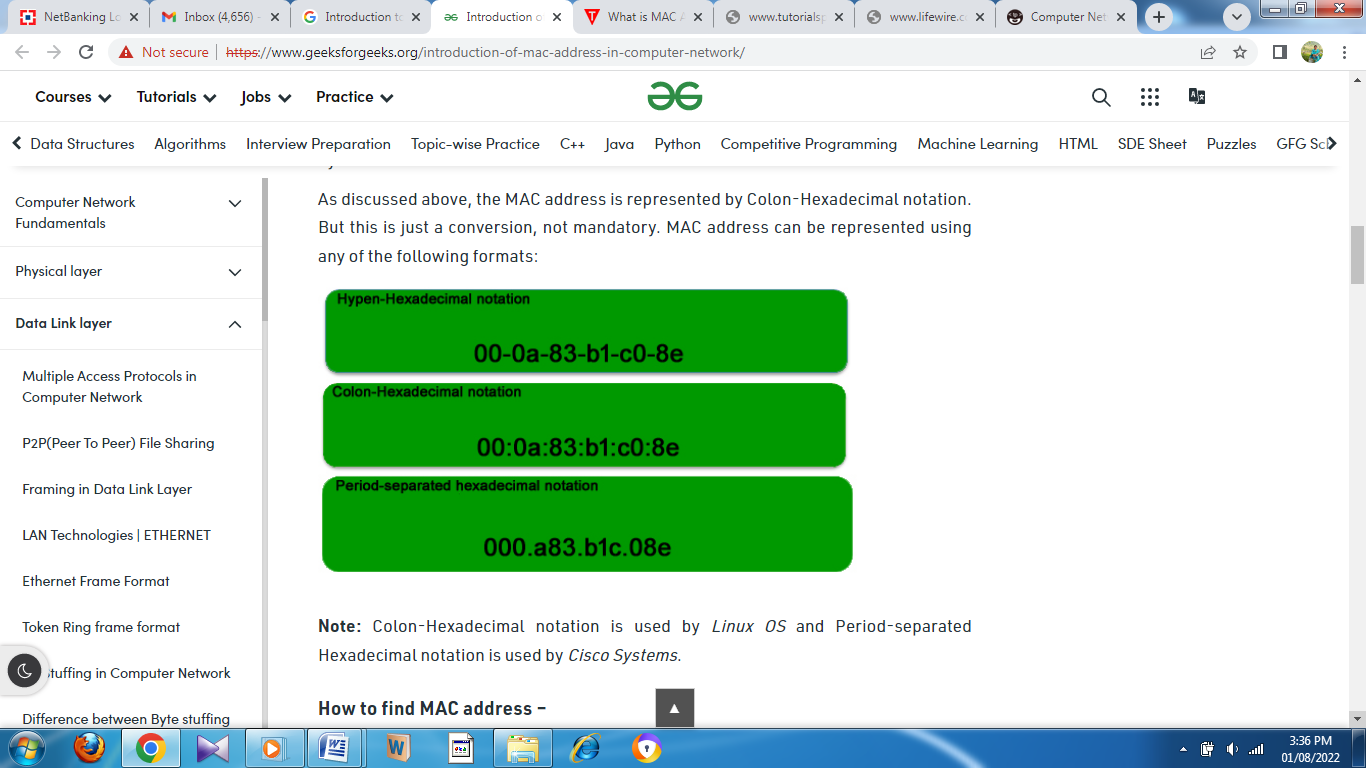
CC:46:D6 - Cisco

3C:5A:B4 - Google, Inc.

3C:D9:2B - Hewlett Packard

00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD

The rightmost six digits represent **Network Interface Controller**, which is assigned by the manufacturer.



As discussed above, the MAC address is represented by Colon-Hexadecimal notation. But this is just a conversion, not mandatory. MAC address can be represented using any of the following formats:

**Note:** Colon-Hexadecimal notation is used by *Linux OS* and Period-separated Hexadecimal notation is used by *Cisco Systems*.

### How to find MAC address –

Command for UNIX/Linux - *ifconfig -a*

*ip link list*

*ip address show*

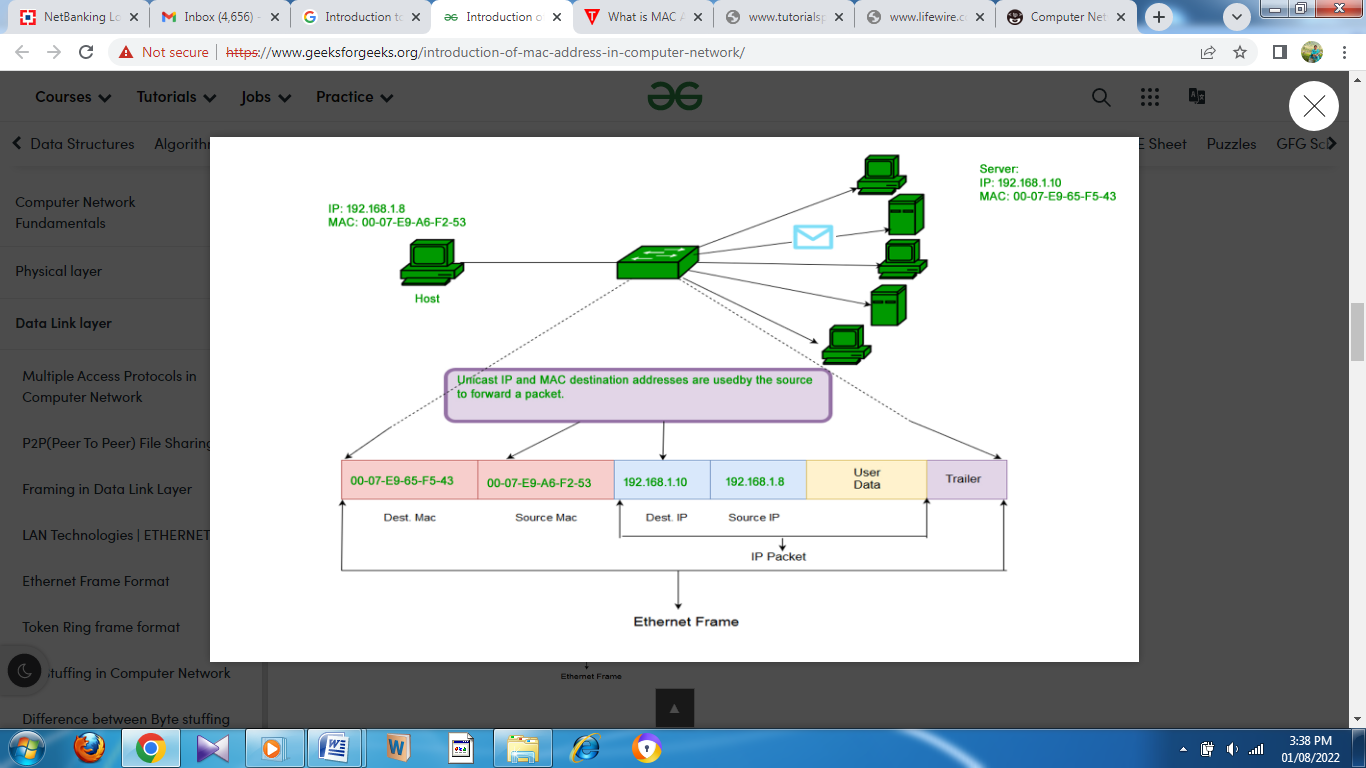
Command forWindows OS -  *ipconfig /all*

MacOS -  *TCP/IP Control Panel*

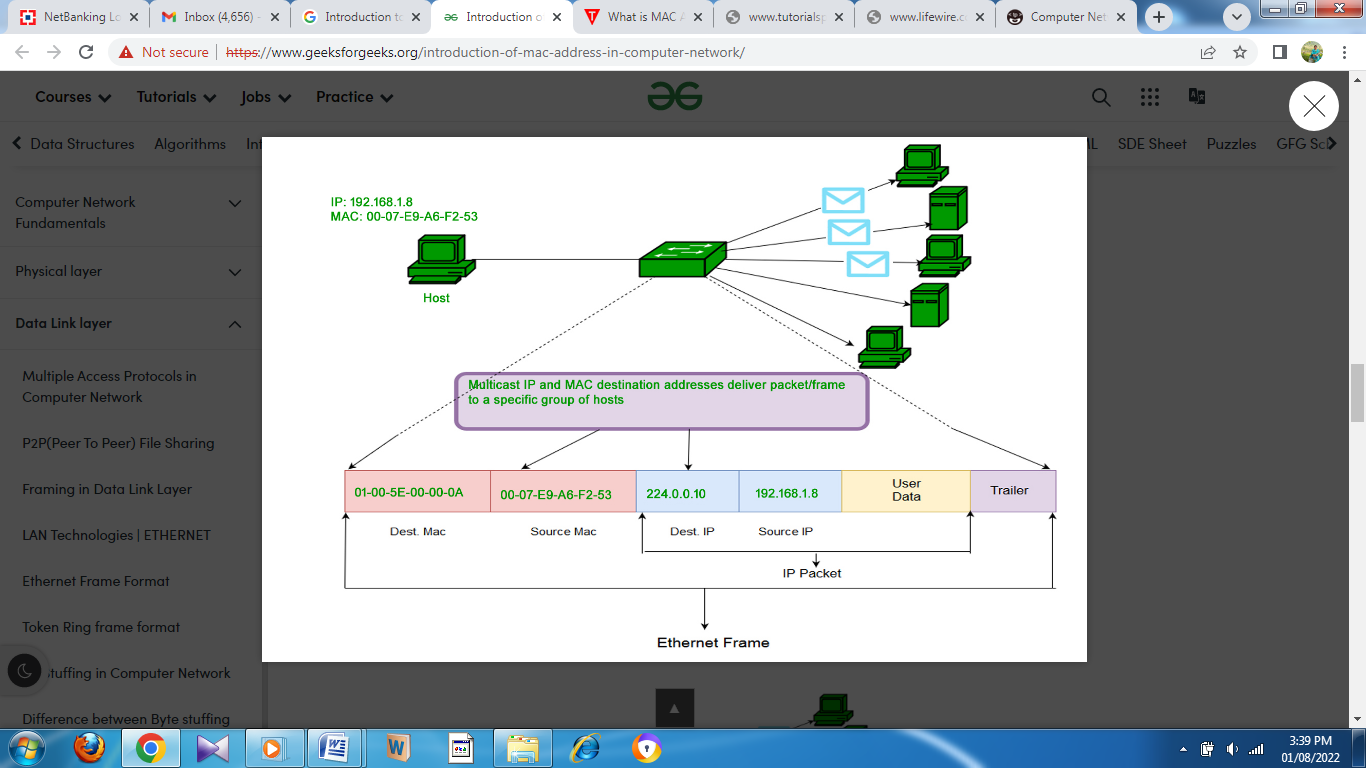
**Note –** LAN technologies like Token Ring, and Ethernet use MAC Addresses as their Physical address but there are some networks (AppleTalk) that do not use MAC addresses.

### Types of MAC Address:

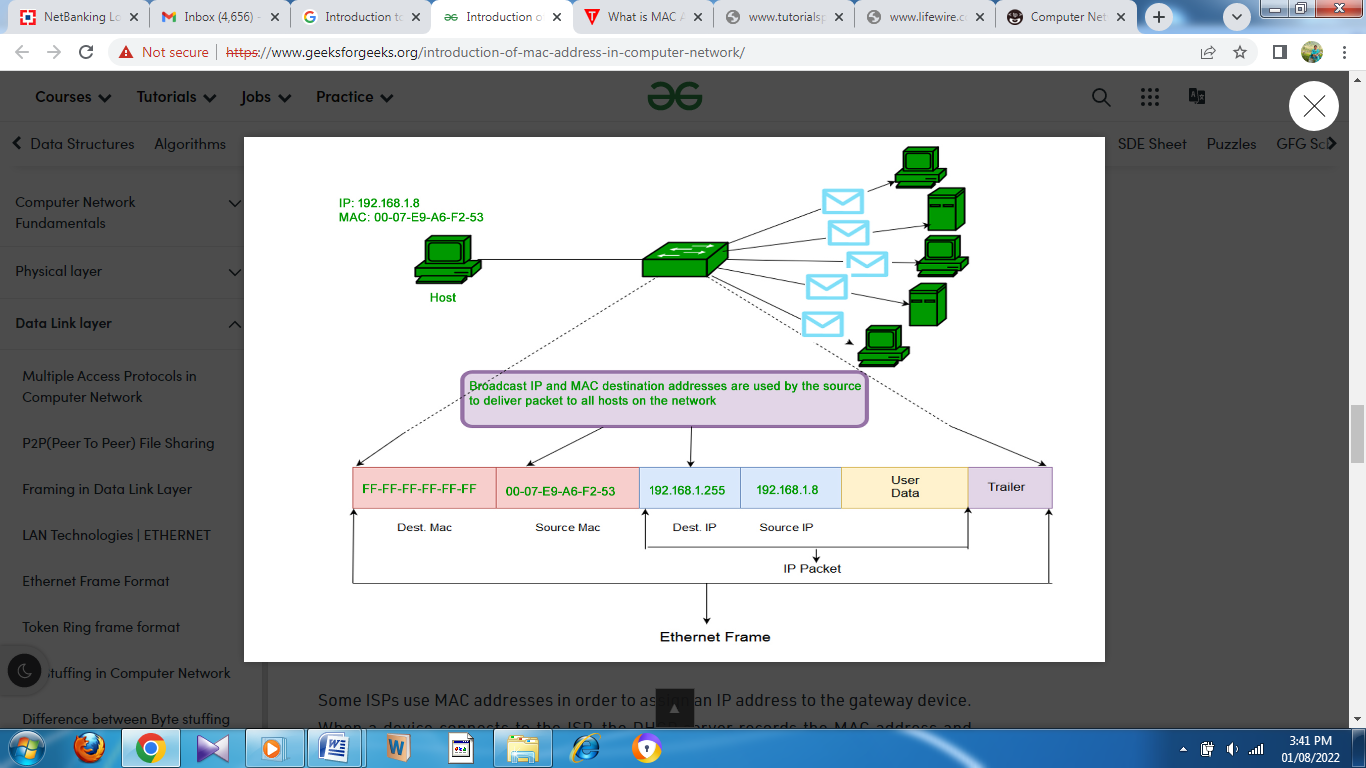
* 1. **Unicast:**A Unicast addressed frame is only sent out to the interface leading to a specific NIC. If the LSB (least significant bit) of the first octet of an address is set to zero, the frame is meant to reach only one receiving NIC. MAC Address of source machine is always Unicast.



* 1. **Multicast:**The multicast address allows the source to send a frame to a group of devices. In Layer-2 (Ethernet) Multicast address, LSB (least significant bit) of the first octet of an address is set to one. IEEE has allocated the address block 01-80-C2-xx-xx-xx (01-80-C2-00-00-00 to 01-80-C2-FF-FF-FF) for group addresses for use by standard protocols.



* 1. **Broadcast:**Similar to Network Layer, Broadcast is also possible on the underlying layer( Data Link Layer). Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are referred to as the broadcast addresses. Frames that are destined with MAC address FF-FF-FF-FF-FF-FF will reach every computer belonging to that LAN segment.



### Characteristics of MAC address:

Media Access Control address (MAC address) is a unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification and used in the Media Access Control protocol sub-layer.  
An Ethernet MAC address is a 48-bit binary value expressed as 12 hexadecimal digits (4 bits per hexadecimal digit). MAC addresses are in a flat structure and thus they are not routable on the Internet. Serial interfaces do not use MAC addresses. It does NOT contain a network and host portion with the address. It is used to deliver the frame to the destination device.

# Multiple access protocol- ALOHA, CSMA, CSMA/CA and CSMA/CD

## Data Link Layer

The [data link layer](https://www.javatpoint.com/data-link-layer) is used in a computer network to transmit the data between two devices or nodes. It divides the layer into parts such as **data link control** and the **multiple access resolution/protocol**. The upper layer has the responsibility to flow control and the error control in the data link layer, and hence it is termed as **logical of data link control**. Whereas the lower sub-layer is used to handle and reduce the collision or multiple access on a channel. Hence it is termed as [**media access control**](https://www.javatpoint.com/mac-full-form) or the multiple access resolutions.

## Data Link Control

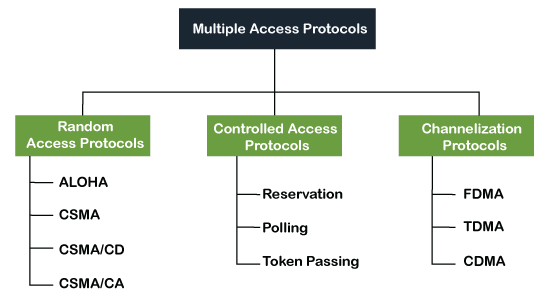
A [data link control](https://www.javatpoint.com/data-link-controls) is a reliable channel for transmitting data over a dedicated link using various techniques such as framing, error control and flow control of data packets in the computer network.

## What is a multiple access protocol?

When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel. Suppose there is no dedicated path to communicate or transfer the data between two devices. In that case, multiple stations access the channel and simultaneously transmits the data over the channel. It may create collision and cross talk. Hence, the multiple access protocol is required to reduce the collision and avoid crosstalk between the channels.

For example, suppose that there is a classroom full of students. When a teacher asks a question, all the students (small channels) in the class start answering the question at the same time (transferring the data simultaneously). All the students respond at the same time due to which data is overlap or data lost. Therefore it is the responsibility of a teacher (multiple access protocol) to manage the students and make them one answer.

Following are the types of multiple access protocol that is subdivided into the different process as:



### A. Random Access Protocol

In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on another station nor any station control another station. Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict. Due to the collision, the data frame packets may be lost or changed. And hence, it does not receive by the receiver end.

Following are the different methods of random-access protocols for broadcasting frames on the channel.

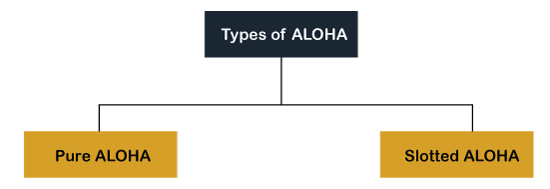
* Aloha
* CSMA
* CSMA/CD
* CSMA/CA

### ALOHA Random Access Protocol

It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

**Aloha Rules**

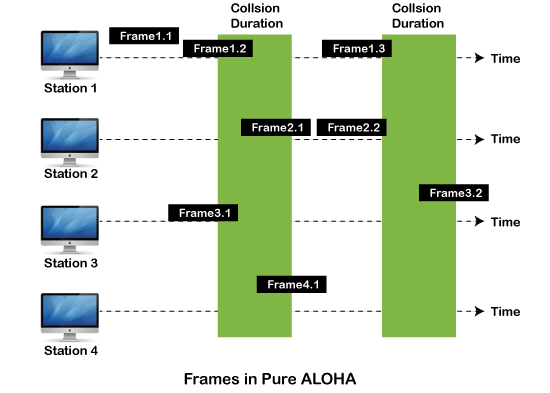
1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.



**Pure Aloha**

Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

1. The total vulnerable time of pure Aloha is 2 \* Tfr.
2. Maximum throughput occurs when G = 1/ 2 that is 18.4%.
3. Successful transmission of data frame is S = G \* e ^ - 2 G.

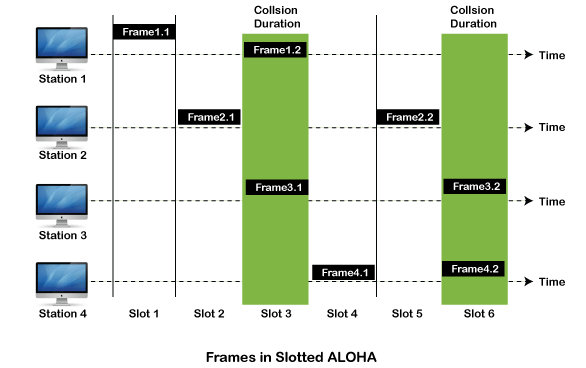


As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same time, other frames are lost or destroyed. Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage. If the new frame's first bit enters the channel before finishing the last bit of the second frame. Both frames are completely finished, and both stations must retransmit the data frame.

**Slotted Aloha**

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

1. Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is S = G \* e ^ - 2 G.
3. The total vulnerable time required in slotted Aloha is Tfr.



### CSMA (Carrier Sense Multiple Access)

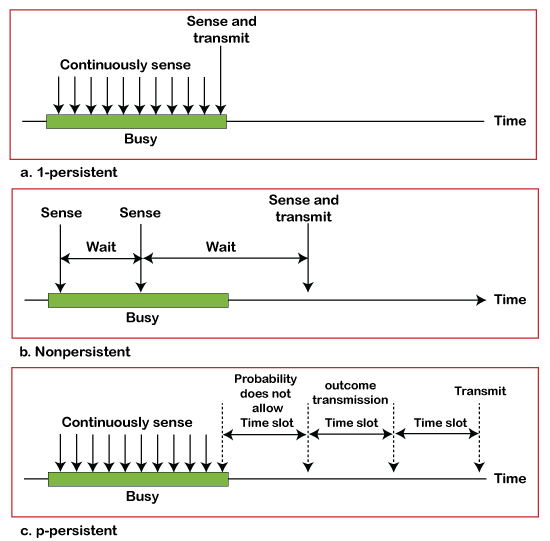
It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

**CSMA Access Modes**

**1-Persistent:** In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.

**Non-Persistent:** It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

**P-Persistent:** It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time and resumes the frame with the next time slot.



### CSMA/ CD

It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

### CSMA/ CA

It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

B. Controlled Access Protocol

It is a method of reducing data frame collision on a shared channel. In the controlled access method, each station interacts and decides to send a data frame by a particular station approved by all other stations. It means that a single station cannot send the data frames unless all other stations are not approved. It has three types of controlled access: **Reservation, Polling**, and **Token Passing**.

**Reservation**

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

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

**Polling**

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

**Token Passing**

* In token passing scheme, the stations are connected logically to each other in form of ring and access to stations is governed by tokens.
* A token is a special bit pattern or a small message, which circulate from one station to the next in some predefined order.
* In Token ring, token is passed from one station to another adjacent station in the ring whereas incase of Token bus, each station uses the bus to send the token to the next station in some predefined 

### C. Channelization Protocols

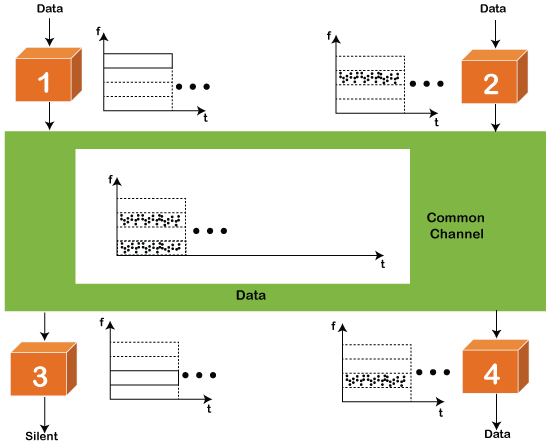
It is a channelization protocol that allows the total usable bandwidth in a shared channel to be shared across multiple stations based on their time, distance and codes. It can access all the stations at the same time to send the data frames to the channel.

Following are the various methods to access the channel based on their time, distance and codes:

1. FDMA (Frequency Division Multiple Access)
2. TDMA (Time Division Multiple Access)
3. CDMA (Code Division Multiple Access)

**FDMA**

It is a frequency division multiple access (**FDMA**) method used to divide the available bandwidth into equal bands so that multiple users can send data through a different frequency to the subchannel. Each station is reserved with a particular band to prevent the crosstalk between the channels and interferences of stations.



**TDMA**

Time Division Multiple Access (**TDMA**) is a channel access method. It allows the same frequency bandwidth to be shared across multiple stations. And to avoid collisions in the shared channel, it divides the channel into different frequency slots that allocate stations to transmit the data frames. The same **frequency** bandwidth into the shared channel by dividing the signal into various time slots to transmit it. However, TDMA has an overhead of synchronization that specifies each station's time slot by adding synchronization bits to each slot.

**CDMA**

The [code division multiple access (CDMA)](https://www.javatpoint.com/cdma-full-form) is a channel access method. In CDMA, all stations can simultaneously send the data over the same channel. It means that it allows each station to transmit the data frames with full frequency on the shared channel at all times. It does not require the division of bandwidth on a shared channel based on time slots. If multiple stations send data to a channel simultaneously, their data frames are separated by a unique code sequence. Each station has a different unique code for transmitting the data over a shared channel.

# Network Addressing

* Network Addressing is one of the major responsibilities of the network layer.
* Network addresses are always logical, i.e., software-based addresses.
* A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.
* A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.
* Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

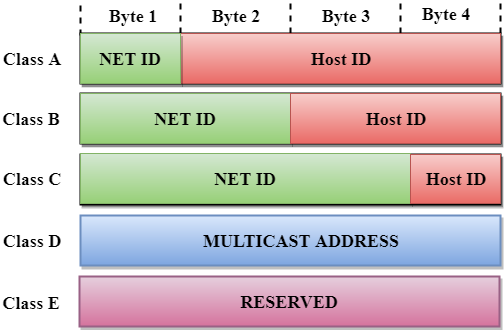
## Classful Addressing

An IP address is 32-bit long. An IP address is divided into sub-classes:

* Class A 1-126
* Class B 128-191
* Class C 192-223
* Class D
* Class E

**An ip address is divided into two parts:**

* **Network ID:** It represents the number of networks.
* **Host ID:** It represents the number of hosts.



In the above diagram, we observe that each class have a specific range of IP addresses. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

## Class A

In Class A, an IP address is assigned to those networks that contain a large number of host

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

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = 27 = 128 network address

The total number of hosts in Class A = 224 - 2 = 16,777,214 host address



## Class B

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

* The Network ID is 16 bits long.
* The Host ID is 16 bits long.

In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B = 214 = 16384 network address

The total number of hosts in Class B = 216 - 2 = 65534 host address



## Class C

In Class C, an IP address is assigned to only small-sized networks.

* The Network ID is 24 bits long.
* The host ID is 8 bits long.

In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

The total number of networks = 221 = 2097152 network address

The total number of hosts = 28 - 2 = 254 host address



## Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.



## Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.



## Classful Network Architecture

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Class** | **Higher bits** | **NET ID bits** | **HOST ID bits** | **No.of networks** | **No.of hosts per network** | **Range** |
| A | 0 | 8 | 24 | 27 | 224 | 0.0.0.0 to 127.255.255.255 |
| B | 10 | 16 | 16 | 214 | 216 | 128.0.0.0 to 191.255.255.255 |
| C | 110 | 24 | 8 | 221 | 28 | 192.0.0.0 to 223.255.255.255 |
| D | 1110 | Not Defined | Not Defined | Not Defined | Not Defined | 224.0.0.0 to 239.255.255.255 |
| E | 1111 | Not Defined | Not Defined | Not Defined | Not Defined | 240.0.0.0 to 255.255.255.255 |

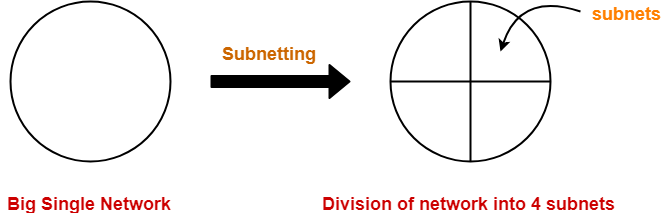
**Subnetting in Networking-**

In networking,

* The process of dividing a single network into multiple sub networks is called as **subnetting**.
* The sub networks so created are called as **subnets**.

**Example-**

Following diagram shows the subnetting of a big single network into 4 smaller subnets-



**Advantages-**

The two main advantages of subnetting a network are-

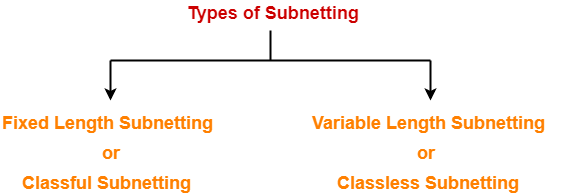
* It improves the security.
* The maintenance and administration of subnets is easy.

**Subnet ID-**

* Each subnet has its unique network address known as its **Subnet ID**.
* The subnet ID is created by borrowing some bits from the Host ID part of the IP Address.
* The number of bits borrowed depends on the number of subnets created.

**Types of Subnetting-**

Subnetting of a network may be carried out in the following two ways-



1. Fixed Length Subnetting
2. Variable Length Subnetting

**1. Fixed Length Subnetting-**

Fixed length subnetting also called as **classful subnetting** divides the network into subnets where-

* All the subnets are of same size.
* All the subnets have equal number of hosts.
* All the subnets have same subnet mask.

**2. Variable Length Subnetting-**

Variable length subnetting also called as **classless subnetting** divides the network into subnets where-

* All the subnets are not of same size.
* All the subnets do not have equal number of hosts.
* All the subnets do not have same subnet mask.

**Subnetting Examples-**

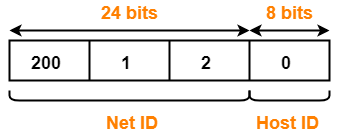
Now, we shall discuss some examples of subnetting a network-

**Example-01:**

Consider-

* We have a big single network having IP Address 200.1.2.0.
* We want to do subnetting and divide this network into 2 subnets.

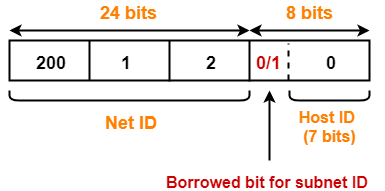
Clearly, the given network belongs to class C.



For creating two subnets and to represent their subnet IDs, we require 1 bit.

So,

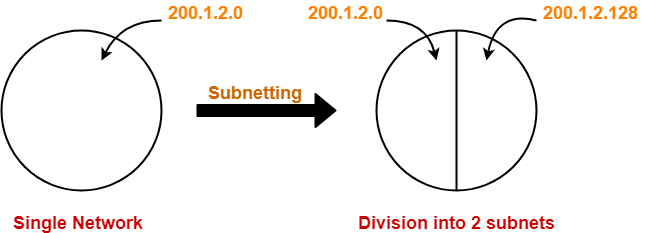
* We borrow one bit from the Host ID part.
* After borrowing one bit, Host ID part remains with only 7 bits.



* If borrowed bit = 0, then it represents the first subnet.
* If borrowed bit = 1, then it represents the second subnet.

IP Address of the two subnets are-

* 200.1.2.**0**0000000 = 200.1.2.0
* 200.1.2.**1**0000000 = 200.1.2.128



**For 1st Subnet-**

* IP Address of the subnet = 200.1.2.0
* Total number of IP Addresses = 27 = 128
* Total number of hosts that can be configured = 128 – 2 = 126
* Range of IP Addresses = [200.1.2.**0**0000000, 200.1.2.**0**1111111] = [200.1.2.0, 200.1.2.127]
* Direct Broadcast Address = 200.1.2.**0**1111111 = 200.1.2.127
* Limited Broadcast Address = 255.255.255.255

**For 2nd Subnet-**

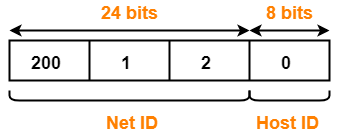
* IP Address of the subnet = 200.1.2.128
* Total number of IP Addresses = 27 = 128
* Total number of hosts that can be configured = 128 – 2 = 126
* Range of IP Addresses = [200.1.2.**1**0000000, 200.1.2.**1**1111111] = [200.1.2.128, 200.1.2.255]
* Direct Broadcast Address = 200.1.2.**1**1111111 = 200.1.2.255
* Limited Broadcast Address = 255.255.255.255

**Example-02:**

Consider-

* We have a big single network having IP Address 200.1.2.0.
* We want to do subnetting and divide this network into 4 subnets.

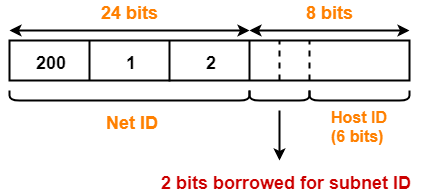
Clearly, the given network belongs to class C.



For creating four subnets and to represent their subnet IDs, we require 2 bits.

So,

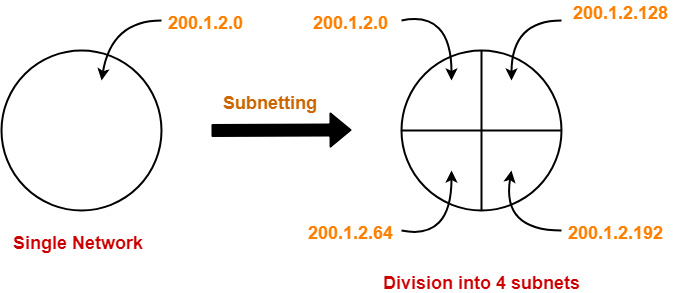
* We borrow two bits from the Host ID part.
* After borrowing two bits, Host ID part remains with only 6 bits.



* If borrowed bits = 00, then it represents the 1st subnet.
* If borrowed bits = 01, then it represents the 2nd subnet.
* If borrowed bits = 10, then it represents the 3rd subnet.
* If borrowed bits = 11, then it represents the 4th subnet.

IP Address of the four subnets are-

* 200.1.2.**00**000000 = 200.1.2.0
* 200.1.2.**01**000000 = 200.1.2.64
* 200.1.2.**10**000000 = 200.1.2.128
* 200.1.2.**11**000000 = 200.1.2.192



**For 1st Subnet-**

* IP Address of the subnet = 200.1.2.0
* Total number of IP Addresses = 26 = 64
* Total number of hosts that can be configured = 64 – 2 = 62
* Range of IP Addresses = [200.1.2.**00**000000, 200.1.2.**00**111111] = [200.1.2.0, 200.1.2.63]
* Direct Broadcast Address = 200.1.2.**00**111111 = 200.1.2.63
* Limited Broadcast Address = 255.255.255.255

**For 2nd Subnet-**

* IP Address of the subnet = 200.1.2.64
* Total number of IP Addresses = 26 = 64
* Total number of hosts that can be configured = 64 – 2 = 62
* Range of IP Addresses = [200.1.2.**01**000000, 200.1.2.**01**111111] = [200.1.2.64, 200.1.2.127]
* Direct Broadcast Address = 200.1.2.**01**111111 = 200.1.2.127
* Limited Broadcast Address = 255.255.255.255

**For 3rd Subnet-**

* IP Address of the subnet = 200.1.2.128
* Total number of IP Addresses = 26 = 64
* Total number of hosts that can be configured = 64 – 2 = 62
* Range of IP Addresses = [200.1.2.**10**000000, 200.1.2.**10**111111] = [200.1.2.128, 200.1.2.191]
* Direct Broadcast Address = 200.1.2.**10**111111 = 200.1.2.191
* Limited Broadcast Address = 255.255.255.255

**For 4th Subnet-**

* IP Address of the subnet = 200.1.2.192
* Total number of IP Addresses = 26 = 64
* Total number of hosts that can be configured = 64 – 2 = 62
* Range of IP Addresses = [200.1.2.**11**000000, 200.1.2.**11**111111] = [200.1.2.192, 200.1.2.255]
* Direct Broadcast Address = 200.1.2.**11**111111 = 200.1.2.255
* Limited Broadcast Address = 255.255.255.255

**Example-03:**

Consider-

* We have a big single network having IP Address 200.1.2.0.
* We want to do subnetting and divide this network into 3 subnets.

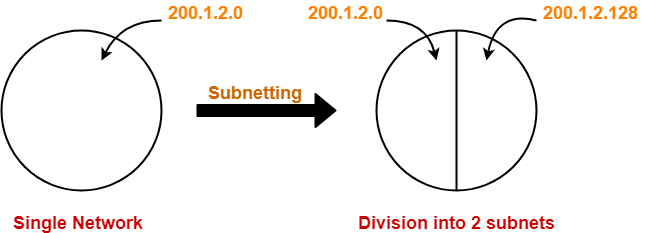
Here, the subnetting will be performed in two steps-

1. Dividing the given network into 2 subnets
2. Dividing one of the subnets further into 2 subnets

**Step-01: Dividing Given Network into 2 Subnets-**

The subnetting will be performed exactly in the same way as performed in Example-01.

After subnetting, we have-



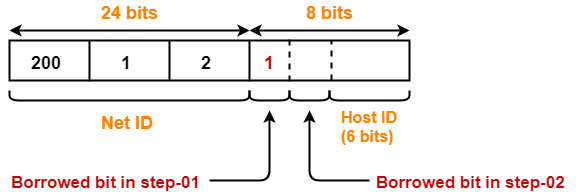
**Step-02: Dividing One Subnet into 2 Subnets-**

* We perform the subnetting of one of the subnets further into 2 subnets.
* Consider we want to do subnetting of the 2nd subnet having IP Address 200.1.2.128.

For creating two subnets and to represent their subnet IDs, we require 1 bit.

So,

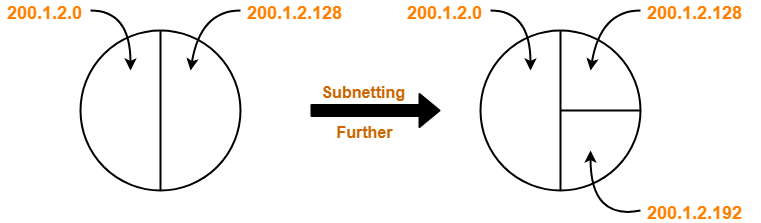
* We borrow one more bit from the Host ID part.
* After borrowing one bit, Host ID part remains with only 6 bits.



* If 2nd borrowed bit = 0, then it represents one subnet.
* If 2nd borrowed bit = 1, then it represents the other subnet.

IP Address of the two subnets are-

* 200.1.2.**10**000000 = 200.1.2.128
* 200.1.2.**11**000000 = 200.1.2.192



Finally, the given single network is divided into 3 subnets having IP Address-

* 200.1.2.0
* 200.1.2.128
* 200.1.2.192

**For 1st Subnet-**

* IP Address of the subnet = 200.1.2.0
* Total number of IP Addresses = 27 = 128
* Total number of hosts that can be configured = 128 – 2 = 126
* Range of IP Addresses = [200.1.2.**0**0000000, 200.1.2.**0**1111111] = [200.1.2.0, 200.1.2.127]
* Direct Broadcast Address = 200.1.2.**0**1111111 = 200.1.2.127
* Limited Broadcast Address = 255.255.255.255

**For 2nd Subnet-**

* IP Address of the subnet = 200.1.2.128
* Total number of IP Addresses = 26 = 64
* Total number of hosts that can be configured = 64 – 2 = 62
* Range of IP Addresses = [200.1.2.**10**000000, 200.1.2.**10**111111] = [200.1.2.128, 200.1.2.191]
* Direct Broadcast Address = 200.1.2.**10**111111 = 200.1.2.191
* Limited Broadcast Address = 255.255.255.255

**For 3rd Subnet-**

* IP Address of the subnet = 200.1.2.192
* Total number of IP Addresses = 26 = 64
* Total number of hosts that can be configured = 64 – 2 = 62
* Range of IP Addresses = [200.1.2.**11**000000, 200.1.2.**11**111111] = [200.1.2.192, 200.1.2.255]
* Direct Broadcast Address = 200.1.2.**11**111111 = 200.1.2.255
* Limited Broadcast Address = 255.255.255.255

## ****Subnet Mask-****

## ****Subnet Mask Use-****

|  |
| --- |
| Subnet mask is used to determine to which network the given IP Address belongs to. |

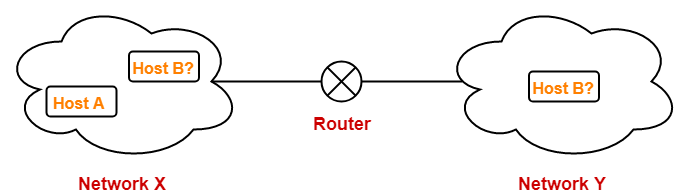
* Host use its subnet mask to determine whether the other host it wants to communicate with is present within the same network or not.
* If the destination host is present within the same network, then source host sends the packet directly to the destination host.
* If the destination host is present in some other network, then source host routes the packet to the default gateway (router).
* Router then sends the packet to the destination host.

## ****Example-****

Consider-

* There is a host A present in some network X.
* There is a host B.
* Host A wants to send a packet to host B.

Before transmitting the packet, host A determines whether host B is present within the same network or not.



Here,

* Host A = Source host
* Host B = Destination host

To determine whether destination host is present within the same network or not, source host follows the following steps-

## ****Step-01:****

* Source host computes its own network address using its own IP Address and subnet mask.
* After computation, source host obtains its network address with respect to itself.

## ****Step-02:****

* Source host computes the network address of destination host using destination IP Address and its own subnet mask.
* After computation, source host obtains the network address of destination host with respect to itself.

## ****Step-03:****

Source host compares the two results obtained in the above steps.

Then, following two cases are possible-

### ****Case-01:****

If the results are same,

* Source host assumes that the destination host is present within the same network.
* Source host sends the packet directly to the destination host.

### ****Case-02:****

If the results are different,

* Source host assumes that the destination host is present in some other network.
* Source host sends the packet via router to the destination host.

## ****Important Points-****

## ****Note-01:****

* Each host knows only its own subnet mask.
* It does not know the subnet mask of any other host.

## ****Note-02:****

* The conclusion drawn by a host about the presence of other host within the same or different network might be wrong.

## ****Note-03:****

* Consider host A draws some conclusion about host B.
* Then, same conclusion might not be drawn by host B about host A.
* Both the hosts have to perform the above procedure separately at their ends to conclude anything.

## ****PRACTICE PROBLEMS BASED ON USE OF SUBNET MASK-****

## ****Problem-01:****

Two computers C1 and C2 are configured as follows-

* C1 has IP Address 203.197.2.53 and net mask 255.255.128.0
* C2 has IP Address 203.197.75.201 and net mask 255.255.192.0

Which one of the following statements is true?

1. C1 and C2 both assume they are on the same network
2. C2 assumes C1 is on same network but C1 assumes C2 is on a different network
3. C1 assumes C2 is on same network but C2 assumes C1 is on a different network
4. C1 and C2 both assume they are on different networks

## ****Solution-****

### ****At Computer C1-****

C1 computes its network address using its own IP Address and subnet mask as-

203.197.2.53 AND 255.255.128.0

= 203.197.0.0

C1 computes the network address of C2 using IP Address of C2 and its own subnet mask as-

203.197.75.201 AND 255.255.128.0

= 203.197.0.0

Since both the results are same, so C1 assumes that C2 is on the same network.

### ****At Computer C2-****

C2 computes its network address using its own IP Address and subnet mask as-

203.197.75.201 AND 255.255.192.0

= 203.197.64.0

C2 computes the network address of C1 using IP Address of C1 and its own subnet mask as-

203.197.2.53 AND 255.255.192.0

= 203.197.0.0

Since both the results are different, so C2 assumes that C1 is on a different network.

Thus, Option (C) is correct.

## ****Problem-02:****

The subnet mask for a particular network is 255.255.31.0. Which of the following pairs of IP Addresses could belong to this network?

1. 172.57.88.62 and 172.56.87.233
2. 10.35.28.2 and 10.35.29.4
3. 191.203.31.87 and 191.234.31.88
4. 128.8.129.43 and 128.8.161.55

## ****Solution-****

Let the given two IP Addresses belong to Host A and Host B.

### ****Checking Option (A)-****

* Host A IP Address = 172.57.88.62
* Host B IP Address = 172.56.87.233

### ****At Host A-****

Host A computes its network address using its own IP Address and subnet mask-

172.57.88.62 AND 255.255.31.0

= 172.57.24.0

Host A computes the network address of Host B using IP Address of Host B and its own subnet mask-

172.56.87.233 AND 255.255.31.0

= 172.56.23.0

Since both the results are different, so host A assumes that host B is on a different network.

Thus, both can’t belong to the same network.

Hence, this option gets eliminated.

### ****Checking Option (B)-****

* Host A IP Address = 10.35.28.2
* Host B IP Address = 10.35.29.4

### ****At Host A-****

Host A computes its network address using its own IP Address and subnet mask-

10.35.28.2 AND 255.255.31.0

= 10.35.28.0

Host A computes the network address of Host B using IP Address of Host B and its own subnet mask-

10.35.29.4 AND 255.255.31.0

= 10.35.29.0

Since both the results are different, so host A assumes that host B is on a different network.

Thus, both can’t belong to the same network.

Hence, this option gets eliminated.

### ****Checking Option (C)-****

* Host A IP Address = 191.203.31.87
* Host B IP Address = 191.234.31.88

### ****At Host A-****

Host A computes its network address using its own IP Address and subnet mask-

191.203.31.87 AND 255.255.31.0

= 191.203.31.0

Host A computes the network address of Host B using IP Address of Host B and its own subnet mask-

191.234.31.88 AND 255.255.31.0

= 191.234.31.0

Since both the results are same, so host A assumes that host B is on the same network.

### ****At Host B-****

Host B computes its network address using its own IP Address and subnet mask-

191.234.31.88 AND 255.255.31.0

= 191.234.31.0

Host B computes the network address of Host A using IP Address of Host A and its own subnet mask-

191.203.31.87 AND 255.255.31.0

= 191.203.31.0

Since both the results are different, so host B assumes that host A is on a different network.

Thus, both can’t belong to the same network.

Hence, this option gets eliminated.

### ****Checking Option (D)-****

* Host A IP Address = 128.8.129.43
* Host B IP Address = 128.8.161.55

### ****At Host A-****

Host A computes its network address using its own IP Address and subnet mask-

128.8.129.43 AND 255.255.31.0

= 128.8.1.0

Host A computes the network address of Host B using IP Address of Host B and its own subnet mask-

128.8.161.55 AND 255.255.31.0

= 128.8.1.0

Since both the results are same, so host A assumes that host B is on the same network.

### ****At Host B-****

Host B computes its network address using its own IP Address and subnet mask-

128.8.161.55 AND 255.255.31.0

= 128.8.1.0

Host B computes the network address of Host A using IP Address of Host A and its own subnet mask-

128.8.129.43 AND 255.255.31.0

= 128.8.1.0

Since both the results are same, so host B assumes that host A is on the same network.

Thus, both the hosts assume that they belong to the same network.

Hence, Option (D) is correct.