What is Network?

- In simple language it means interacting with someone
- When two computer are connected than it is also the network
- If multiple computers are connected to a common device that is known as **switch,** so this also comes in the network
- When two computer are connected let us suppose say one in India and other In USA then they are connected through **submarine cable** that is also the network.
- Computer network is a collection of computing devices that are connected in various Ways in order to communicate and share resources

What is Internet?

- Network of networks or we can say **interconnection of network**
- A very big network which is the combo of small network

What is device?

- In networking the things we are connecting , is a device and is mostly known as host or node

What is Host?

- Any device which gets the IP address is the host.
- If refers to any device on a network

What is networking?

- When the devices actually share the data
- Sharing of data and resources in a network is known as networking

What is Data transfer rate?

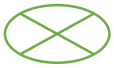
- The speed with which data is moved from one place on a network to another

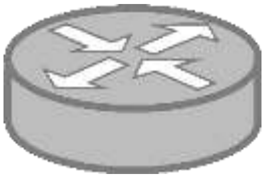
What is file server?

- A computer that stores and manages files for multiple users on a network

What is web server?

- A computer dedicated to responding to requests(from the browser client) for web pages

Representation of Router-> 



What is the router?

- When you want to Connect two or more different networks then we use the router

- So let’s suppose we have a branch in Mumbai and other in Chennai then if we want to connect both the location then we need a hardware device known as router
- Router is a network device which is used to connect different networks with each other

So below router we have a device known as switch, which has a lot of pods where we can connect are computers, servers, printers, or any type of network device and then this switch is actually connected with your router

Types of Network->

What is LAN?

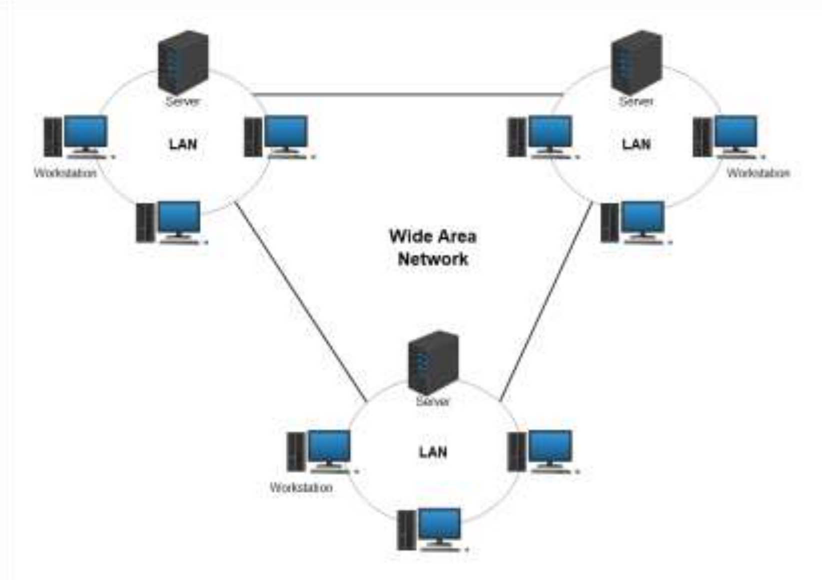
- LAN stands for Local Area Network
- A network that connects a relatively small number of machines in a relatively close geographical area .
- It refers to a network of computers and devices that are connected within a limited geographical area, such as a home, office building, school, or campus. LANs allow devices to share resources like files, printers, and internet connections. LANs typically use Ethernet cables or wireless technology like Wi-Fi to connect devices to a central networking device such as a router or switch.

  Different types of topology in LAN
- Various configurations are known as topologies. In simple language kis pattern per arrange kar rahe hai .
- 1)Ring topology-> a configuration that connects all nodes (device) in a closed loop on which Messages travel in one direction
- 2) star topology-> A configuration that centers around one node(device) to which all others Are connected and through which all messages are sent
- 3) Bus topology-> all nodes are connected to a single communication line that carries messages in both directions . it is called as Ethernet and has become the industry standard for lan

What is WAN?

- WAN stands for Wide Area Network
- It refers to a network that connects two or more local area network over a potentially large geographic distance
- It is a type of computer network that covers a broad area, such as a city, country, or even multiple countries. WANs are used to connect geographically dispersed locations, enabling communication and data exchange between different sites.
- Often one particular node on a LAN is set up to serve as a gateway to handle all communication going between that LAN and other networks

Communication between networks is called internetworking



Wan can be two types

- 1) private-> it means your private connection (leased line), it is costly but secure
- 2) public -> it means internet, it's a cheap connection buts it's not secure

3)what is MAN?

-> Metropolitan area network . The communication infrastructure that have been developed in and around the large cities

What is BoardBand?

- A connection in which transfer speeds are faster than 128 bits per second. Dsl and cable modem are boardband connections. The speed for downloads may not be same as uploads.

When you want to connect two location let suppose Mumbai and Chennai with internet then we need to create a **VPN connection** and then it is known as Public WAN, means when you use your public resources and connecting your location

And we want to secure the network then we use private WAN

So we do not have to create the Cable the connection. It is done through ISP. An internet service provider (ISP) is a company that provides access to the internet

In private Wan your ISP will be same on Both the Ends. Like in Mumbai we use Airtel connection and in Chennai we will use Airtel network then only Airtel can create a virtual connection or hardware connection

What are Switches in Computer Network?

- ➔ Switch is the device which is used to connect two or more host or two or more computers

Unmanageable switches->suppose there are four devices A,B,C,D . Now A wants to communicate with B then the information will pass to C and D also. These are just extension to the devices. We do not get any feature here. Unmanaged switches are designed to just plug in and run, with no settings to configure. These are fine to use in small networks with only basic needs.

Manageable Switches-> vlan is the concept which comes under manageable switches. Managed switches, however, are fully configurable, are customizable, and provide a range of data on performance.

So now in switches we have the term known as L2,L3

When we setup router at home then that is not router. it is the combination of rotuter,modem and this is what we called as ADSL.

ADSL-> **Asymmetric Digital Subscriber Line**

Modem-> The word "modem" is a contraction of "modulator-demodulator." A modem is a device that modulates (converts) digital signals from a computer or other digital device into analog signals suitable for transmission over analog communication channels, such as telephone lines or cable systems. At the receiving end, the modem demodulates (converts) the analog signals back into digital signals that the receiving device can understand.

Modulation:

Modulation is the process of encoding digital information onto an analog carrier signal for transmission. In modulation, a modulating signal (the digital data) is combined with a carrier signal (a continuous wave of a specific frequency) to produce a modulated signal that carries the information over the communication channel.

There are different modulation techniques, including:

Amplitude Modulation (AM): The amplitude of the carrier signal varies in accordance with the digital data.

Frequency Modulation (FM): The frequency of the carrier signal varies based on the digital data.

Phase Modulation (PM): The phase of the carrier signal changes according to the digital data.

Fiber Modem-> converting your light signals into electrical signals

Now days fiber cable is directly inside the router and one can think why is this not inside pc is because in this router there is a small chip known as SFP which stands for Small **Form-factor Pluggable**. So this chip is a small modem which help to covert light signals into electrical signals

NIC-> Network Interface Card. so NIC is a chip or any type of part which is helping to connect your computers with the network

Bits->0, 1

When we count 8 zero or ones then that 8 bites are known as 1 byte

1024 bytes->1kilo byte

1024kb->1 megabyte

Throughput-> How much data they can send or receive

When we have 10mbps speed we call it Ethernet

100mbps-> fast Ethernet

1gbps->gigaethernet

Bandwidth->

Bandwidth refers to the maximum data transfer rate of a network or internet connection, typically measured in bits per second (bps), kilobits per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps). It represents the capacity of the network to transmit data from one point to another within a given time frame

IP address->

A type-> 0-127

B type->128-196

cType->197-223

d type->224-239

e type->240-255

and here 0 and 127 are reserved

DLCP

IPV4->it is 32 bits, in a form of 4 groups. Here each gp is knows as octat and each is of 8 bit

Decimal format->200.1.1.1

IPV6->128 bits, in a form of 8 gp and each gp is of 16 bit

Decimal format->

How to check if one pc is connected to other-> there is a command known as ping . ping means Packet InterNet Groper

When we are sending 4 ping request that is known as echo request and how computer understand it as a echo request as there is a code in it and that code is basically 8. It is a type code

So basically echo is the message we send from pc a to b with a code that is type code (8) and when b is going to repley back all the request that is known as echo request

For every request we will receive one reply

So by default in one request we are sending 32 bits of packet and here time is representing how much time my computer is sending data to another device and that device is sending reply this reply time is represting the time

TTL-> time to leave -> suppose we are sending a packet to device but it is not present in the network.

TTL in the ping command and networking serves as a mechanism to limit the lifespan of packets and prevent them from circulating endlessly in the network. It helps in diagnosing network connectivity issues and determining the path taken by packets between the source and destination.

In short when ttl value is 0 then that packet is rejeacted

Lactency means delay

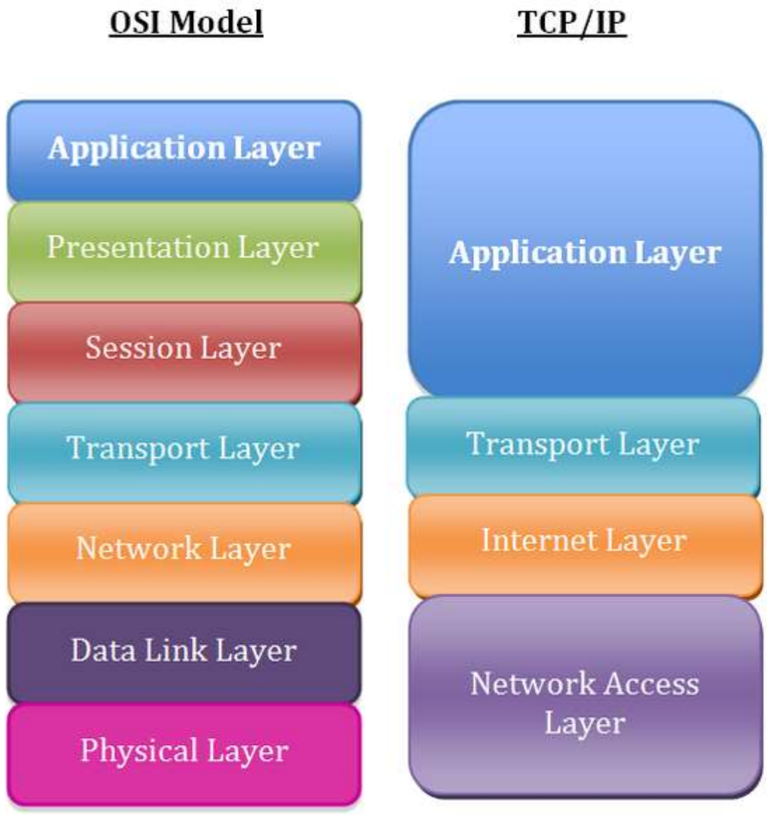
IANA-> Internet Assigned Numbered Authority

RiR->regional internet registry

Where does internet comes from??

- ➔ When all isp are connected to each other then they are actually making the internet so we can say that it’s the combination of all the networks that are connected

OSI MODEL



PROTOCOL-> A simple set of rules
Osi model-> open source Interconnection
Tcp/ip-> transmission control protocol /internet protocol

Instead of HUB Nowdays we are using Switches
Because hub only works on signal where as switches understand mac address
Hub can we consider like your extension like a hub is connected to A to B,C,D . and when A transfer data to B then it gets also transfer to C and D . it so the broadcasting where as switches does not do this switches creates a table which is known as mac address so whnever you send data to A to B or C to B then there mac address gets stored then by knowing there address it transfer the data
Hub is the layer one device that is physical layer device
And switches do not contain the mac address than it will do broadcast

BroadCast->
when one device is sending data to one device that is known as unicast
Sending data from one to many device that is known as multicast
Sending data to all the device is known as BroadCast

NIC->Network Interface Card
It a chip and we put this chip in motherboard,pci slot but nowdays every device has inbuilt nic card

Bridge-> to connect the Hubs with each other as earlier bridge was the device that actually stores the mac address and combination **of hub+bridge is know known as switch**
It work was to reduce the broadcast

Application layer> the software which interact one human to another works in application layer
For ex-> web browser->HTTP, HTTPS, SMTP, TELNET, POP
To access the website we will use HTTP or HTTPS
To send mail we use SMTP and for receiving mails we use POP
When we want to access any file remotely we use TELNET and there is a secure version for it which is known as SSH
For file transfer we use FTP protocol
2. Presentation layer->it tells about format of data. So it means whenever we see a website like youtube we use its thumnails,videos,comments so that data is coming from you tube server in some format and presenation layer present it .so basically it converts data from the generic network format to a format that the receiving application can understand
A special software facility called "a redirector" operates at this layer to determine if a request is network related or not and forward network related requests to an appropriate network resources.
For ex->image-> png,jpeg, audio->mp1,wav, video-> mp4or avi
Encryption/decryption
Compression/decompression-> means to increase or decrease the size of the file
3. Session Layer-> it creates and maintain the session . whenever you open any bank website so it has a time limit and then the session will automatically log out if not responded within time frame
4. **Transport Layer - >from above three layers data comes in data form and this layer converts data into segments .it manages the transmission of data across a network.**it means it will divide the data in the form of chunks and parts.
And this layer is also responsible for **sequences.** It means it will actually add up numbers in the data which it segmented. In segments we add up port number . in this layer we do **retransmission** . all these 3 comes .also so in short **this layer is responsible for end to end delivery of data.**
In transport layer we have two protocol->
1->TCP->TRANSMISSION CONTROL PROTOCOL
2-> UDP->USER DATAGRAM PROTOCOL
Whenever we send data with TCP

- ➔ So whenever a packet is going to its destination then destination is going to send back a receipt which is known **as acknowledgement**
- ➔ **But whenever we send data with UDP we are not going to receive the receipt**

- **SO HERE TCP IS MORE RELIABLE THAN UDP**
- **TCP ALSO HELP IN RETRANSMIT THE DATA whereas in udp it is not possible**
- **Retransmit means if the packet id dropped or disgarded or any thing happen to data then it is going retransmit the data**
- **TCP is connection oriented but UDP is connection less**
- **UDP has less overhead**
- **TCP TAKES 20 BYTES TO ADD A INFIRMATION WHEREAS UDP TAKES 8 BYTES AND THAT INFORMATION is about the port number**
- **TCP WORKS UNDER IP AND HAS PROTOCOL NU 6 WHERE AS UDP ALSO WORKS UNDER IP AND AS PROTOCOL NU 7**

let's use the example of sending the phrase "Hello, World!" over the internet. When you send this message, it gets broken down into packets at the transport layer, typically using a protocol like TCP (Transmission Control Protocol) or UDP (User Datagram Protocol). Let's focus on TCP for this example.

When "Hello, World!" is divided into packets, each packet will have a header attached to it. This header contains essential information for routing and reassembling the packets at the receiving end. Here's a simplified breakdown of what might be included in the header:

1)Source Port: This field indicates the port number of the sender's application sending the data. For our example, let's say it's port number 1234.

2)Destination Port: This field indicates the port number of the application at the receiving end. Let's say the receiver's application is listening on port number 5678

3)Sequence Number: This number helps in ordering the packets at the receiving end. Each packet is given a sequence number to ensure that they can be put back in the correct order

)Acknowledgment Number: In TCP, this field acknowledges receipt of packets. When a packet is received successfully, the receiver sends back an acknowledgment with the next expected sequence number

5)Checksum: This field is used for error-checking. It contains a value calculated based on the packet data and is used to ensure that the packet hasn't been corrupted during transmission.

6)Window Size: This field indicates the size of the receiving window, which tells the sender how much data it can transmit before receiving an acknowledgment.

7)Flags: Various flags are used to control the behavior of TCP, such as SYN (synchronize), ACK (acknowledge), FIN (finish), etc.

8)Data: Finally, the payload or data of the packet is included. In our example, the payload would be "Hello, World!"

So, when you send the message "Hello, World!" over TCP, it gets divided into packets, each with a header containing this kind of information. These headers help ensure that the packets are routed correctly and can be reassembled in the correct order at the receiving end, forming the original message again.

5. Network Layer-> now segments are converting into packets . and along with data it will have source ip and destination ip means packet adds up source ip and destination ip. Here the routers works . this layer also selects the best path for data to be transmitted as router choose the best path . handles addresses messages for delivery as well as translating logical network addresses and names into their physical counterparts.

6. Data link layer-> now here packets are converting into frames and along with data it will have source mac add, destination mac add etc. and here switches work
7. Physical layer-> all frames is Converting into signal. Which means nic card will convert it into 0 and 1 and that is known as encoding and then into signals and now data is going over the cable , connector

SUBNETING-> Dividing the big networks into small network
A -> 1-126 , in class A ->2power(24) host are possible,
B-> 128-191,in class B
C-> 192-223 in class c ->256 host are possible and 254 are logically useable
For .0-> all network manage and.255 is boardcast
D AND E CLASSES ARE NOT USE WITH HOST AS D IS reserved for multicasting and e for future use

Subnet mask->represent the network bits

Private ip are like free ip we can use it for free and we can not access internet through private ip

In class A-> 10.0.0.0-10.255.255.255

In class B-> 172.16.0.0-172.31.255.255

In class c-> 192.168.0.0-192.168.255.255

Need of Subneting->

Maintaince Is easy in subnetting

Security enachement

How we implement it?

- **200.10.20.0 ko divide karo two parts mein**
- **S1->200.10.20.0 to 200.10.20.127**
- **S2->200.10.20.128 to 200.10.20.255**

Subnet id for s1 is 200.10.20.0 and boardcast id is 200.10.20.127
So total nu of host is 128 and usable host is 126 as 200.10.20.0 is the network id and last one is direct boardcast id

Subnet id for s2 is 200.10.20.128 and boardcast id is 200.10.20.255

So total nu of host is 128 and usable host is 126 as 200.10.20.128 is the network id and last one is direct boardcast id

So without subnetting usable host were 254 and with subnetting it is 126+126 which is 252

So to communicate we need a internal router and then submet mask . so its internal submet mask is 255.255.255.128->

.128 is here as we reserved one bit only and we will take it as 1 and rest all 0 and all 7 are zero as 10000000 and it is 128

Now there will be another router which we conneting to this router so another router submet mask would be 255.255.255.0 which is known as default subnet mask

Disadvantage of subnetting is ->first we sreach network id then which subnet you want to go then host then process id . so computation increase as first we go to network id then host id and then process id

Whenever we add 1 bit->128 5 bit->248

2 bit->192 6 bit->252

3 bit->224 7 bit-> 254

4 bit->240 8 bit->255

Static ip

Diff between between router and gateway

So router is a hardware which can have multiple gateway for each LAN

And entry point of LAN is known as gateway

In router configuration when you see->

Router> -> this is user mode Router(config)#Global configuration

Router#-> privledge mode

ARP

➔ IT STANDS FOR Address resolution protocol

Router never do boardcast

DHCP->

Dynamic Host Configuration protocol

- Your router assign ip automatically to your computers
- Some configure it on servers and some on routers
- So if you have a big company you can configure dhcp pool on server and when you have small/ medium enterprise you can have same in router
- So now both the devices will work as DHCP servers
- So there is a concept known DORA do d stands for discover and it is a boardcast packet
  O stands for offer means offer the ip address from pool and it a unicast packet
  R stands for request means send me the ip configuration
  A stands for acknownlegdement which means here is the configuration
- Discover means to dhcp server and that in dhcp table it searches for free ip and then send the ip configuration and in tha ack packet the server will send the ip configuration details

TELNET

- It is the protocol to remotely access the network devices
- It works on port nu TCP 23
- It Is Unsecure so we have SSH

SSH

- Secure shell
- -> it is the protocol to remotely access the network devices securely
- Its port nu is TCP 22

PORT NUMBER

- Identification of the service means to uniquely identify the service or application
- 1-1023 - > well known ports
- 1024-49151 ->registered Numbers
- 49152-65535-> dynamic ports
- Dynamic ports are generated by pc so that port will added to source port caatogry

  Anding process->

  So whenever a computer wants to go to another computer then it will actually calculate its binary value, so basically in this process system calculates its information

UNDERSTANDING OF BGPl

WHAT is Internet?

-

INTERNET TABLE?

- ➔ PREFIX OF YOUR LAN

THE INTERNET PROTOCOL(IP)

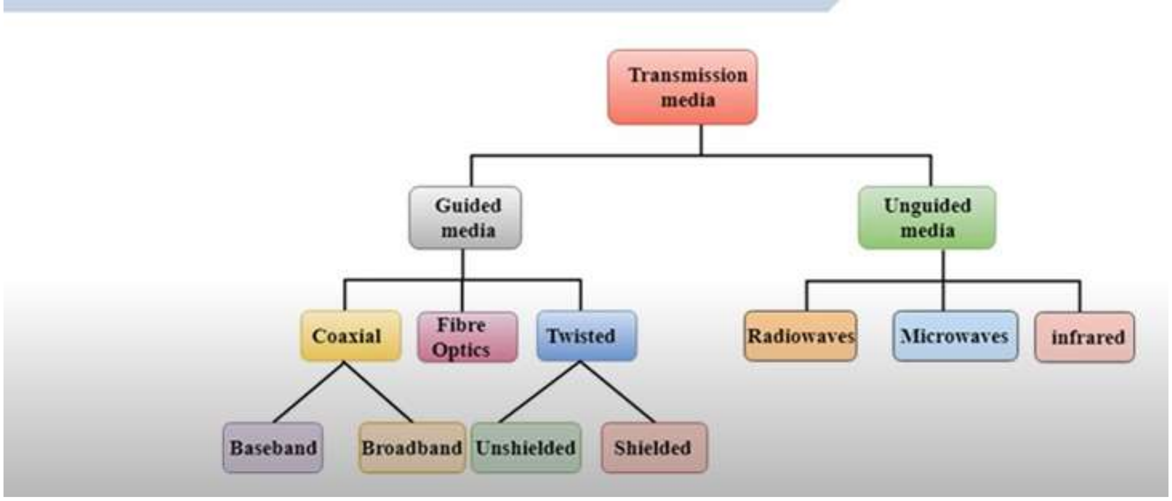
- ➔ Data is transferred in the form of packet via logical network paths in an ordered format controlled by the network layer
- ➔ It does this by forwarding packets to network routers which rely on algorithm to determine the best paths for data to travel. These paths are known as virtual circuits
- ➔ It is the method or protocol by which data is sent from one computer to another on the internet. Each computer (known as host) on the internet has at least one IP address that uniquely identifies it from all other computers on the internet

1) Physical Layer

- ➔ It converts logical data into physical streams
- ➔ Interface hardware with networks means make the understanding between hardware and network
- ➔ Convert data packets into bit streams to transfer them through the physical transmission media.
- ➔ Functions of physical layers
  - a) Cables and Connectors(Guided (wire)and Unguided(wireless))
  - b) Physical Topology(Tree,bus,star,mesh)
  - c) Hardware (Repeater(regenerates the signal),Hub)

    *->hub->I. It is essentially a multi-port repeater. When a hub receives data from one device connected to it, it broadcasts that data out to all other devices connected to the hub.

d) Transmission Mode(Simple(ek taraf se aa rhi hai per dusri taraf se nhi),Duplex(both sided))
e) MultiPlexing(FDM(Frequency division Multiplexing),TDM(Time division MultiPlexing))
f) Encoding(Analog(it means no discrete values only continuous value),Digital(only two values i.e 0 and 1))



2)Data Link Layer

-> it works between two hosts which are directly connected in some sense(same network) , point to point or broadcast

-> Takes data from the network layer and provides data to the physical layer

-> Provides node to node delivery

-> At the receiving end, it picks up data from hardware as electrical signals , assembles them in a recognizable frame format and hands over to upper layer.

Functions

a) Hop to Hop(node to node) delivery
b) Flow Control(Sliding window)
c) Error Control(CRC(Cyclic redundancy check(it is the method to check whether data received or not), Checksum(it checks the crc is correct or not)
d) Access Control(CSMA/CD,ALOHA(it fixes the time of packet), TOKEN Ring)
e) Physical Addressing(MAC)
f) Data Framing-> jo network layer se packet mila hai us mein dll apna kuch header add karta hai in short packet+trailer+payload=frame
   Trailer->The trailer typically contains error detection information, such as a Frame Check Sequence (FCS) or a Cyclical Redundancy Check (CRC), which allows the receiver to detect if the data in the frame has been corrupted during transmission

Framing in Data-link Layer

- ➔ It is a point to point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits
- ➔ These bits must be framed into discernible blocks of information
- ➔ Ethernet, token ring, frame relay and other data link layer technologies have their own frame structures.

Problem in Framing

- ➔ Detecting start of the frame: how does the receiver knows ki ek block mein kitna consider karna hai. So here we look out for special sequence(SFD) of bits which marks the beginning of the frame
- ➔ How do station detect a frame: so here we use sequential circuit where every station listen to link for sfd pattern
- ➔ Detecting end of frame-> when to stop reading the frame.

Types of framing

- ➔ 1) Fixed Size-> the frame is of fixed size and there is no need to provide boundaries to the frame,length of the frame itself act as delimiter

  Drawback-> it suffers from internal fragmentation if data size is less than frame size. It means that if data is 200 byte and frame size is 500 then rest all is wasted. So the space which is left is known as internal fragmentation

  So ther is a solution of this problem that is padding. So padding means jo space bach rahi hai us mein 0 ya 1 fill kar denge . this is known as padding

- ➔ 2) Variable size-> in this there is a need to define end of frame as well as beginning of next frame to distinguish. This can be done in two ways
  - a) Length Field-> we can introduce a length field in the frame to indicate the length of the frame. Used in Ethernet(802.3) . The problem with this is that sometimes the length field might get corrupted
  - b) End Delimiter-> we can introduce a ED(pattern) to indicate the end of the frame. Used in Token Ring. The problem with ths is that ED can occur in the data. This can be solved by:
    - i) Character/Byte Stuffing->
    - ii) Bit Stuffing

Ethernet At Data Link Layer

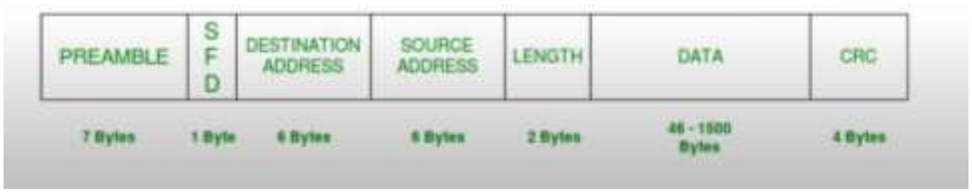
- ➔ Ethernet specifies what the data should look like, including the header and trailer
- ➔ The protocol is defined by IEEE 802.3 and divides the data link layer into two sublayers:

  a)Logical Link Control(LLC) sublayer and the

  b) Media Access Control(MAC) sublayer

Ethernet Frame Format

- Ethernet frame starts with Preamble and SFD, both works at the Physical Layer



PREAMBLE	SFD	DESTINATION ADDRESS	SOURCE ADDRESS	LENGTH	DATA	CRC
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 - 1500 Bytes	4 Bytes

- Preamble: this is a pattern of alternative 0 and 1 which indicates starting of the frame and allow sender and receiver to establish bit synchronization
- Start of frame Delimiter(SFD): Always set to 10101011. SFD indicated that upcoming bits are starting of the frome. Which is the destination address
- Destination Address: Contains the Mac Address of the machine for which data is destined.
- Source Address: Contains the Mac Address of source machine. As source Address is always an individual address (Unicast), the least significant bit of first byte is always 0.
- Length: indicates the length of entire Ethernet frame. This can hold the length value between 0 to 65534, but length cannot be larger than 1500 because of some own limitations of Ethernet
- Data: this is the place where actual data is insterted,also known as Payload. The maximum data present may be long as 1500 bytes.
- Cyclic Redundancy Check(CRC): this field contains a 32 bits hash code of data which is generated over the Destination Address, Source Address,Length and Data field.

  If the checksum computed by destination is not the same as sent checksum value , data received is corrupted.

Datalink Layer Sublayers

- 1) Logical Link Control
- Media Access Control

Logical Link Control->
The primary function of LLC is to multiplex protocols over the MAC layer and de-multiplex while receiving.
It provides hop-to-hop flow and error control.

MAC Sub Layer->
It is responsible for encapsulating frames for transmission via physical medium
It resolves the addressing of source station as well as the destination station
It determines the channel access methods for transmission for ex, GSMA/CD, ALOHA

Access Control

➔ Random Access
  a) ALOHA
  b) CSMA
  c) CSMA/CD
  d) CDMA/CA
➔ Controlled Access
  a) Reservation
  b) Polling
  c) Token Passing
➔ Channelization Protocol
  a) FDMA(Frequency Division)
  b) TDMA(Time Division)
  c) CDMA(Code division)

ALOHA(Pure Aloha)

- ➔ It is one of the earliest random access method which was designed for a radio (wireless) LAN, but it can be used on any shared medium
- ➔ Not used nowdays
- ➔ It's idea is that no station will sense the channel . station ke pass jab bhi frame hoga who tab bejdega.
- ➔ The idea is that each station sends a frame whenever it has a frame to send
- ➔ IT relies on acknowledgments from the receiver because the frame can collide with each other
- ➔ It the acknowledgment does not arrive after a time-out period, the station assumes it to be destroyed and resends the frame
- ➔ The station waits for a random amount of time and sends the frame again

<u>Address Configuration</u>

There are 2 parts of an IP Address:

1)Network Part

2)Host Part

<u>A)Network Part</u>

- ➔ Contains the network ID
- ➔ Identifies which network you're on

B)Host part

1) Used to identify hosts(any device requiring a network interface card, such as pc, networked printer) on the network.

AN Ip address can be represented as

➔ Dotted decimal notation: 192.168.1.1
➔ Binary Notation:11000000.10101000.00000001.00000001
➔ Hexadecimal Notation:C0A80101

With 32 bits, we have an address space of 2^32

We separate and allocate some bits to the network part and remaining to the host part

Class A

➔ NET ID: 8 bits
➔ Host ID: 24 bits
➔ First bits of first octet always set to 0
➔ Number of Networks: 2^7-2=126
➔ Number of Hosts=2^24-2=16,777,214
➔ Used by very large organizations or government

Class B

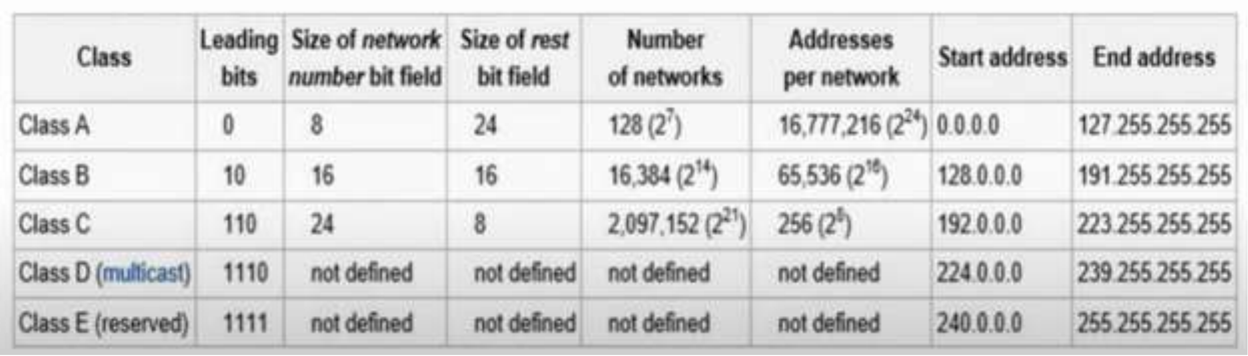
➔ NET ID:16 bits
➔ Host ID:16 bits
➔ First two of first octet are 10
➔ Number of Networks:2^14=16384
➔ Number of Hosts:2^16-2=65534
➔ Used by large or medium sized companies

Class C

➔ NET ID: 24 bits
➔ Host ID: 8 bits
➔ First three bit of first octet are 110
➔ Number of networks:2^21=2097152
➔ Number of Hosts:2^8-2=254

Class D

- Reserved for multicasting
- Network and Host ID not applicable(28 hosts)
- First Four bit of first octet are 1110
- Range:224.0.0.0- 239.255.255.255
- Reserved for experimental and research purposes
- Network and Host Id are not applicable
- First four bit of first octet are 1111(28 hosts)
- Range: 240.0.0.0- 255.255.255.254



Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

Private IP blocks

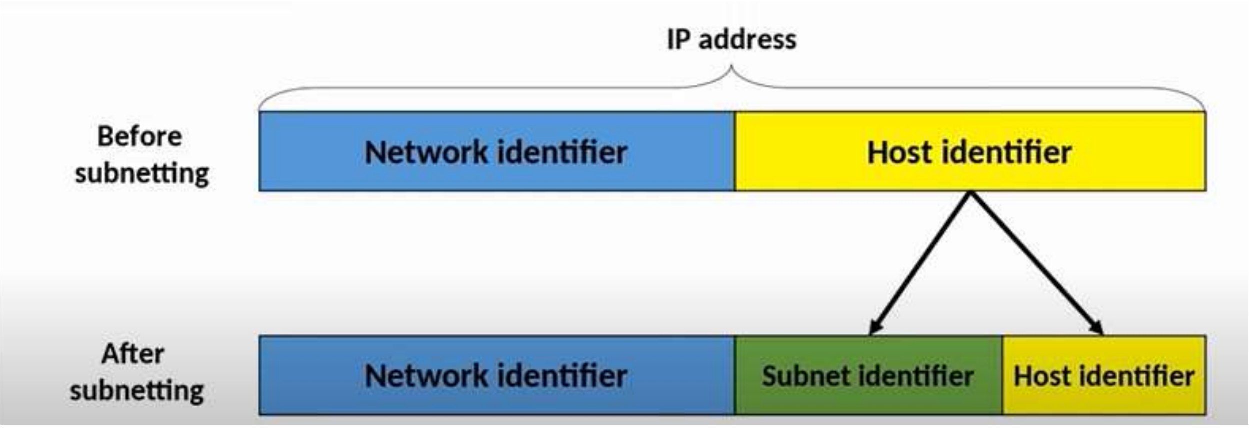
- IANA has reserved some blocks to be used in private networks
- Private IP are non-routable
- Class C:192.168.0.0- 192.168.255.255(65,536 IP address)
- Class B: 172.16.0.0-172.31.255.255(1,048,576 IP address)
- Class A: 10.0.0.0-10.255.255.255(16,777,216 IP address)

Other Special Addresses

- 169.254.0.0-169.254.0.16: Link local Addresses
- 127.0.0.0-127.255.255.255:loop-back Addresses
- 0.0.0.0-0.0.0.8- used to communicate within the current network

Classless Addressing

- ➔ **To reduce the wastage of IP addresses in a block, we use sub-netting.**
- ➔ **Subnetting: Dividing a large block of addresses into several contiguous sub-blocks and assigning these sub-blocks to different smaller networks**
- ➔ **We use host id bits as net id bits of a classful IP address**
- ➔ **We give the IP address and define the number of bits for mask along with it(usually followed by a "/" symbol), like 192.168.1.1/28**
- ➔ **For ex put 28 out of 32 bits as 1 and the rest as 0 ans so the subnet mask would be 255.255.255.240**
- ➔ A subnet mask is a four-octet number used to identify the network ID portion of a 32-bit IP address
- ➔ **Subnet Address-> And result of Subnet mask and the given IP address**



Subnetting:

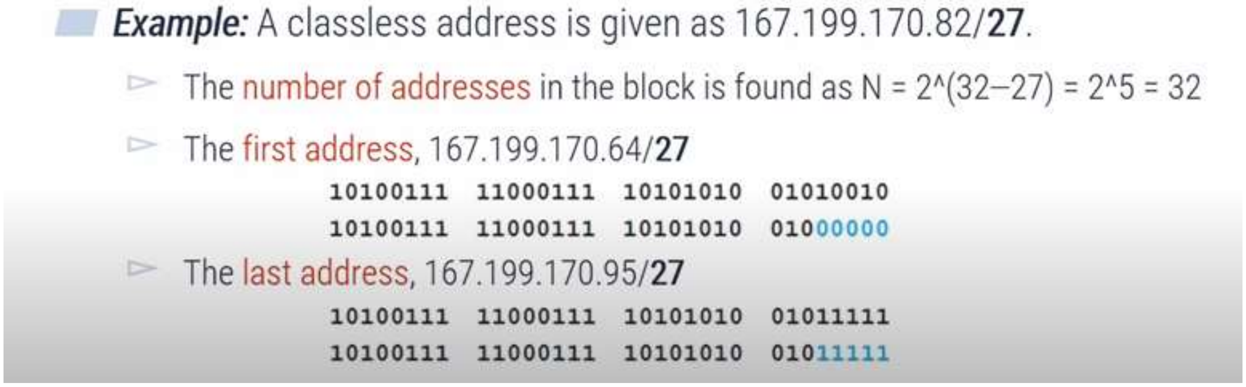
To alleviate address depletion, two trategies were proposed and to some extent ,implemented: subnetting and supernetting

- ➔ **Use the same address space but to change the distribution of addresses to provide a fairshare to each organization called classless addressing**

- **The prefix is an address defines the block(network , block is said when there is classless and for network when it is classfull)**
- **The suffix defines the node**
- **The size of the network is inversely proportional to the length of the prefix**

Extracting Information from an Address:

- We normally like to know three pieces of information about the block to which the address belongs: the nu of addresses, the first address in the block and the last address.
- The number of addresses in the block is found as N=2^(32-n)
- To find the first address, we keep the n leftmost bits and set the (32-n) rightmost bits all to 0s.
- To find the last address, we keep the n leftmost bits and set the (32-n) rightmost bits al to 1s.



Example: A classless address is given as 167.199.170.82/**27**.

- The number of addresses in the block is found as N = 2^(32–27) = 2^5 = 32
- The first address, 167.199.170.64/**27**

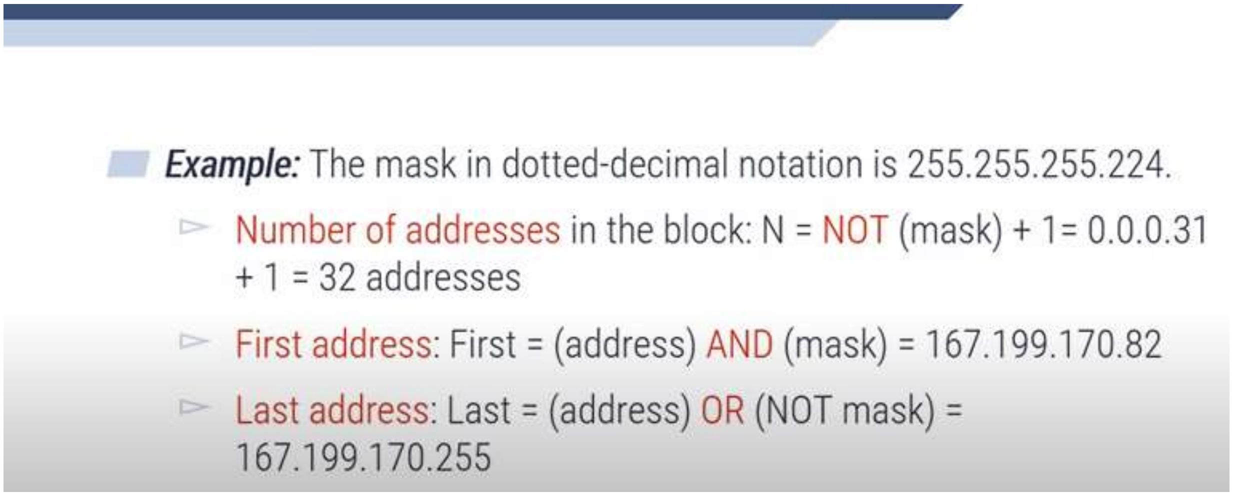
```
10100111  11000111  10101010  01010010
10100111  11000111  10101010  01000000
```

- The last address, 167.199.170.95/**27**

```
10100111  11000111  10101010  01011111
10100111  11000111  10101010  01011111
```

Address Mask:

- The address mask is a 32-bit number in which the n leftmost bits are set to 1s(means network bits are 1) and the rest of the bits (32-n) are set to 0s(means host bits are 0)
- The nu of addresses in the block N=NOT(mask)+1
- The first address in the block=(Any address in the block) AND (Mask)
- The last address in the block =(Any address in the block) OR[(NOT(mask))]



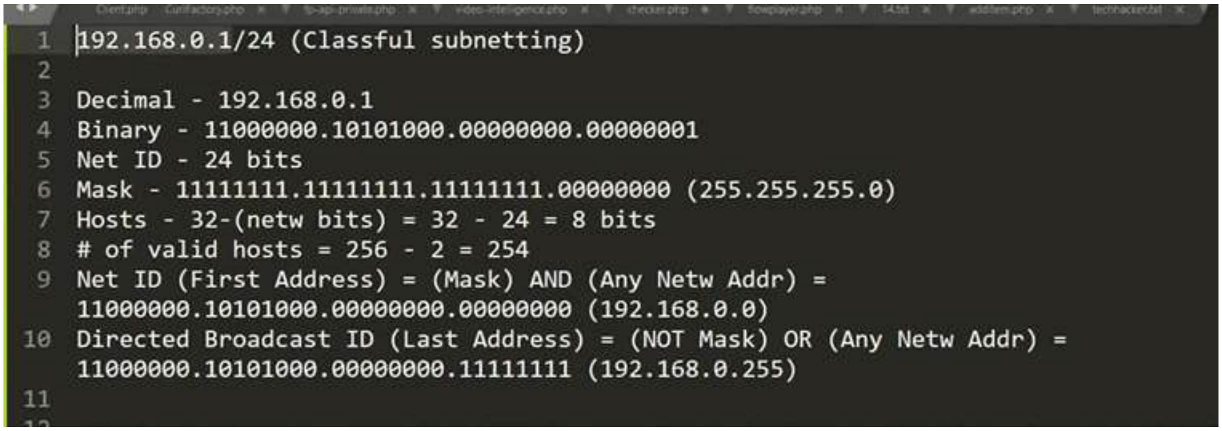
- ***Example:*** The mask in dotted-decimal notation is 255.255.255.224.
  - Number of addresses in the block: N = NOT (mask) + 1= 0.0.0.31 + 1 = 32 addresses
  - First address: First = (address) AND (mask) = 167.199.170.82
  - Last address: Last = (address) OR (NOT mask) = 167.199.170.255

Designing Subnets:

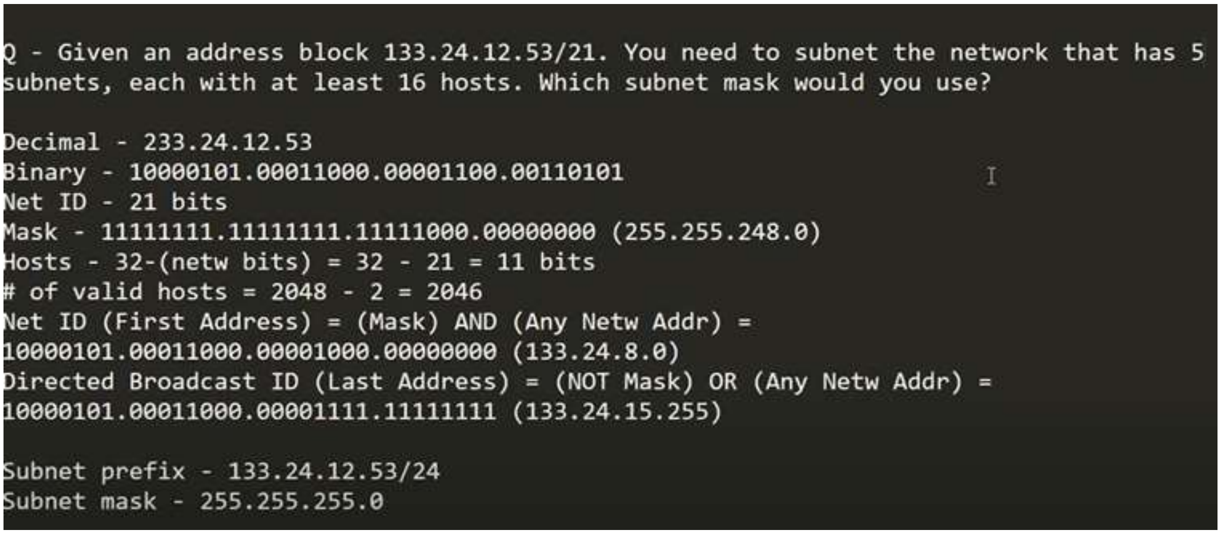
➔ We assume the total nu of addresses granted to the organization is N, the prefix length is n, the assigned number of addresses to each subnetwork is N(sub) and the prefix length for each subnetwork is n(sub)

➔ The following three conditions need to be met:

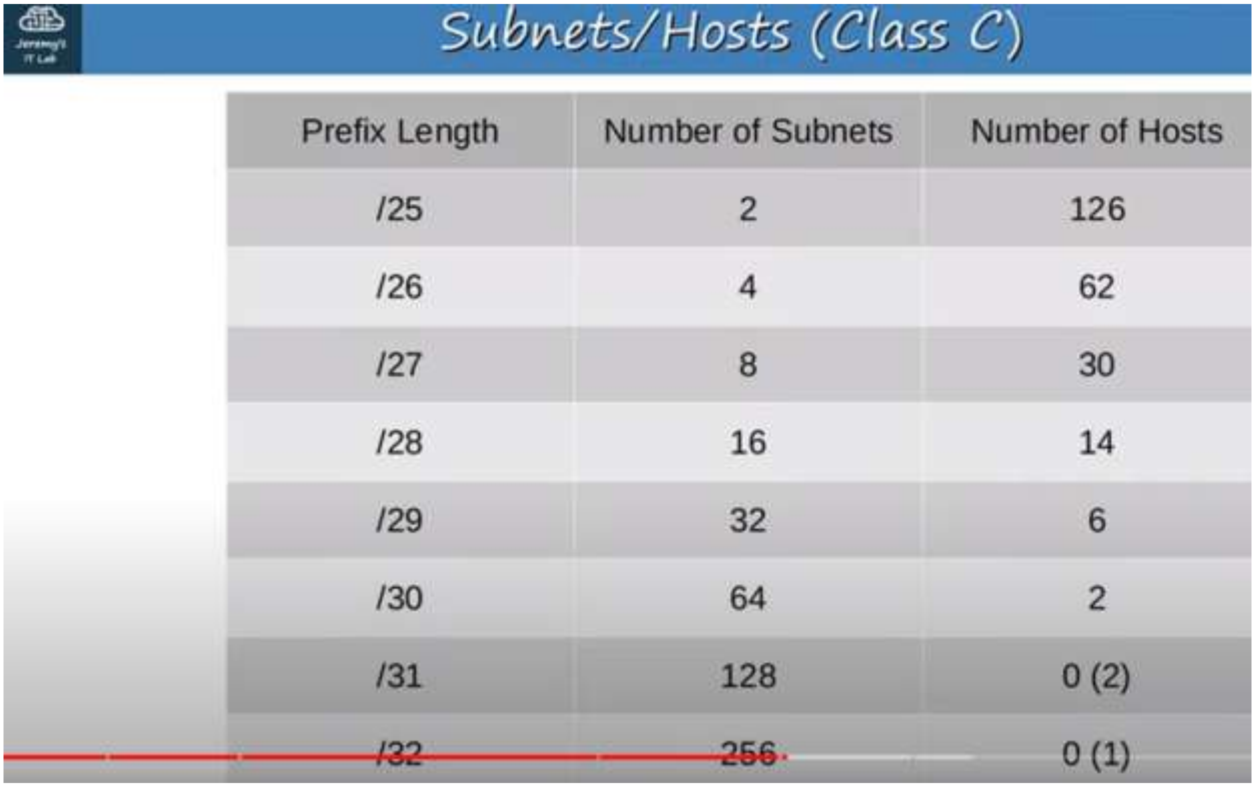
a) The nu of addresses in each subnetwork should be a power of 2
b) The prefix length for each subnetwork should be found using the following formula-> nsub=32-log2Nsub
c) The starting address in each subnetwork should be divisible by the number of addresses in the sunbetwork. This can be achieved if we first assign address to larger subnetworks .



```
192.168.0.1/24 (Classful subnetting)

Decimal - 192.168.0.1
Binary - 11000000.10101000.00000000.00000001
Net ID - 24 bits
Mask - 11111111.11111111.11111111.00000000 (255.255.255.0)
Hosts - 32-(netw bits) = 32 - 24 = 8 bits
# of valid hosts = 256 - 2 = 254
Net ID (First Address) = (Mask) AND (Any Netw Addr) =
11000000.10101000.00000000.00000000 (192.168.0.0)
Directed Broadcast ID (Last Address) = (NOT Mask) OR (Any Netw Addr) =
11000000.10101000.00000000.11111111 (192.168.0.255)
```

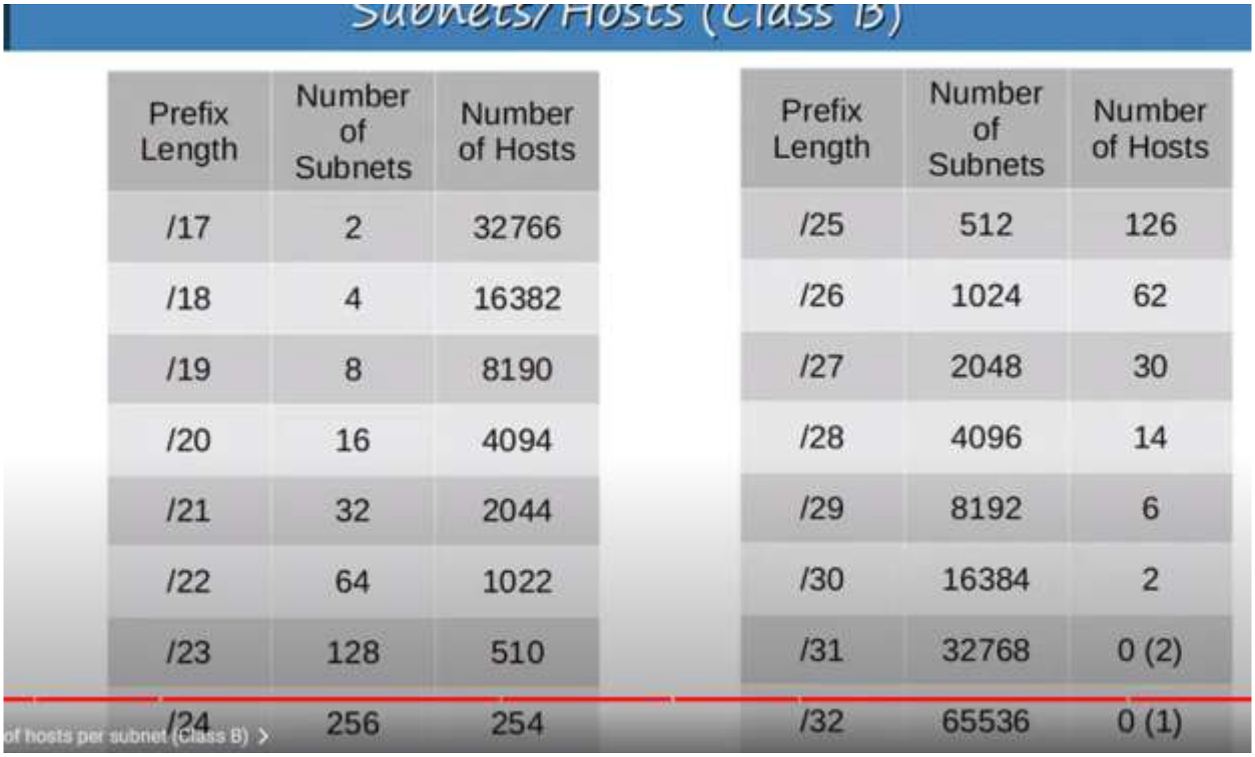


```
Q - Given an address block 133.24.12.53/21. You need to subnet the network that has 5
subnets, each with at least 16 hosts. Which subnet mask would you use?

Decimal - 233.24.12.53
Binary - 10000101.00011000.00001100.00110101
Net ID - 21 bits
Mask - 11111111.11111111.11111000.00000000 (255.255.248.0)
Hosts - 32-(netw bits) = 32 - 21 = 11 bits
# of valid hosts = 2048 - 2 = 2046
Net ID (First Address) = (Mask) AND (Any Netw Addr) =
10000101.00011000.00001000.00000000 (133.24.8.0)
Directed Broadcast ID (Last Address) = (NOT Mask) OR (Any Netw Addr) =
10000101.00011000.00001111.11111111 (133.24.15.255)

Subnet prefix - 133.24.12.53/24
Subnet mask - 255.255.255.0
```



Subnets/Hosts (Class C)

Prefix Length	Number of Subnets	Number of Hosts
/25	2	126
/26	4	62
/27	8	30
/28	16	14
/29	32	6
/30	64	2
/31	128	0 (2)
/32	256	0 (1)



Subnets/Hosts (Class B)

Prefix Length	Number of Subnets	Number of Hosts
/17	2	32766
/18	4	16382
/19	8	8190
/20	16	4094
/21	32	2044
/22	64	1022
/23	128	510
/24	256	254

Prefix Length	Number of Subnets	Number of Hosts
/25	512	126
/26	1024	62
/27	2048	30
/28	4096	14
/29	8192	6
/30	16384	2
/31	32768	0 (2)
/32	65536	0 (1)

Variable Length Subnet Mask

- ➔ **Here the** subnet design uses more than one mask for different subnets of a single class A,B,C or a network
- ➔ It is also defined as a process of subnetting of a subnet
- ➔ In(FLSM->Fixed length subnet mask) all subnets are of equal size but in VLSM the size is variable and it can have variable nu of hosts
- ➔ There is a min wastage of ip address
- ➔ It is the process of creating subnets of different sizes , to make your use of network addresses more efficient .

Steps for doing VLSM

- ➔ Assign the largest subnet at the start of the address space
- ➔ Assign the second largest subnet after it.
- ➔ Repeat the process until all subnets have been assigned

VLANS

What is a Lan?

- ➔ Lan is a gp of devices(PC,servers,routers,switches,etc) in a single location
- ➔ A lan is a single broadcast domain,including all devices in that broadcast domain.
- ➔ A Broadcast domain is the gp of devices which will receive a broadcast frame sent by any one of the members.