Raushan kumar (IIEST Shibpur(2019-2023))

Computer Network

Total videos= 95 , Completion target=19 days(5 videos/day)

Syllabus

1. Physical layer (cables, topology , transmission modes , encoding,LAN Device, Modulation)
2. Data Link (stop and wait , go back and selective repeat, MAC protocols, Switching error control, ethernet frame format)
3. Network(IP addressing , Routing Protocols, IPV4 header, IPV6 header
4. Transport(TCP, UDP, Headers)
5. Session
6. Application
7. Presentation
8. Network Security

Computer Network :

To share the data is the main purpose between sender and Receiver through some connection

- ***Data flow occurring three types***

1. Simplex
2. Half duplex
3. Full duplex

Simplex:

1. Communication is always unidirectional
2. One device can transmit and one device can receive
   Example : keyboard, monitors

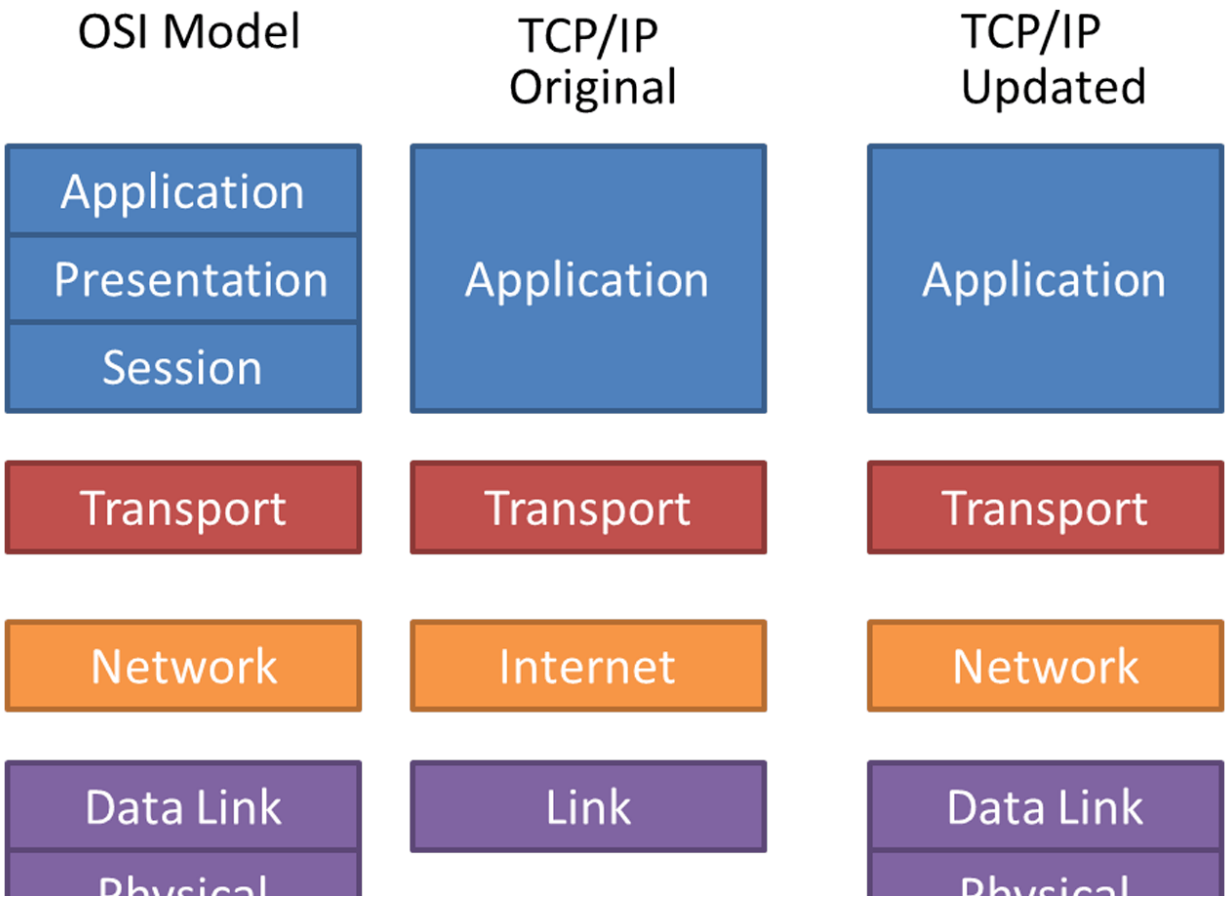
Half Duplex:

1. Communication in both direction but not at same time
2. If one device sending then other can receive vice -versa
   Example : wookie-tookie

Full duplex:

1. Communication in both direction simultaneously
2. Device can send and receive at same time

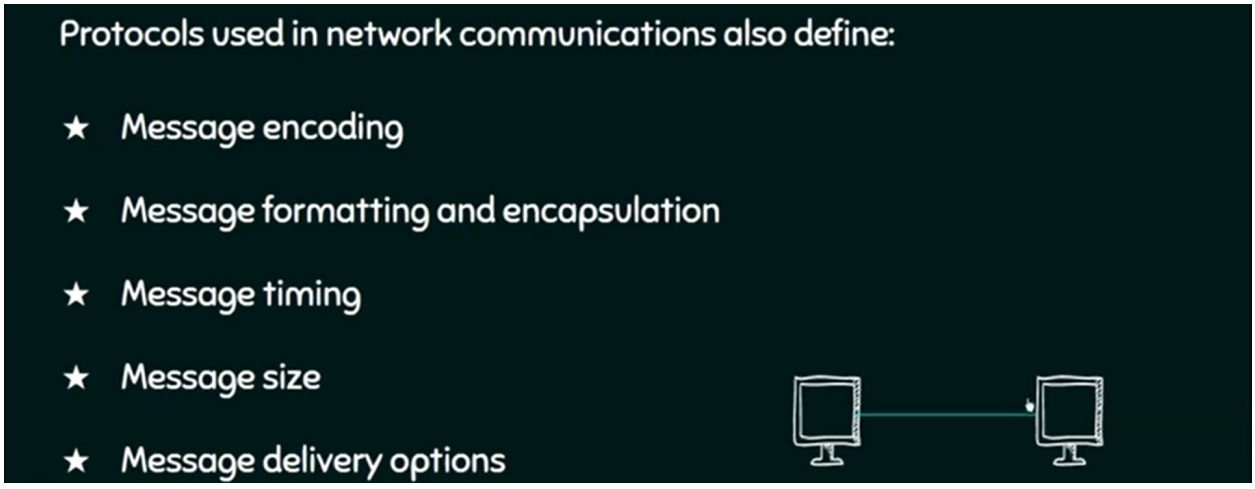
Example : Telephone-line



Proper Communication

Message(protocol) (connection) Message (some Protocol)
S—----------->R

To understand both sides of the message , we generally use protocol
Protocol = Set of proper instruction is call Protocol



- Agar Sender and Receiver same machine me raha to usko Operating system handle karta hai (keyboard sender and Monitor Receiver)
- Where client and server present at different machines then computer networks come .
- Let's assume client india me present hai and server USA me , then main functionality of computer network is feel like both are present in the same machine(like linkedin ,insta ko open me hona me kitna time lagta hai normally 1 sec ,2 sec haha)

- **Components of COMPUTER NETWORK**
    1. Nodes(starting and ending point) 2. Media(wired and wireless media) 3. Services

→ **Wired Media (Guided media)**

1. Ethernet straight- through cable
2. Ethernet crossover cable
3. Fiber optic cable
4. Coaxial cable
5. USB cable;

→**wireless Media(unguided media)**

1. Infrared
2. Radio
3. Microwaves
4. Satellite

→ **Services**

1. E-mail 2. Storage Services 3.File sharing 4.instant messaging 5.Online game 6. W.w.w

Classification of computer networks

1. **Local Area Network (LAN)**

A local Area network (LAN) is a computer network that interconnects computers within a limited area such as a residence , school , laboratory , university campus or office building

LAN-DEVICES

Wired LAN (example - Hub, Switch)

Wireless LAN (example - Wi-fi)

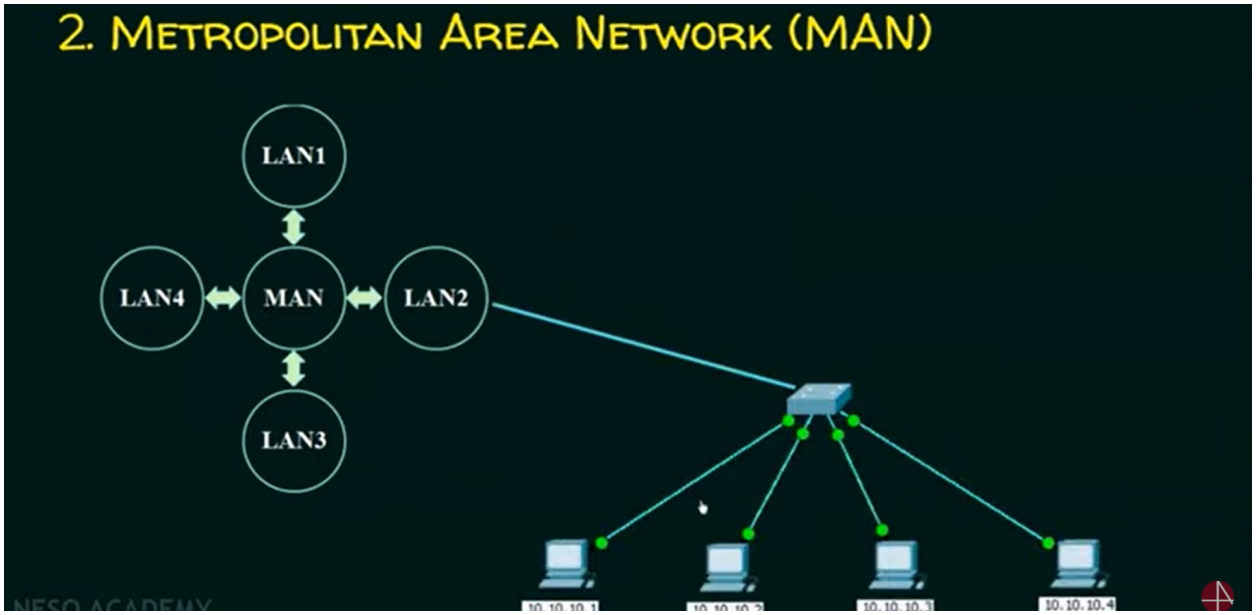
2. **Metropolitan Area Network(MAN)**
3. **Wide Area Network(WAN)**

Metropolitan Area Network(MAN)

A metropolitan area network (MAN) is a computer network that interconnects users with computer resources in a geographic region of the size of a metropolitan area(city)

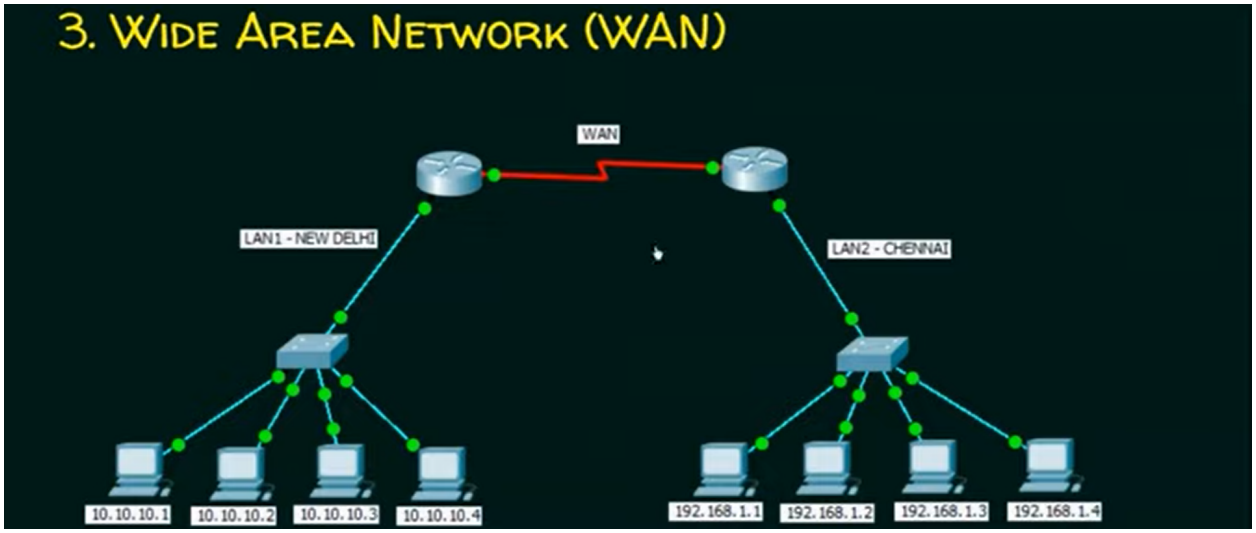
MAN-DEVICES

- Switches/Hub
- Routers/Bridges



WAN :- A wide area network (WAN) is a telecommunications network that extends over a large geographical area for the primary purpose of computer networking

Example : end devices and intermediary devices



⇒**STORAGE AREA NETWORK (SAN) (cloud computing)**

It is the on-demand availability of computer system resources , especially data storage and computing power, without direct active management by the user .

- In server to client and client to server communication we use 2 ways functionality

1. Mandatory	2. Optional
a. Error Control	a. Encryption/Decryption
b. Flow Control	b. Check Point
c. Mux , DEMUX	

What is the need of the OSI model ?

Uper so saare functionality mention hai , to usko combine karke ek model bana tha that is known as OSI model (theoretical model)

To sender send karne se pahle or Receiver se pahuchne se pahle to saare protocol ko follow karege (OSI)

- OSI stands for Open System interconnection
- It is a model for understanding and designing a network architecture that is flexible and interoperable.
- Developed by the international standards for Organizations (ISO)
- The OSI model is not a Protocol.
- It is only a guideline and hence it is referred to as the OSI reference Model .

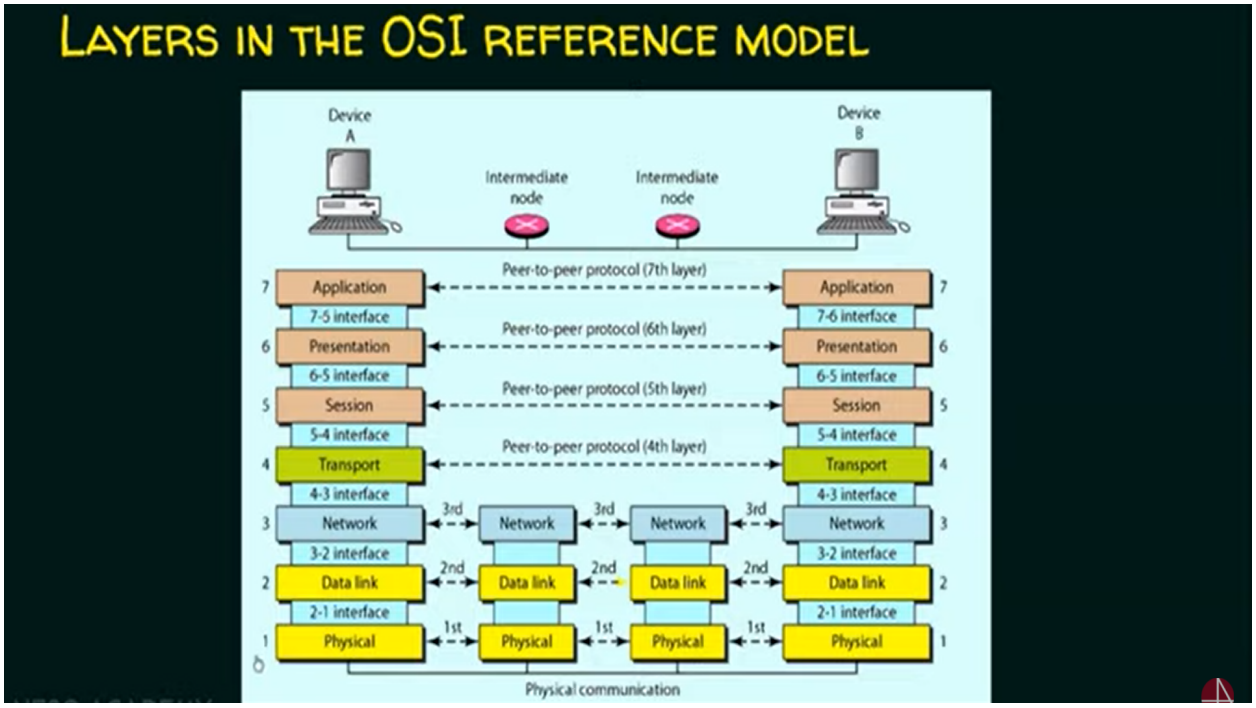
And further OSI model further divides into seven layer

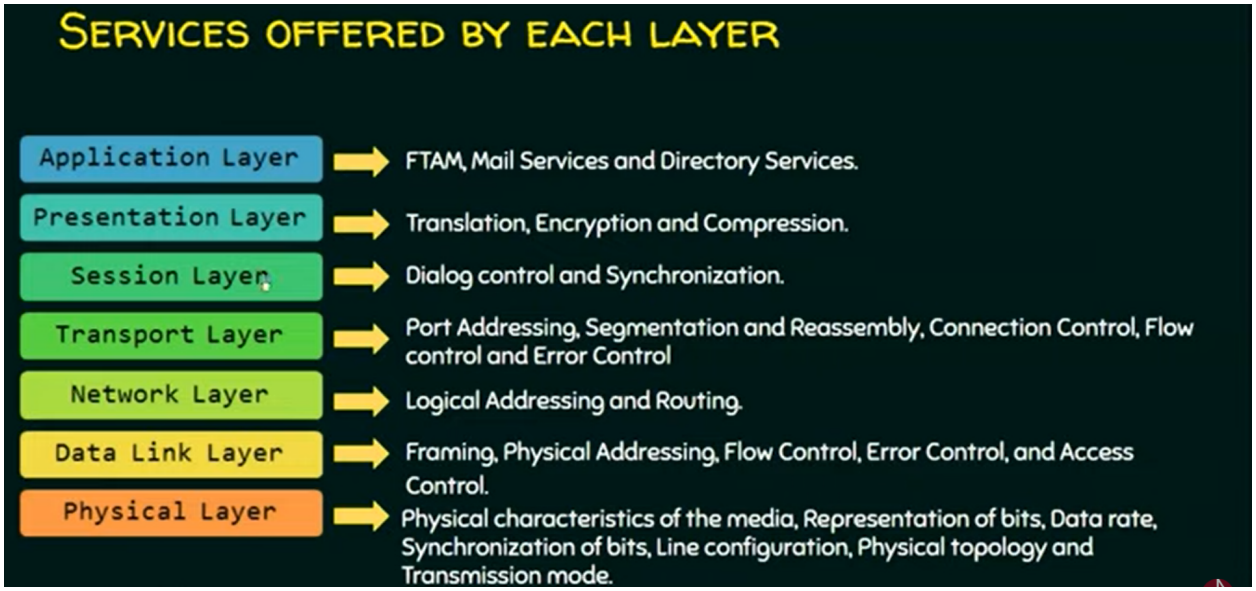
Heart of the OSI model (total 7 layers)

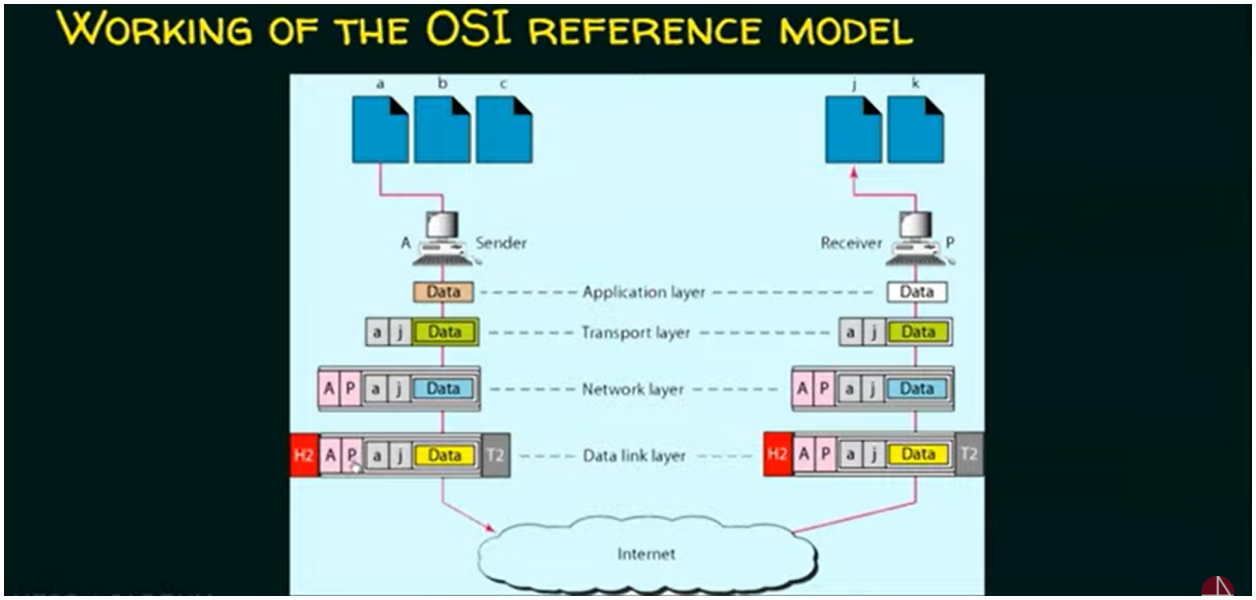
Application layer
Presentation layer
Session layer
Transport layer
Network layer
Data layer
Physical layer

Way to remember it

Please Do Not Throw Sausage Pizza Away





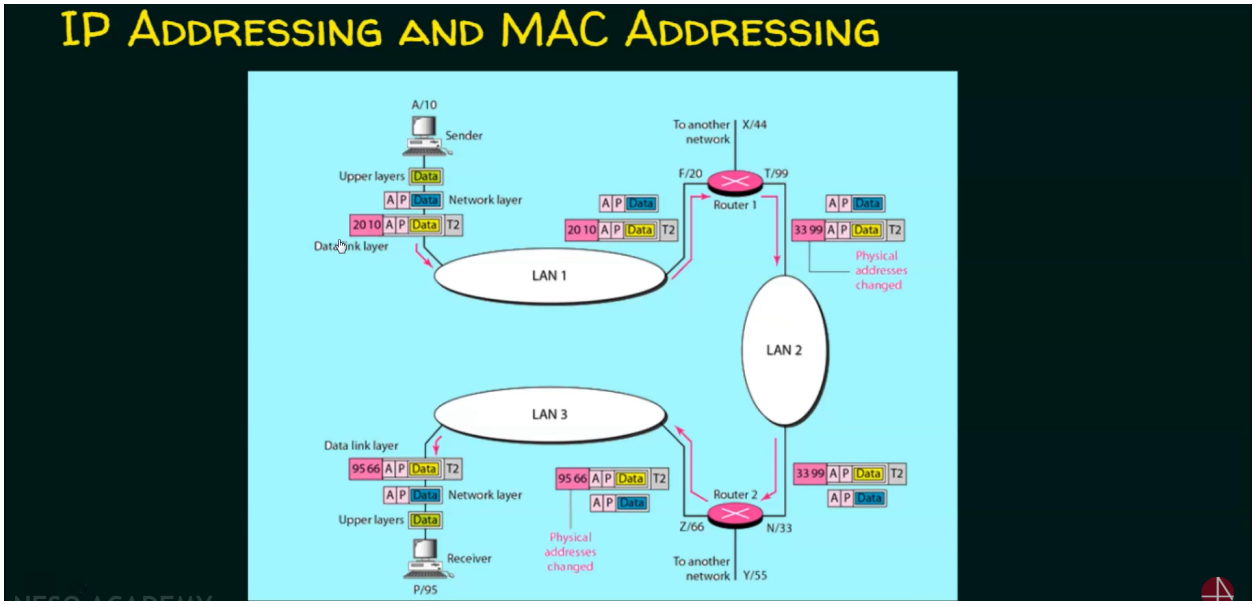


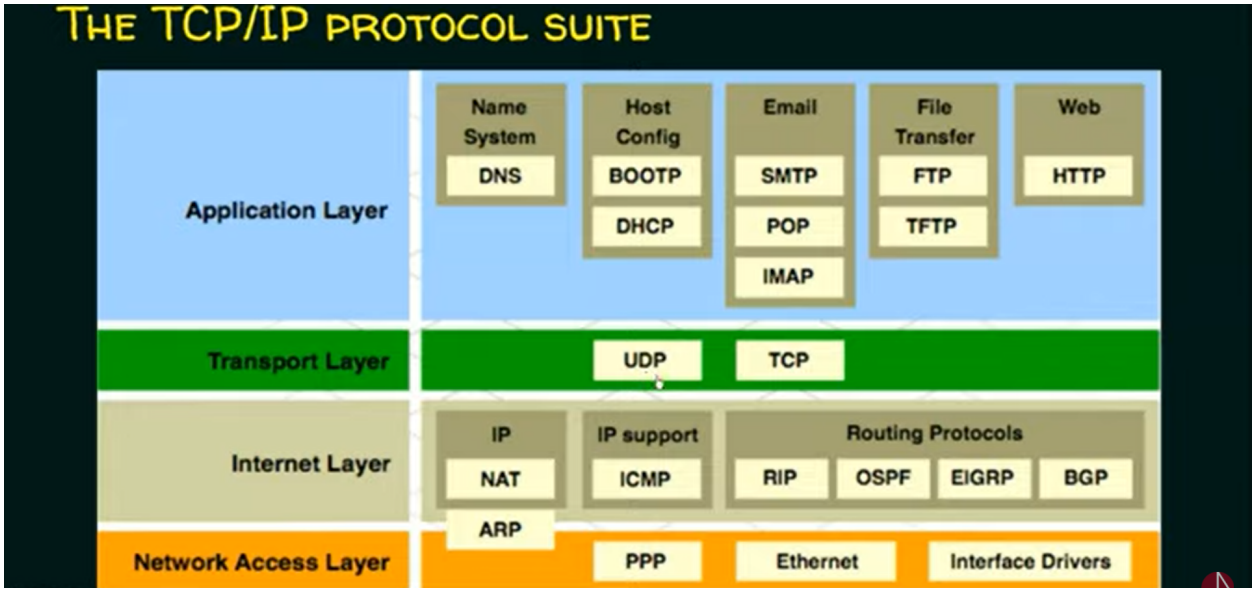
APPLICATION : Represents data to the user , plus encoding and dialog control

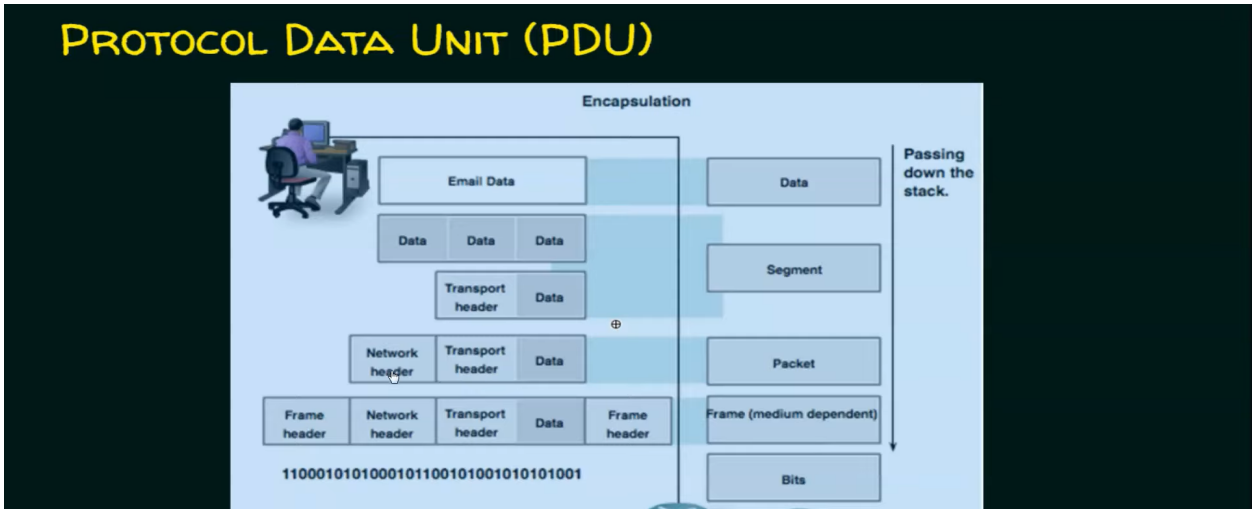
TRANSPORT: Supports communication between diverse devices across diverse networks

INTERNET: Determines the best path through the network

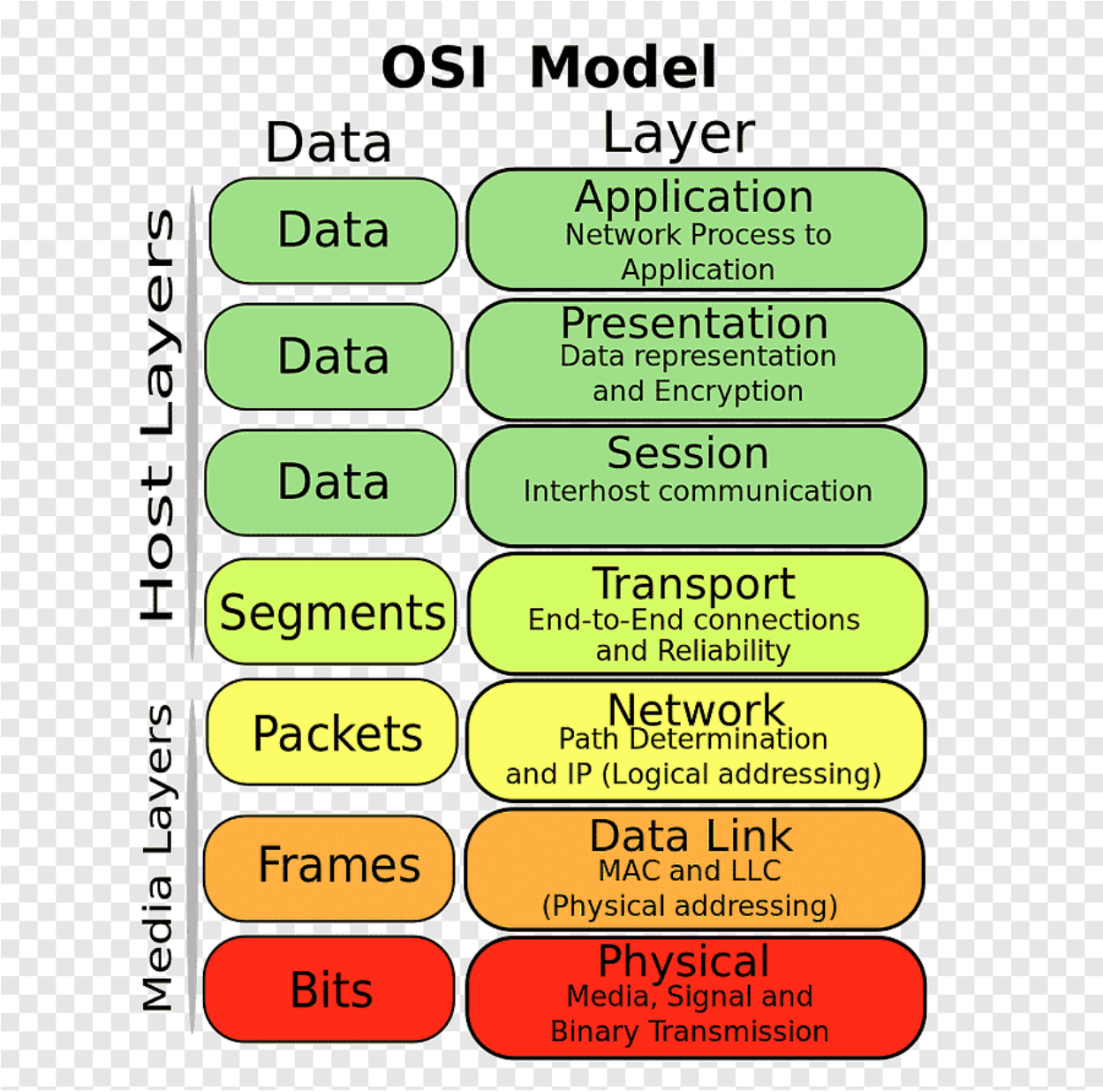
NETWORK ACCESS : Controls the hardware devices and media that make up the network







That means when ever we send the message it will have to pass all the layers of the OSI models (for the both end receiver and sender)



TCP/IP vs OSI model

TCP/IP protocol suit or internet protocol

1. Developed by ARPANET
2. Support Client-server and Peer to peer

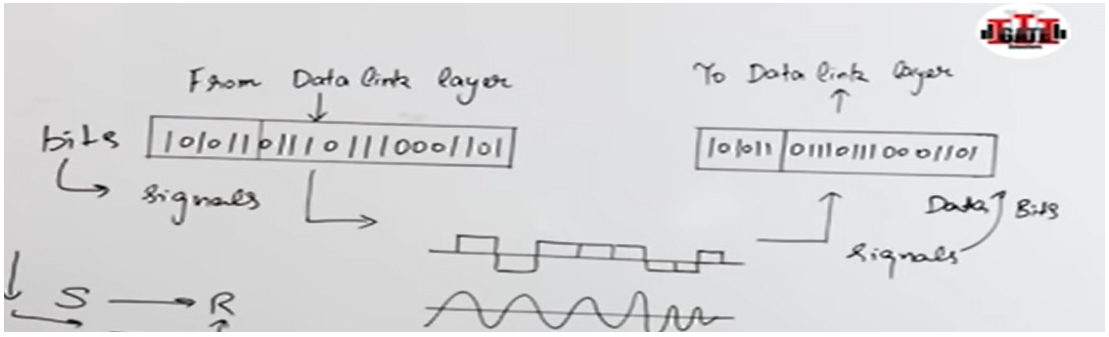
Another name of the layer

1. Process to process (blue region)
2. Host to host (red region)
3. Source to destination (Yellow region)
4. Node to node (Purple region)

Physical layer and Its functionality

1. Cables and Connectors
2. Physical topology
3. Hard wares (Repeaters , Hubs)
4. Transmission mode(one sided)
5. Multiplexing (frequency ko divide kar sakte hain issme)
6. Encoding

Physical layer , hardware se deal karte hain
Isske upper saare software + hardware se deal karta hai but physical layer deals with only
Hardware (tangible things)



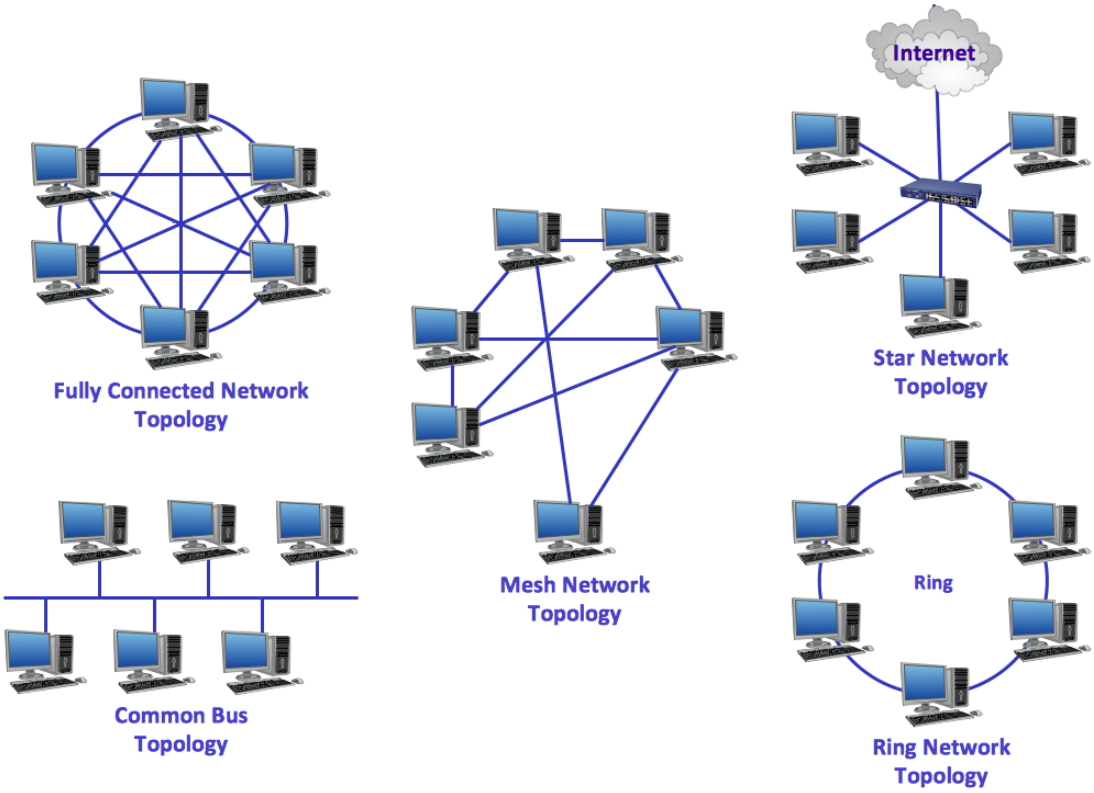
Topology

It tells that how devices connected to each other

Physical Topology : Placement of various nodes
Logical Topology : Deals with the data flow in the network

Types of Topology (intermidatary nodes)

1. Mesh
2. Star
3. Bus
4. Ring
5. Hybrid



n = no of devices

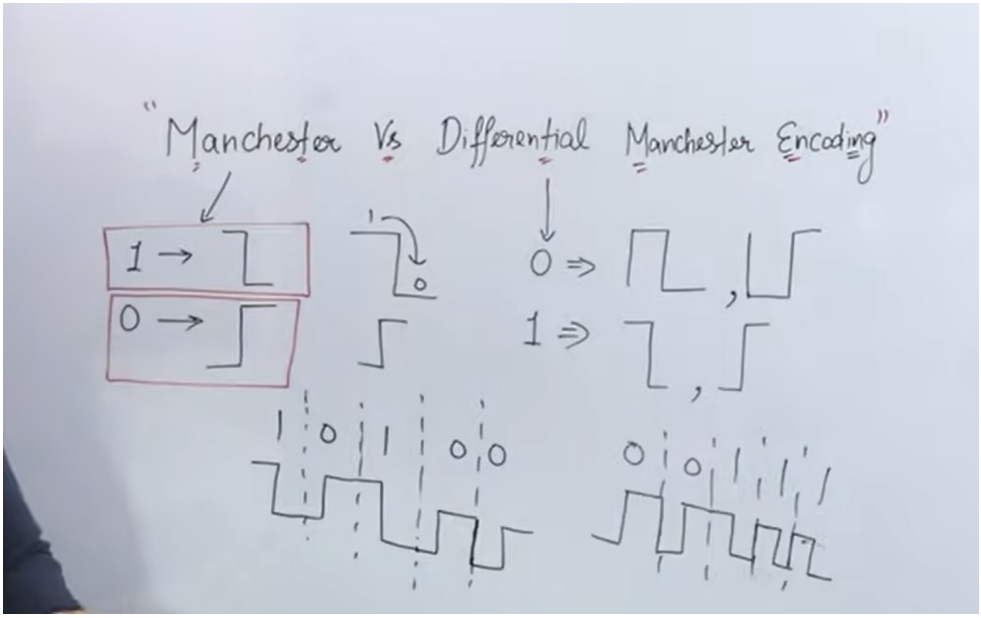
Types	No of cables	No of ports	Reliability	Cost	Security
Mesh	n*(n-1)/2	(n-1)*n	Highest	High	High
Star	n	1*n	Very less	Low	Mesh se Ls
Bus	1(bb)+ n (DL)	1*n	Not at all	Low	Not at all
Ring	1+n	1*n	Low	Low	Low

Mesh and star *supporting point to point communication* (dedicated communication)
Star ke center me hub use hua and hub is multiport devices
Bus topology is multi point , agar multi point hua to collision to hoga (maximum collision can be n)

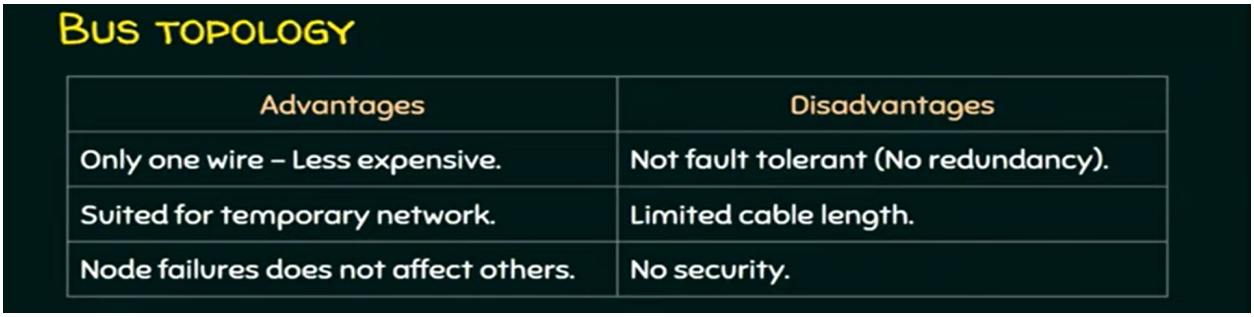
Ring topology unidirectional hota hai

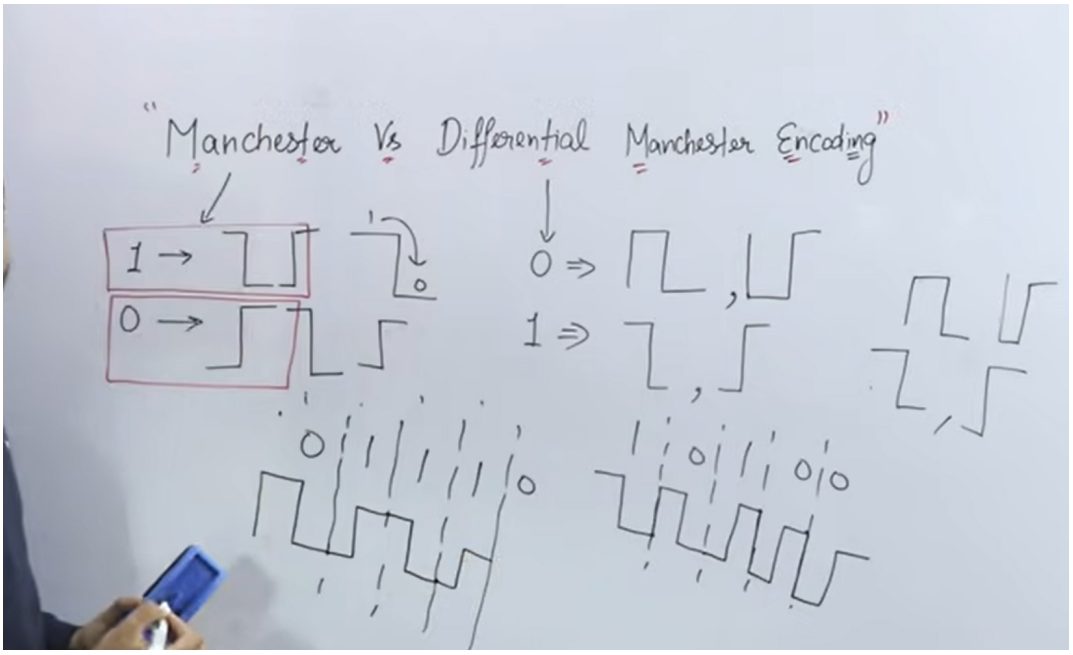
Difference between Manchester and Differential Manchester Encoding

Ye digital to digital me use hota hai



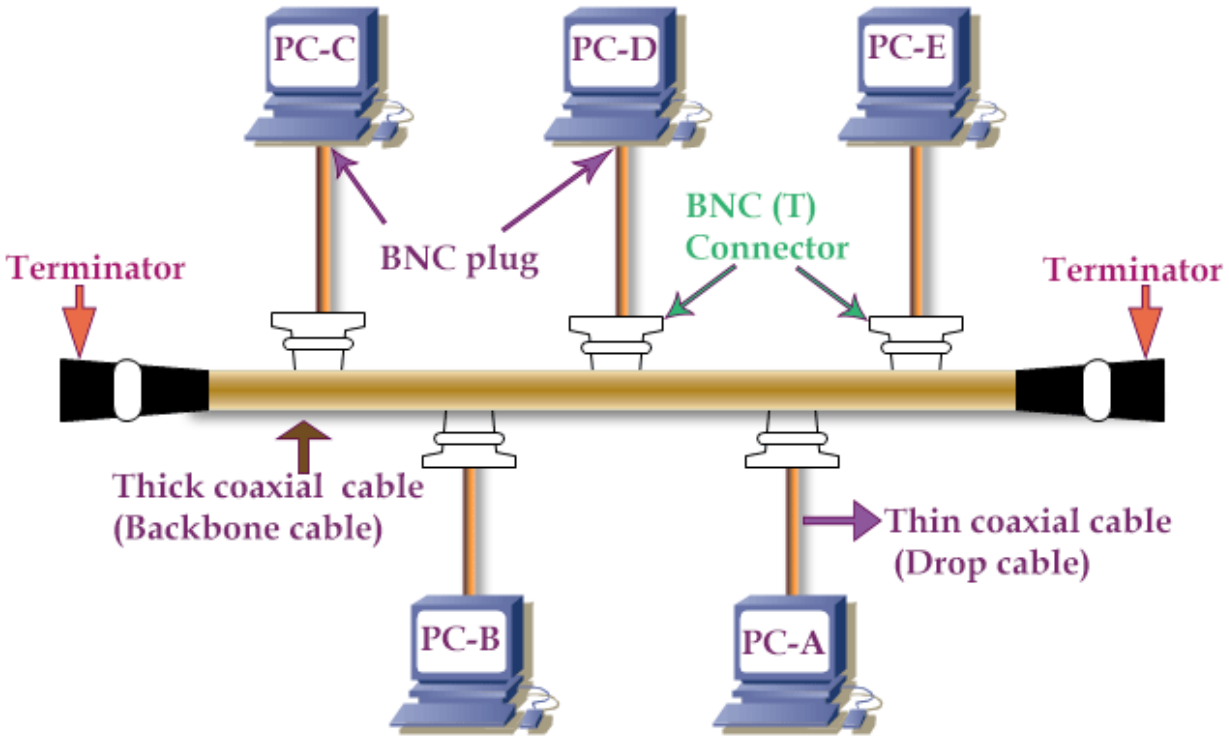
Yeh Manchester Encoding hai





Ye differential Manchester Encoding

Bus topology

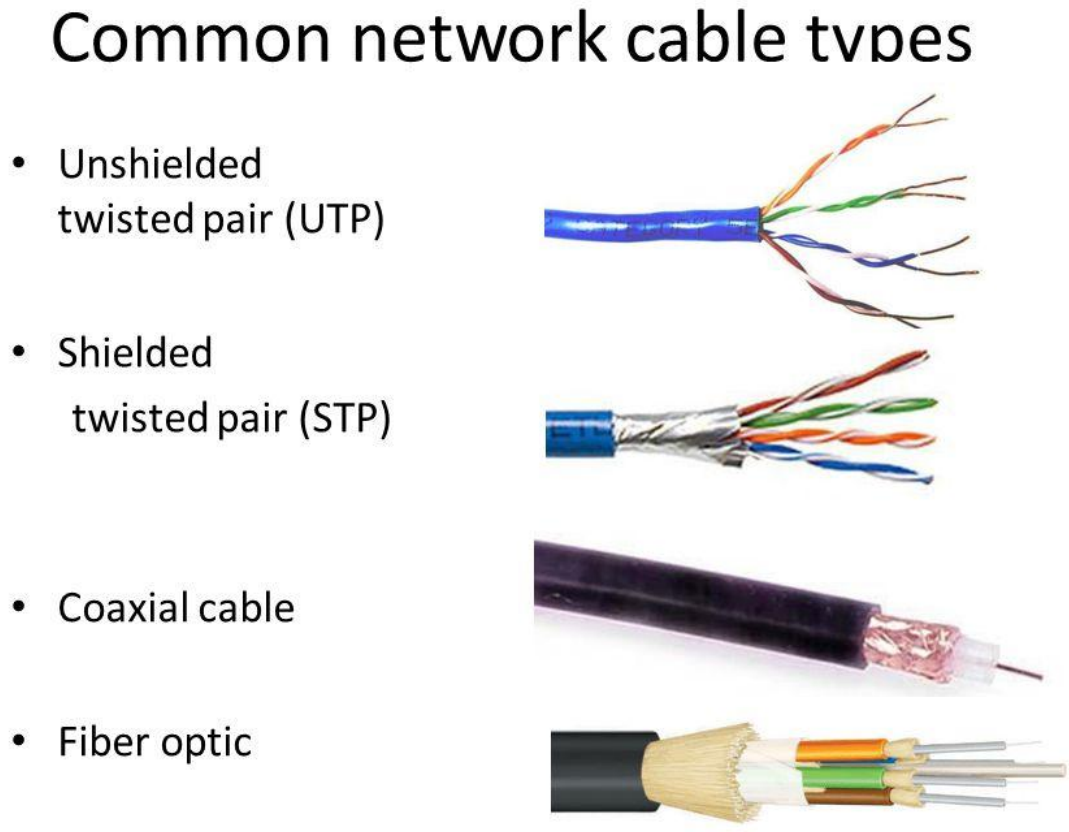


Various Devices in computer Networks

1. Cables
2. Repeaters
3. Hubs
4. Bridges
5. Switches
6. Routes
7. GateWay
8. IDS
9. Firewall
10. Modem

1 to 3 ===> pure hardware
4 to 6====> hardware and software dono work karta hai issme
8 to 9 ===> security purpose

Cables



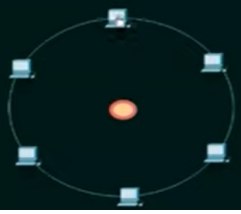
Types

1. ***Unshielded Twisted* Pair cable** (10 Base T = 10 Mbps base matlab unidirectional and T= 100 meters,matlab 100 meter ke baad attenuation ho jayega , Ethernet LAN ,local)

2. ***Coaxial Cable*** (10 Base 2 or 10 base 5)
3. ***Fibre Optics*** (100 base FX==2km) and speed light ke barabar

RING TOPOLOGY

- ★ A ring topology is a bus topology in a closed loop.
- ★ Peer-to-Peer LAN topology.
- ★ Two connections: one to each of its nearest neighbors.
- ★ Unidirectional.
- ★ Sending and receiving data takes place with the help of a TOKEN.



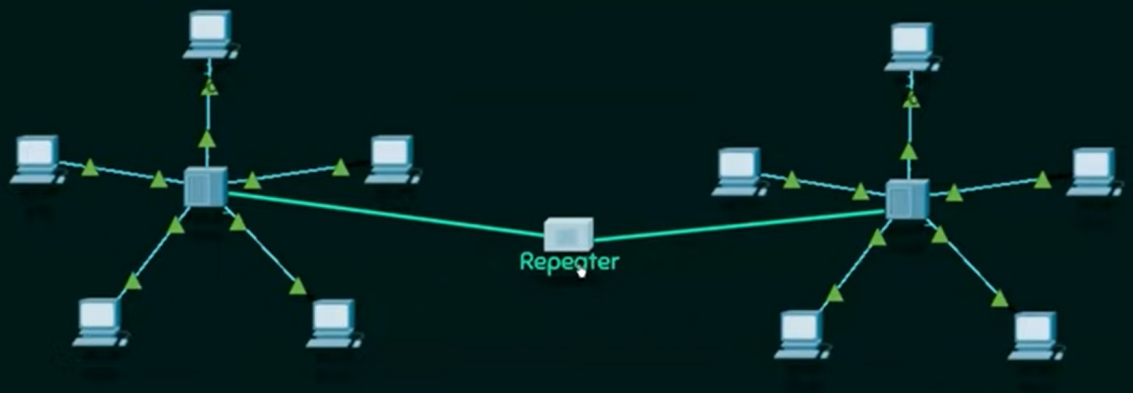
RING TOPOLOGY

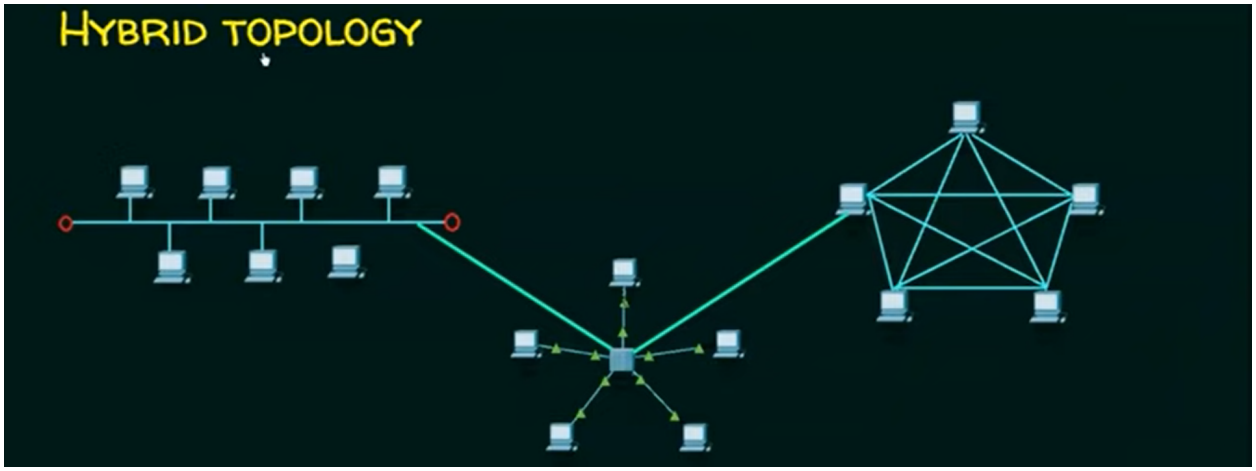
Advantages	Disadvantages
Performance better than Bus topology.	Unidirectional. Single point of failure will affect the whole network.
Can cause bottleneck due to weak links.	↑ in load – ↓ in performance.
All nodes with equal access.	No security.

STAR TOPOLOGY

Advantages	Disadvantages
Easy to design and implement.	Single point of failure affects the whole network.
Centralized administration.	Bottlenecks due to overloaded switch/Hub.
Scalable.	Increased cost due to switch/hub.

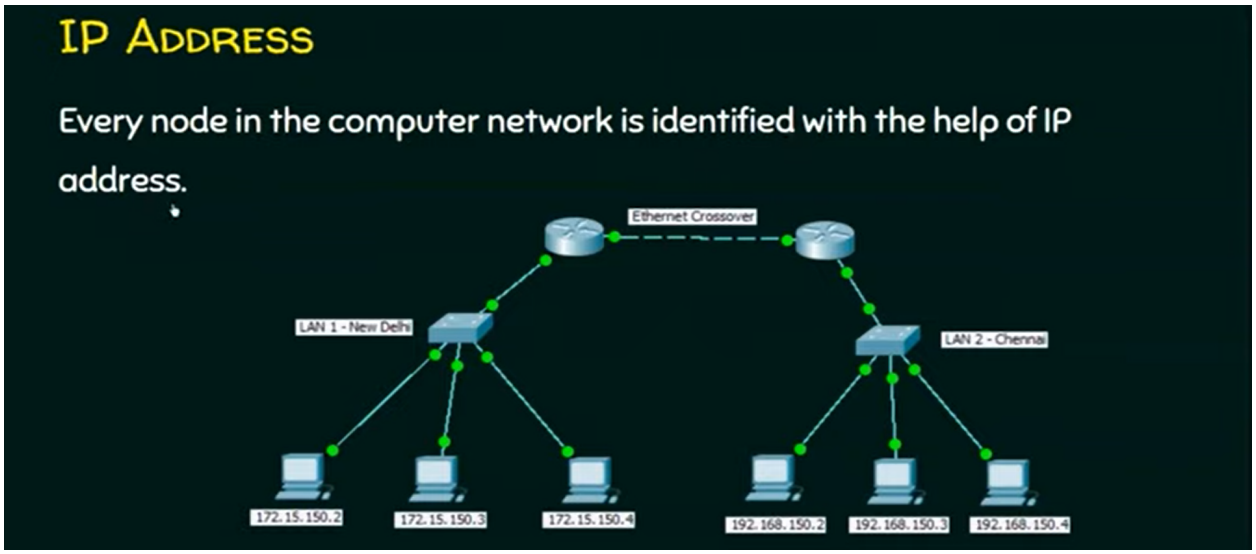
EXTENDED STAR TOPOLOGY

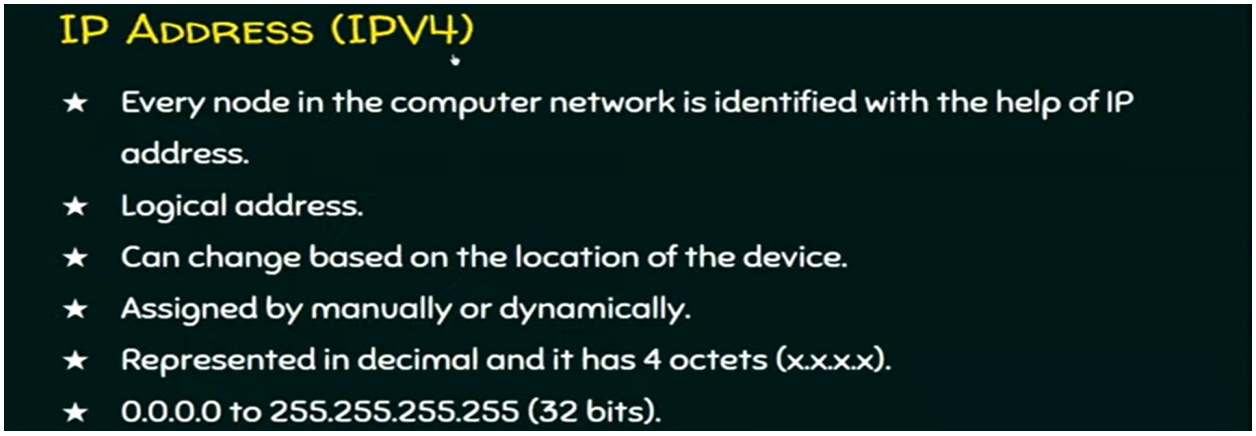




IP Address

- IP stands for Internet Protocol
- Every node in the computer network is identified with the help of an IP address.





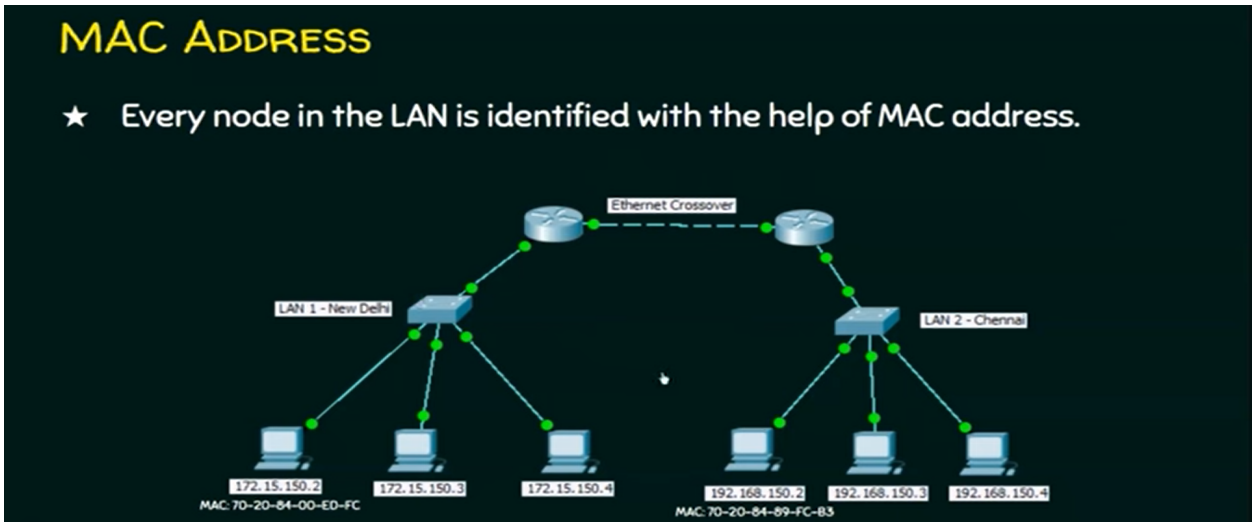
MAC address

MAC stands for Media access control

Ever node in the LAN is identified with the help of MAC address

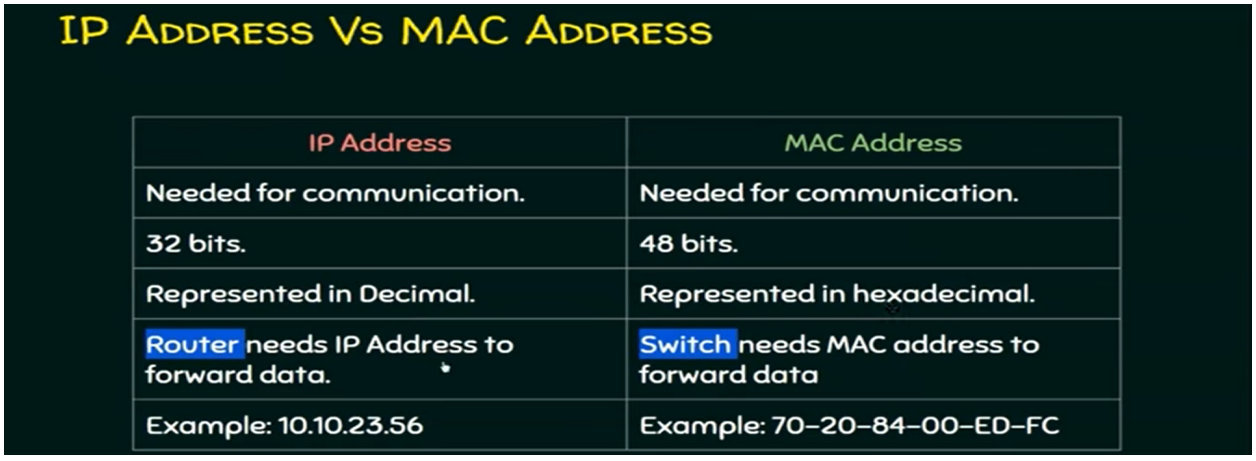
IP address = Location of a person

MAC address= Name of the person



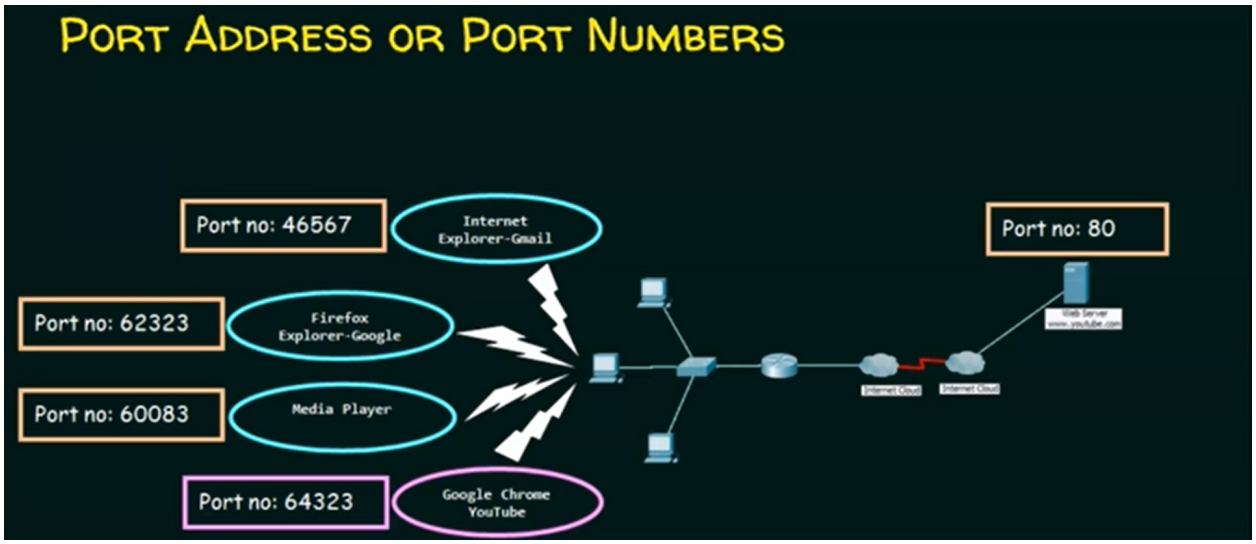
MAC Address:

1. Every node in the LAN is identified with the help of MAC address
2. Physical address or Hardware Address
3. Unique
4. Can not be changed
5. Assigned by manufacturer
6. Represented in hexadecimal
7. Example : 70-20-84-00-ED-FC(48 bits)
8. Separator : hyphen(-), period(.), and colon(:).



DERIVATION FROM ANALOGY

⇒ Reaching Our CIty → Reaching our network (IP Address)
⇒Reaching Our Apartment→ Reaching the host (MAC address)
⇒Reaching the right Person → Reaching the right process(Port Address)

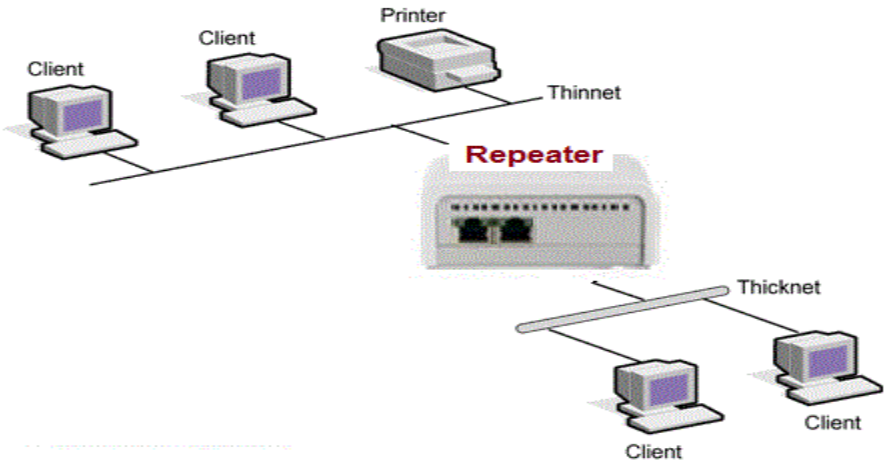


⇒ 3 key Points to Ponder
Before sending the data , any node must

- Attach source IP address and destination IP address
- Attach source MAC address and destination MAC address
- Attach source port number and destination port number

Reater (physical layer or hardware)

Jan 27, 2022



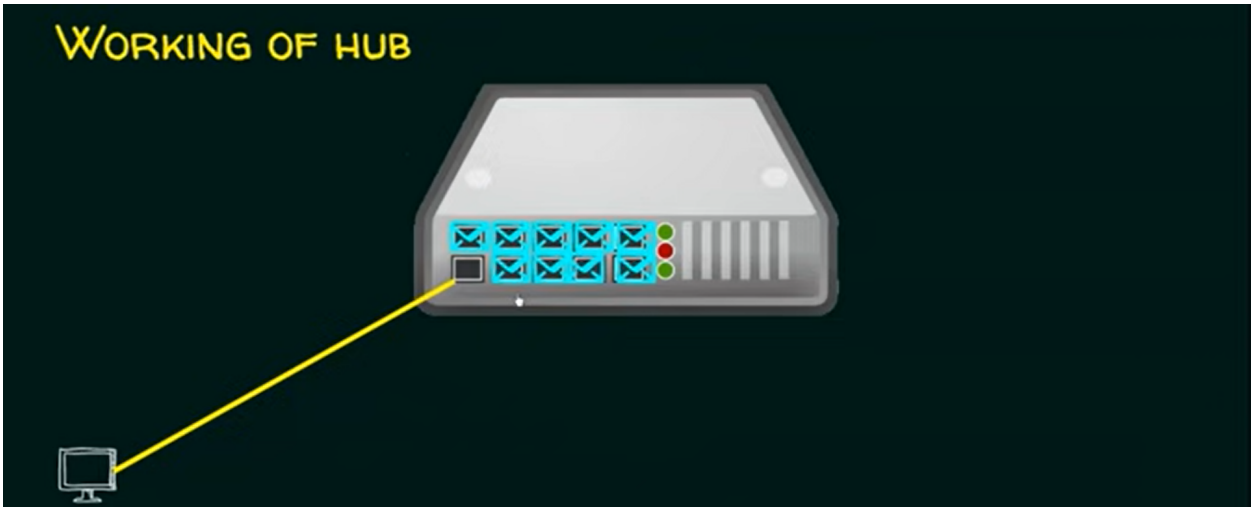
Repeater jo hai , strength ko regenerate kar deta hai (original strength ke barbar hi karega) and it is two port device and yes it's forwarding and no filtering and maximum n

collision possible ho sakta hai where n= no of devices and it always work as physical layer and physical layer means its purely a hardware

- 2 port device

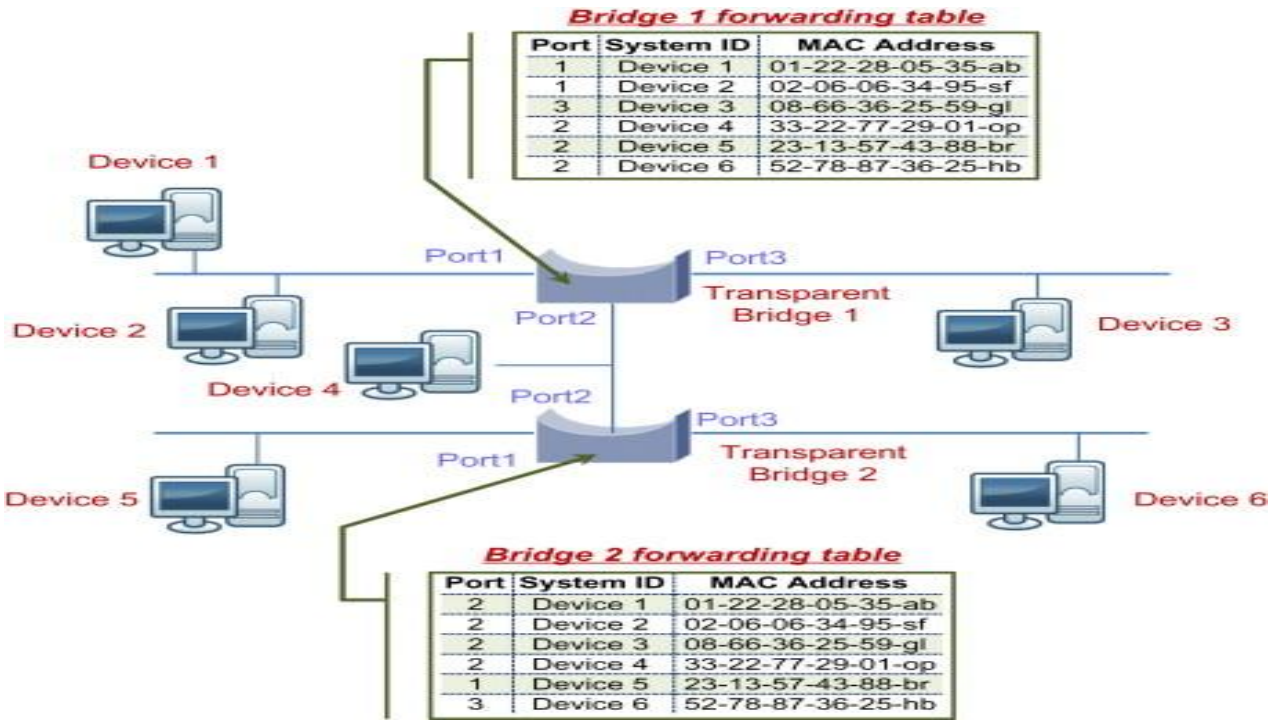
Farwardin ⇒ Yes
Filtering ⇒ No
Collision ⇒ maximum because of no filter due to hardware

Hub(Physical Layer)



1. A.k.a Network Hub.
2. Hub works at the physical layer of the OSI model
3. Used to set up LAN
4. Star topology
5. When a packet arrives at one port , it is copied to the other ports so that all segments of the LAN can see all packets.
6. Multiport Repeater
7. Forwarding
8. No filtering (because ye software nahi hai pure hardware hai to ye decide nahi kar pata)
9. Collision domain (maximum n sab ek baar hi bhej de toh ?)
10. Blink waala (indicator)

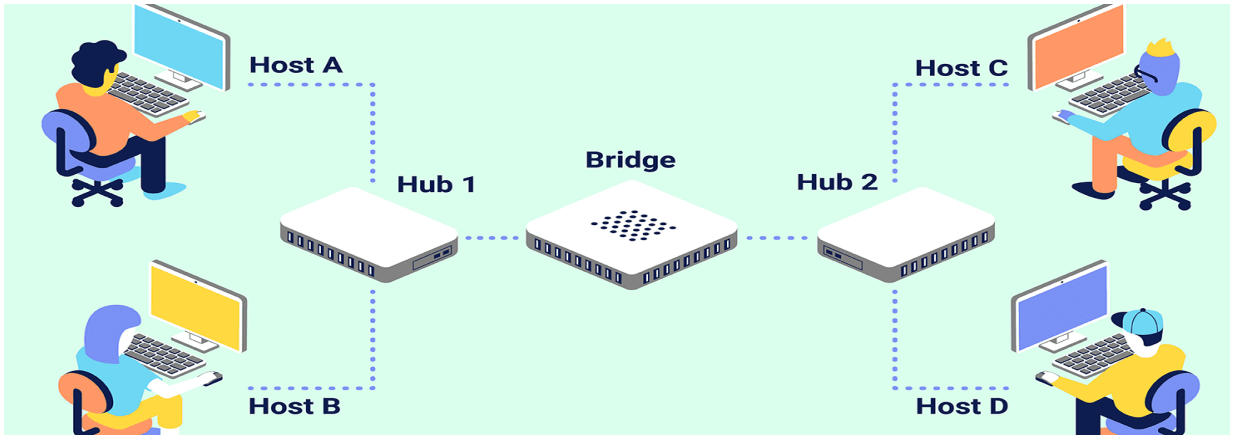
Filtering(stopping) and forwarding



Bridges are Two types

1. Static (manually type karna pdta hai)
2. Dynamic or Transparent (ye learn karta hai , real life me use hota hai)

Bridges (physical and Data link Layer)



1. Connect two different LANs
2. Forwarding
3. Filtering

4. Collision Domain (no collision because bridge use store and forward strategy)
5. Bridge Data unit protocol (loops ko hatane ke liye through spanning tree)
6. Bridge = Repeater + functionality of reading MAC address
7. It is layer 2 device
8. It is also used for interconnecting two LANs on the same protocol
9. It is also 2 port device

Two types of bridges:

1. **Transparent Bridges**
    - These are the bridge in which the stations are completely unaware of the bridge existence
    - Reconfiguration of the stations is unnecessary even if a bridge is added or removed from the network.
2. **Source Routing Bridges**

- In these bridges , routing operation is performed by the source station and the frame specifies which route to follow .

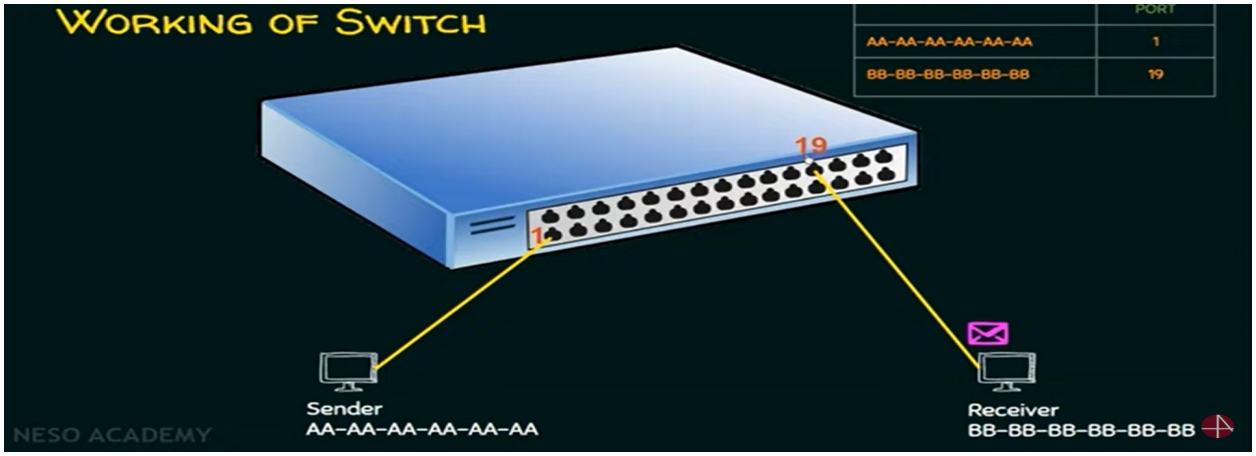
Working of Bridges

Bridge connects two networks which are running on the same protocol . It is a layer 2 device .

Difference between Bridge and router is that routers connect the two different networks which run on different protocols.
Router is a layer 3 device.

Switch

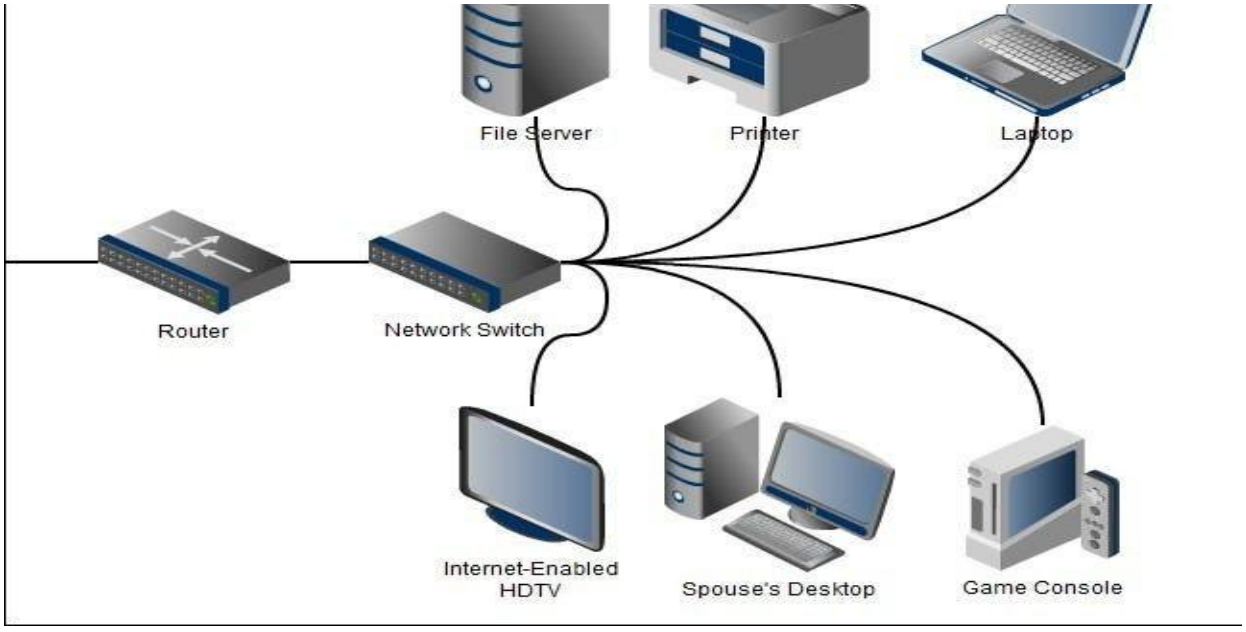
- ***A switch is a network hardware that connects devices on a computer network to establish a local area network***
- Unlike hub , switch has memory
- Store MAC ADDRESS TABLE
- Layer 2 Devices for setting up LAN.
- Layer-2(data link Layer) Device
- Multiport Bridge
- Full Duplex Links
- Traffic is minimal
- Collision Domain is zero (0)



It depends on requirement ki kitna ko bhejna hai

Routers(physical , data link, network layer)

- To connect two different network
- Issm humlog especially internet ki (WAN ki)
- Routers , three layer pe kaam karta hai baaki 2 layer pe kaam karta hai)
- Forwarding (by using routing table)
- Iske sath multiple network v connect ho sakte hain
- Filtering ⇒yes it can stop
- Routing ⇒
- Collision⇒ no collision
- Flooding ⇒ har direction me network bhejna
- MAC address⇒ local area , IP address⇒ wide area ke liye
- A router is a networking device that forwards data packets between computer networks.
- A router is connected to at least two networks , commonly two LANs or WANs or a LAN and its ISPs network.
- It is a layer 3 (network layer) device.
- Stores routing table.



Collision Domain Vs BroadCast Domain

Domain = kitna area cover kar sakta hai

Collision Domain vs Broadcast Domain

Sr no.	Device Name	Collision Domain	Broadcast Domain
1	Repeater	No Change	No Change
2	Hub	No Change	No Change
3	Bridge	Reduce	No Change
4	Switch	Reduce	No Change
5	Router	Reduce	Reduce

1. Collision Domain – A Collision Domain is a scenario in which when a device sends out a message to the network, all other devices which are included in its collision domain have to pay attention to it, no matter if it was destined for them or not. This causes a problem because, in a situation where two devices send out their messages simultaneously, a collision will occur leading them to wait and re-transmit their respective messages, one at a time. Remember, it happens only in the case of a half-duplex mode.

2. Broadcast Domain –

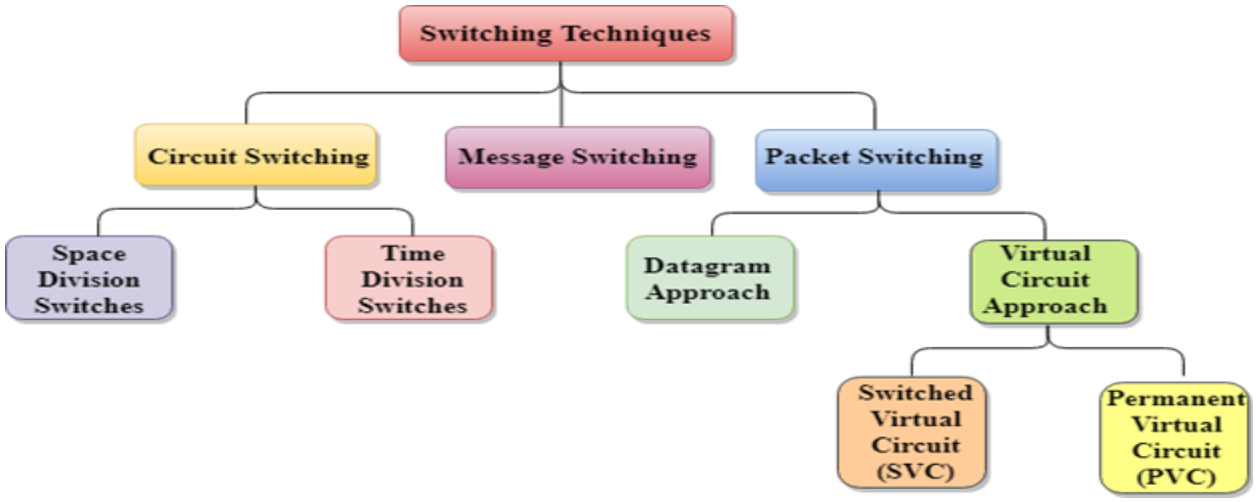
A Broadcast Domain is a scenario in which when a device sends out a broadcast message, all the devices present in its broadcast domain have to pay attention to it. This creates a lot of congestion in the network, commonly called LAN congestion, which affects the bandwidth of the users present in that network.

From this, we can realize that the more the number of collision domains and the more the number of broadcast domains, the more efficient is the network providing better bandwidth to all its users.

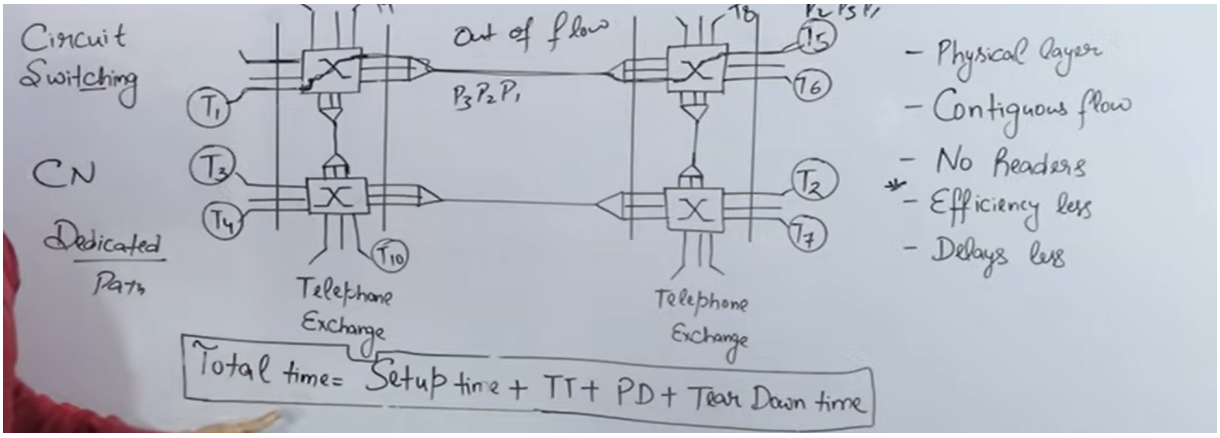
Repeater = ye to sirf frequency maintain karta hai

Jan 28, 2022

- ***Switching*** in a computer network helps in deciding the best route for data transmission if there are multiple paths in a large network .
- ***One -to-one connection***



Circuit Switching



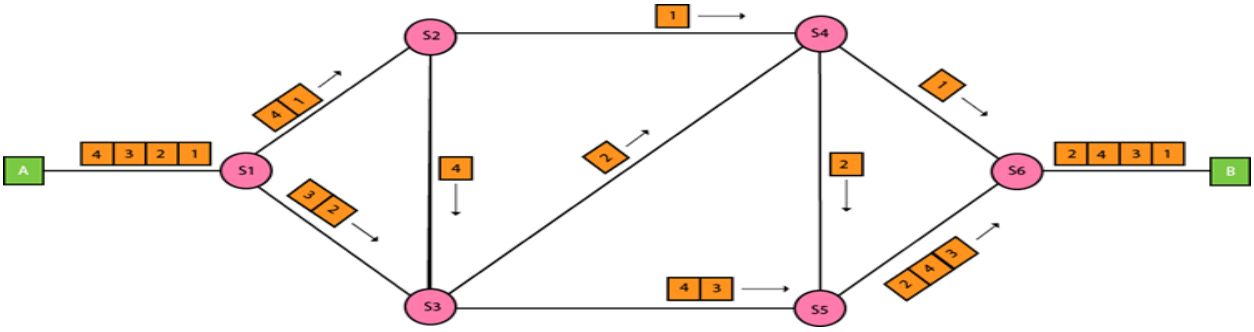
PD= propagation Delay (d/speed) TT= transmission time (message size/bw)

3 phases in circuit switching

1. **Connection establishment 2. Data transfer 3. Connection Disconnection**

- ***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, or video, a request signal is sent to the receiver then the receiver sends back the acknowledgement to ensure the availability of the dedicated path. After receiving the acknowledgment, a dedicated path transfers the data.
- Fixed data can be transferred at a time in circuit switching technology.

Packet switching

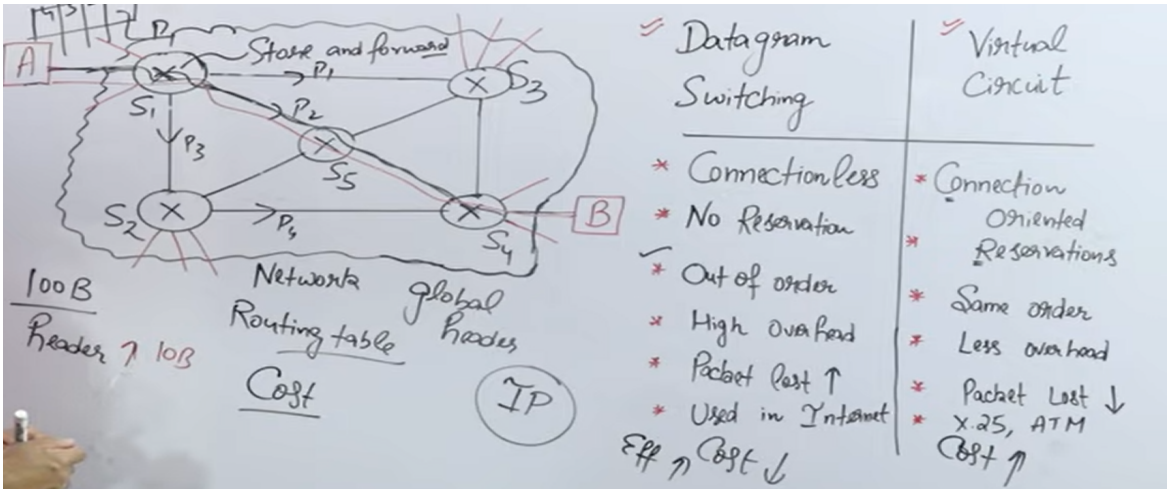


1. Data link and Network layer 2. Store and forward 3. Pipeline use 4. Efficiency high 5.Delay high

- The internet is a pocket switched network
- Message is broken into individual chunks called as packets
- Each packet is sent individually
- Each packet will have a source and destination IP address with sequence number.
- Sequence number will help the receiver to

1. Reorder the packets
2. Detect missing packets and
3. Send acknowledgements.

Two types of packet switching

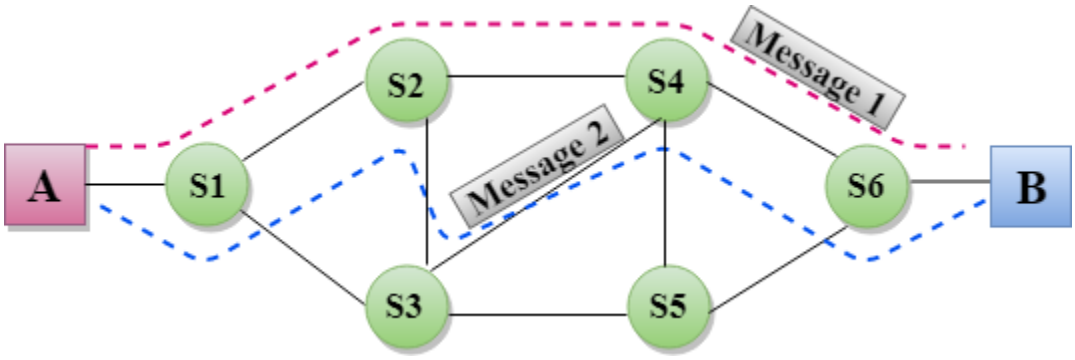


ATM= asynchronous transfer mode

Message Switching

- Predecessor of packet switching
- Store and forward
- Hop by hop delivery
- Dely will be more
- 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 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 forwards it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



Advantages Of Message Switching

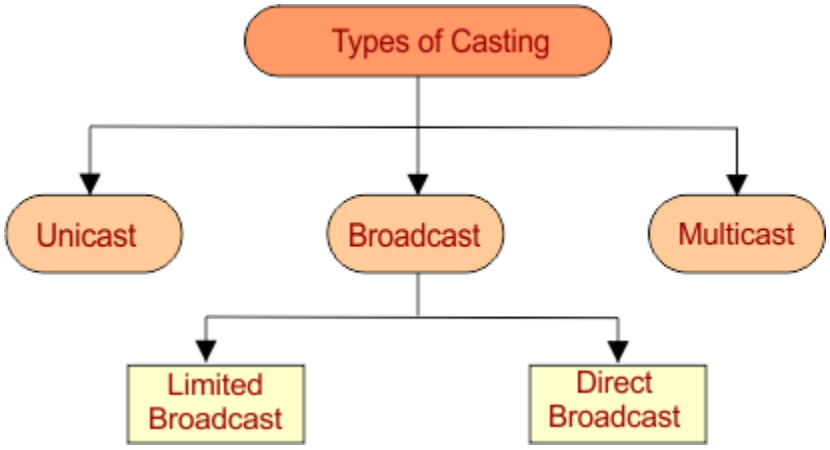
- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent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

Disadvantages Of Message Switching

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

Types of casting

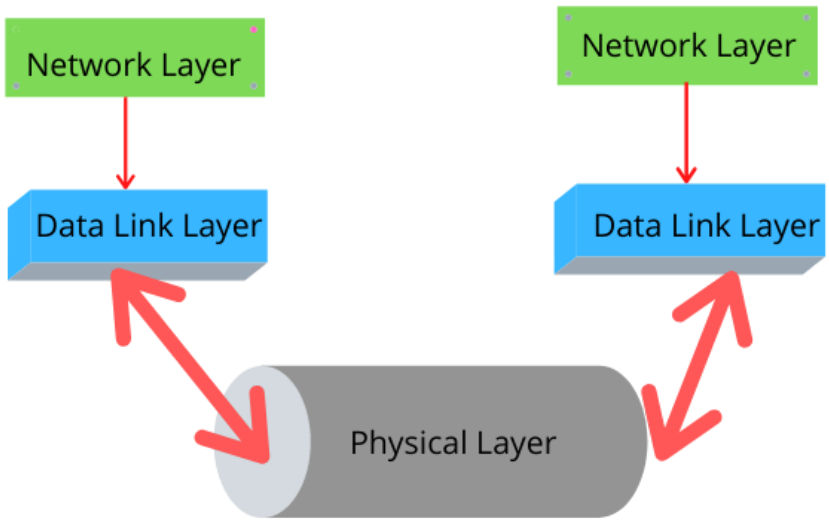
1. Unicast (one to one communication)
2. BroadCast (Limited and direct broadcast)
3. Multicast (group me message karna)



Data Link Layer (hop to hop)

Jan 29, 2022

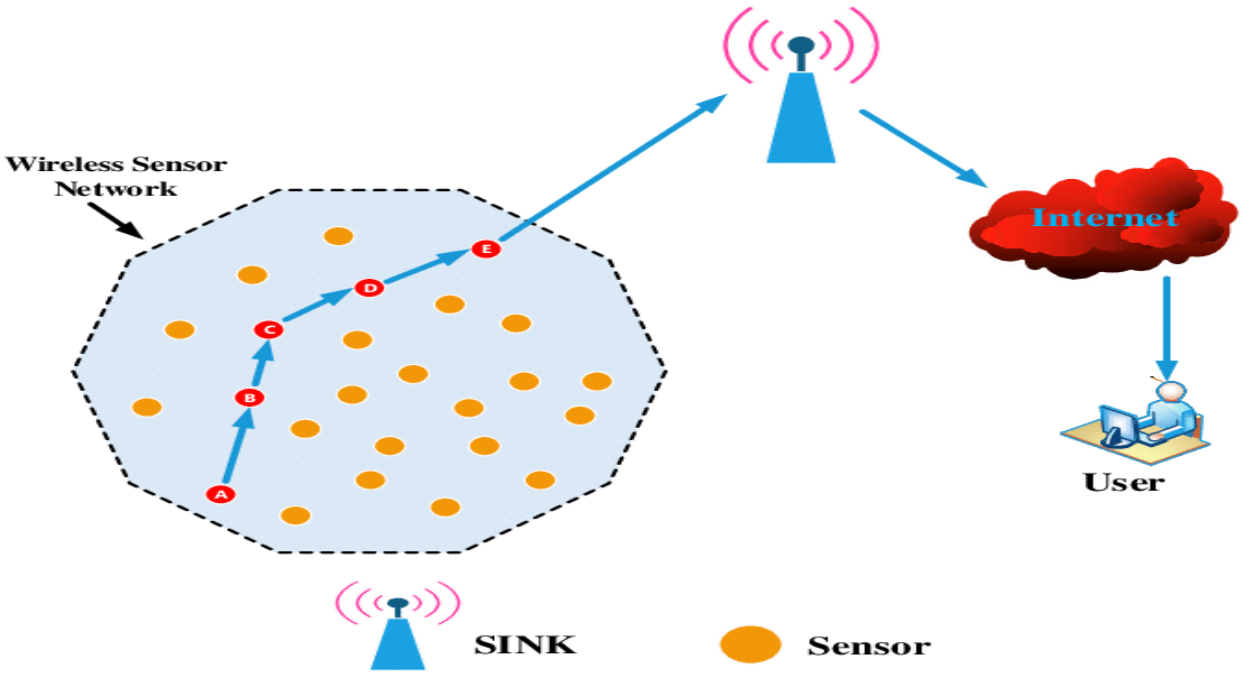
Data Link Layer In OSI Model

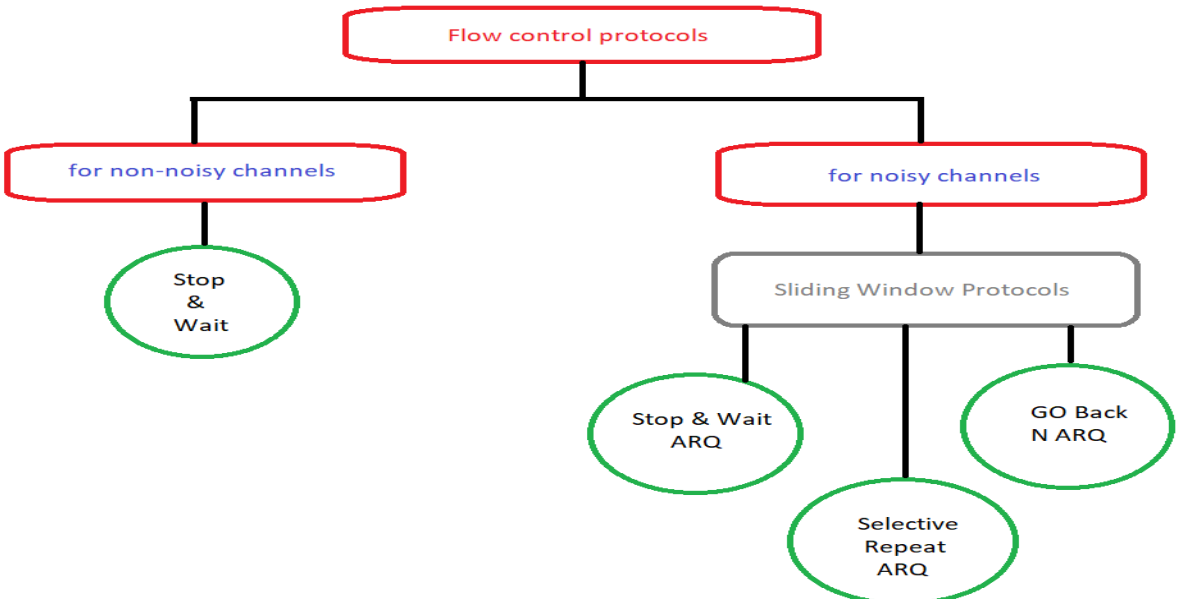


1. **Data link layer work within the network**
2. **Hop to hop delivery (node to node delivery)**
3. **Flow control**
   Flow control ke 3 protocol
   a. Stop and wait
   b. Go back N
   c. Selective repeat
4. **Error control (hop to hop error control)**
   1. CRC(iska use data link layer me karte hain)
   2. Checksum(iska use transport layer me karte hain)
   3. Parity
5. **Access control**
   1. (CSMA/CD)(ethernet)
   2 . ALuma
   3. Token ring ya phir bas
6. **Physical Address (MAC address)**
   Intranetwork communication me MAC address use hota hai but internetwork communication me MAC address use nahi hota .

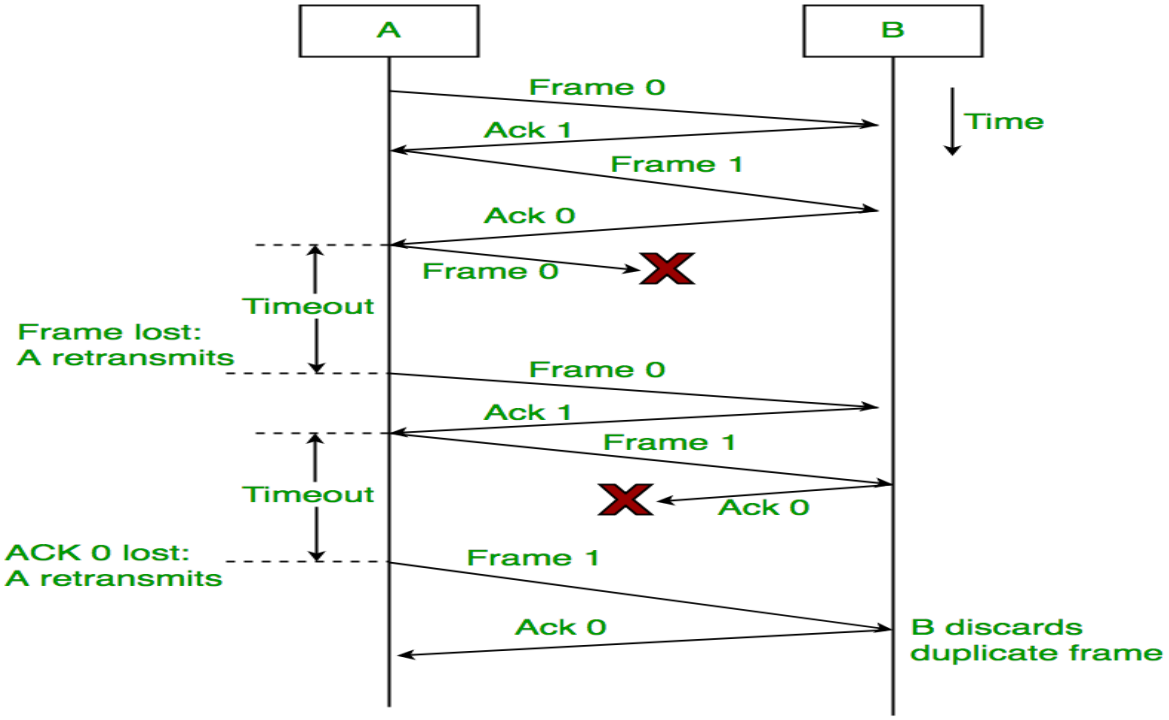
- Data link ka kaam ye hota hai hi jo packets aaya through network layer use frame me change karna and head and tail add karna dega.

Hop to Hop Example



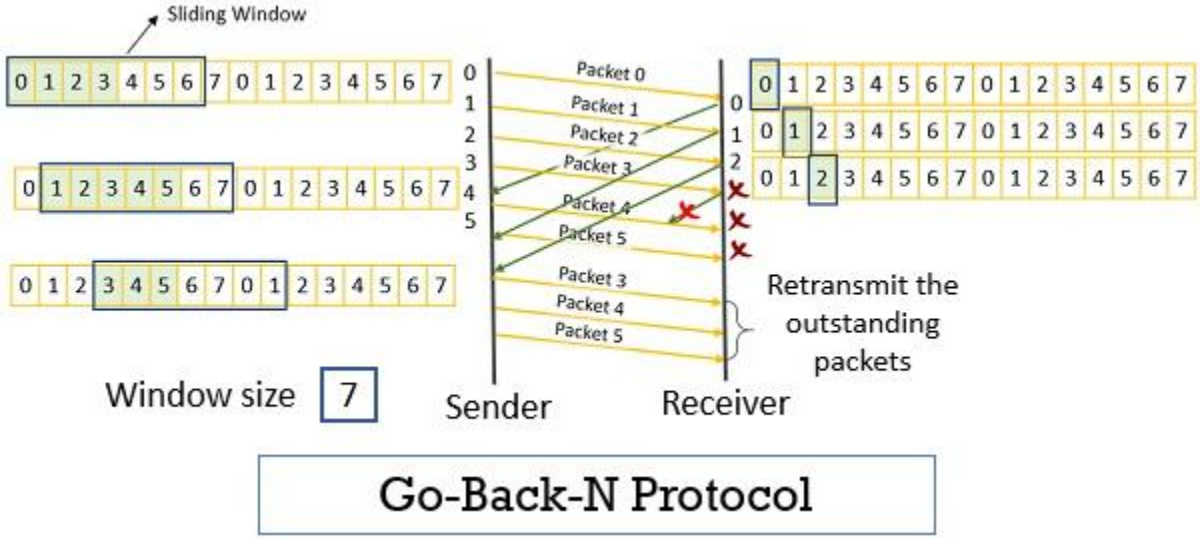


Stop and wait Protocol



Issme Sender ka size 1 and receiver ka size v 1 hota hai

Go-Back-N ARQ

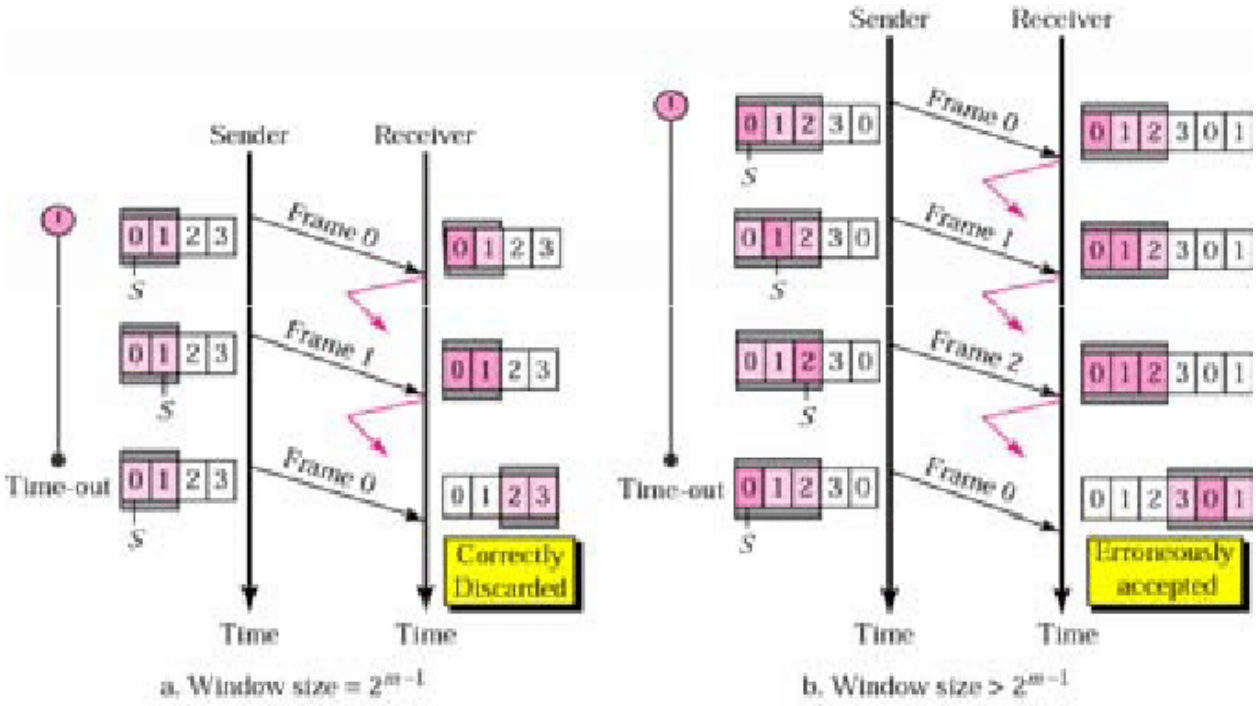


Isme Window Sender Size = 2^m-1

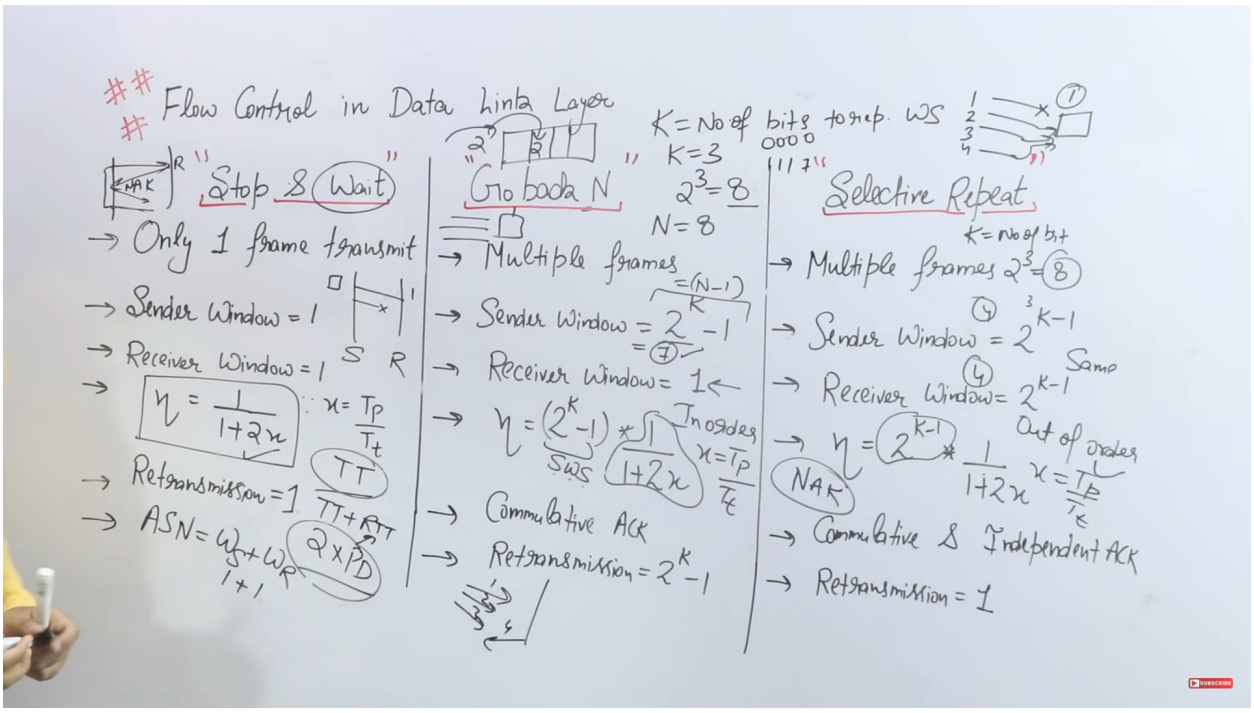
Window Receiver size= 1

Where m= Sequence No

Selective Repeat ARQ



Sender size= 2^(m-1)
Receiver size= 2^(m-1)



Framing in Data Link Layer

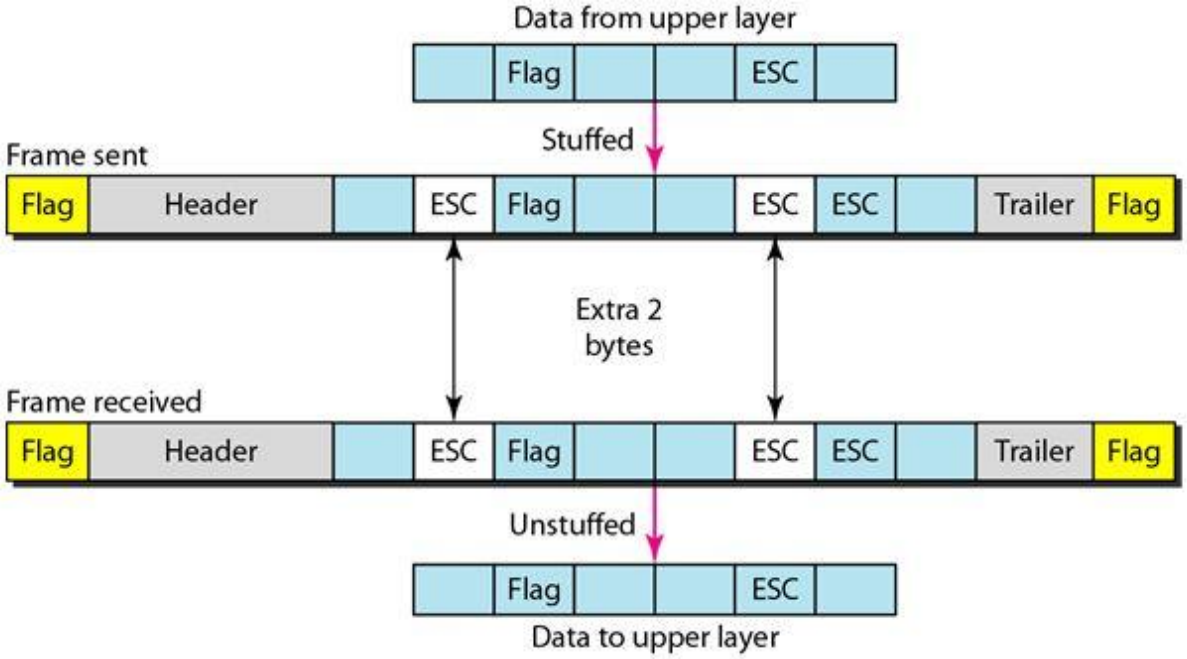
The data link layer needs to pack bits into Frames, so that each frame is distinguishable from another . Our postal system practices a type of framing . The simple act of inserting a letter into an envelope separates one piece of information from another , the envelope serves as the delimiter .

Types of framing

1. **Fixed-size Framing**
2. **Variable-size framing**

A frame in a character-oriented protocol

Byte stuffing is the process of adding 1 extra byte whenever there is a flag or escape character in the text .



Error Detection and Correction

Types of error

1. Single bit error
2. Burst error

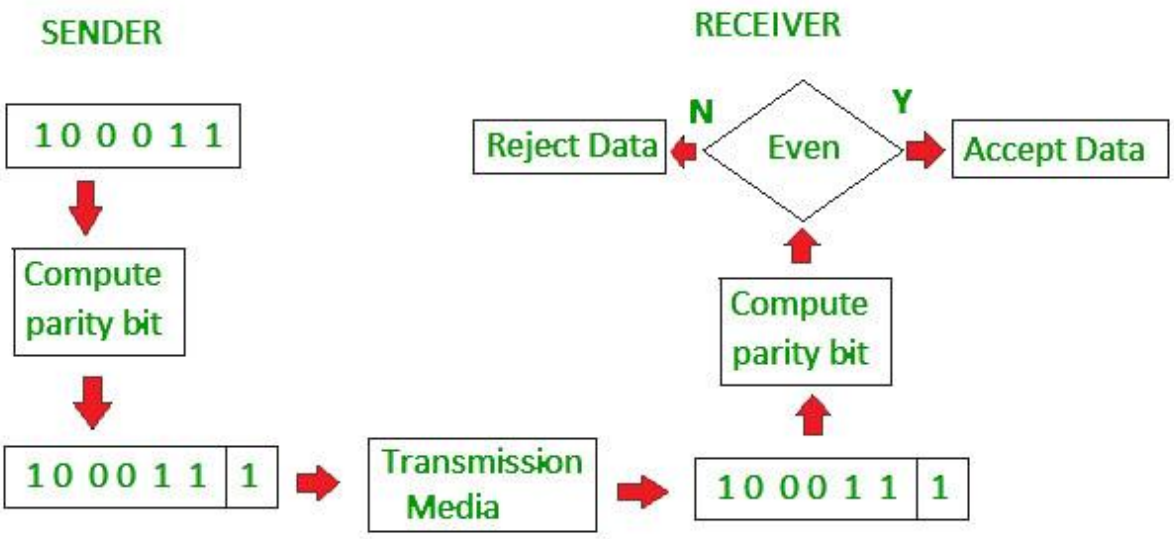
Detection

1. Simple parity (even ,Odd)
2. 2 D parity Check
3. Check Sum
4. CRC (cyclic Redundancy Check) (data link layer use)

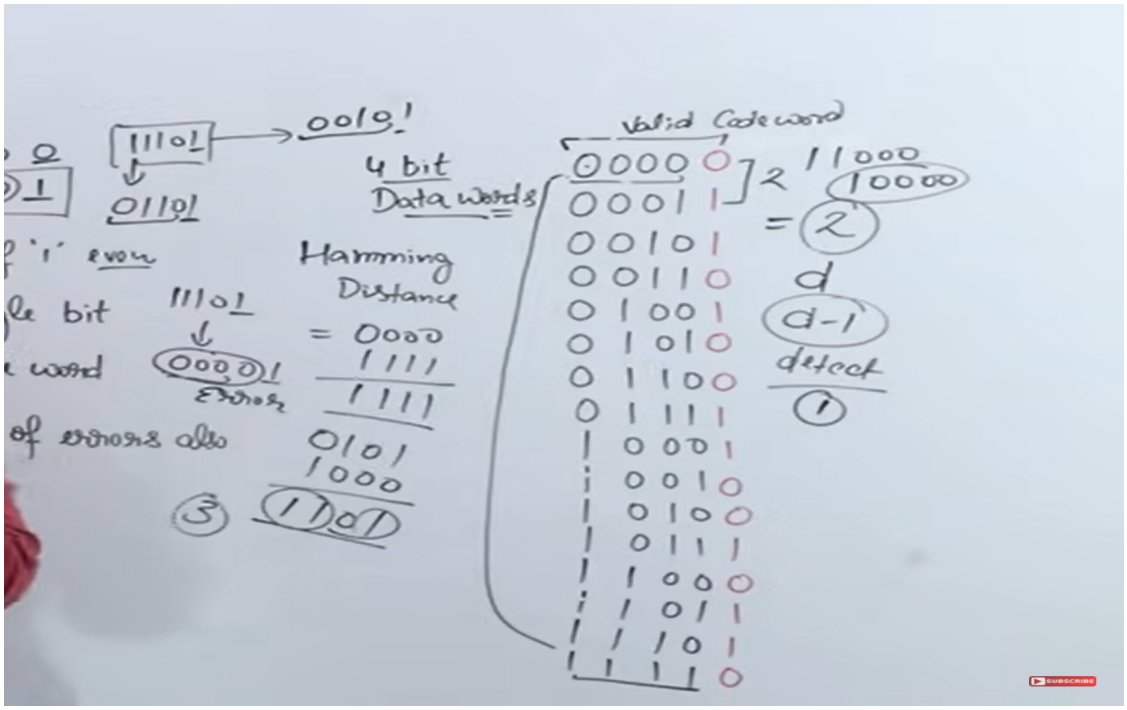
Correction

Hamming codes

Single Parity bit



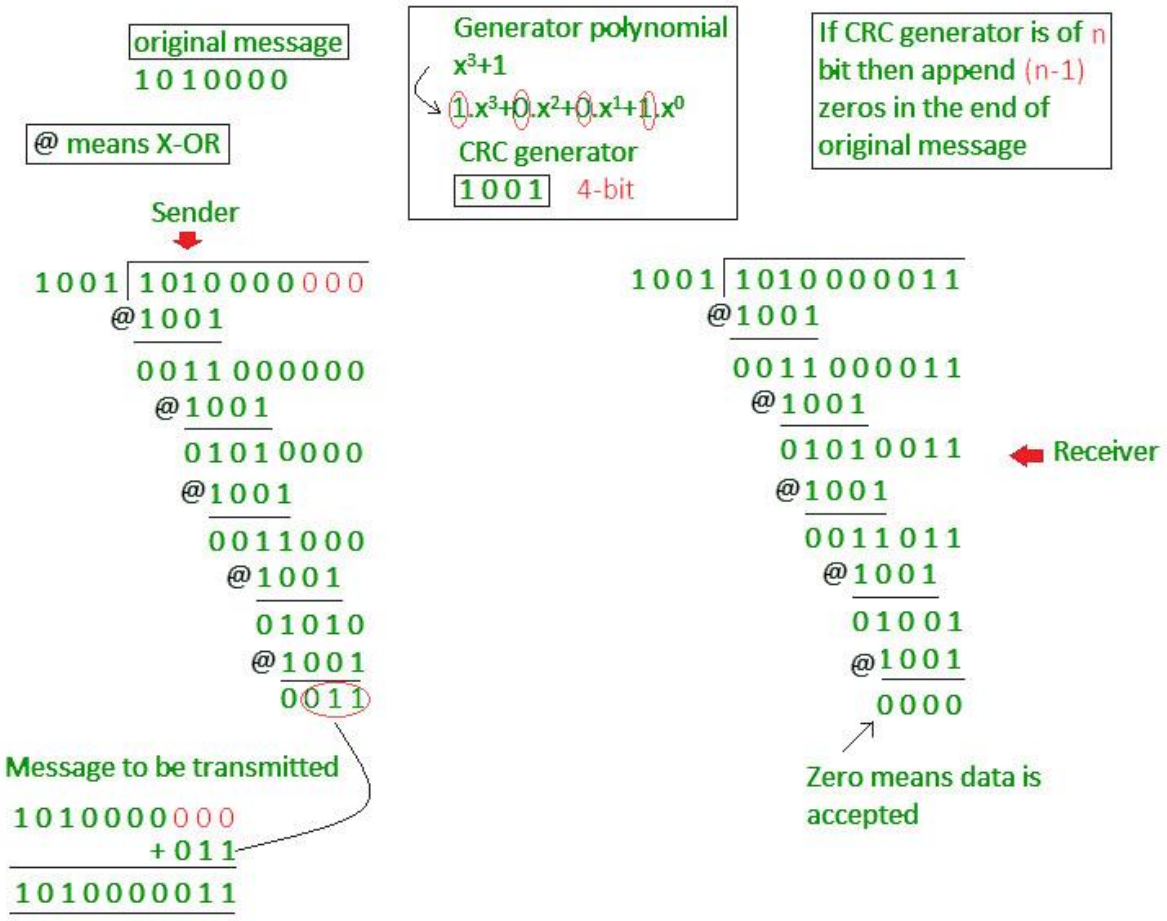
1. **M+1 bits (M= message bits)**
2. **Even Parity**
3. **Can detect all single bit errors in code word**
4. **Can detect all odd no of errors also**



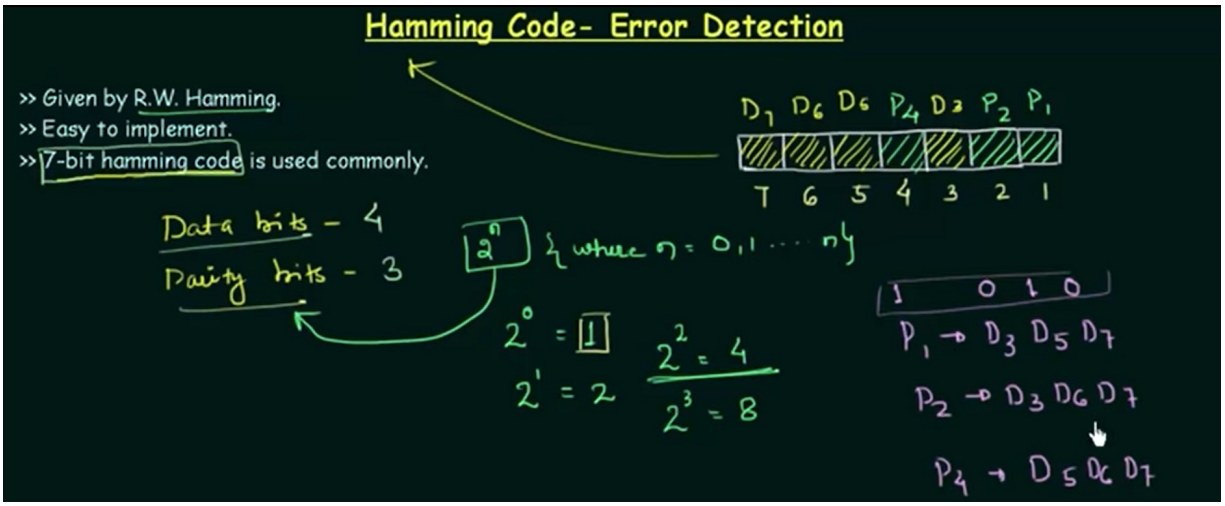
d= minimum Hamming distance
Hamming distance between two bits is xor of both and no of ones
And red baala parity bit hai and d-1 bit tak detect kar sakta hai

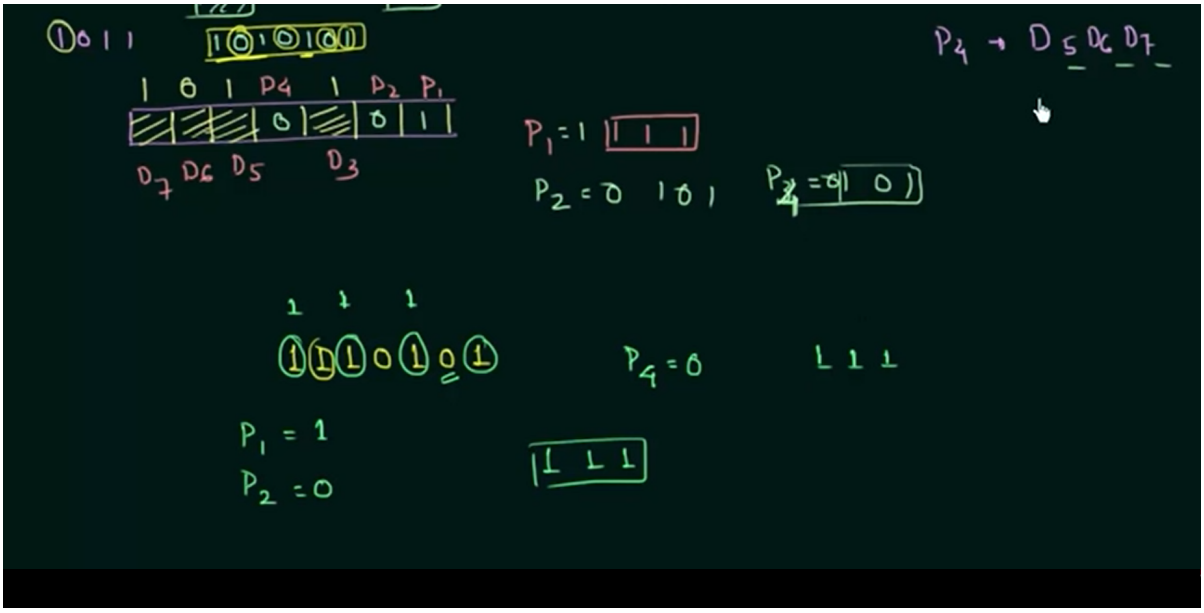
Cyclic Redundancy Check(CRC)

→ Based on binary division
Total bits=(m+r)
→ polynomial should not be divisible by x
→ also not with (x+1)
→can detect all odd errors , single bit, burst error of length equal to polynomial degree



Hamming code for error detection and Correction



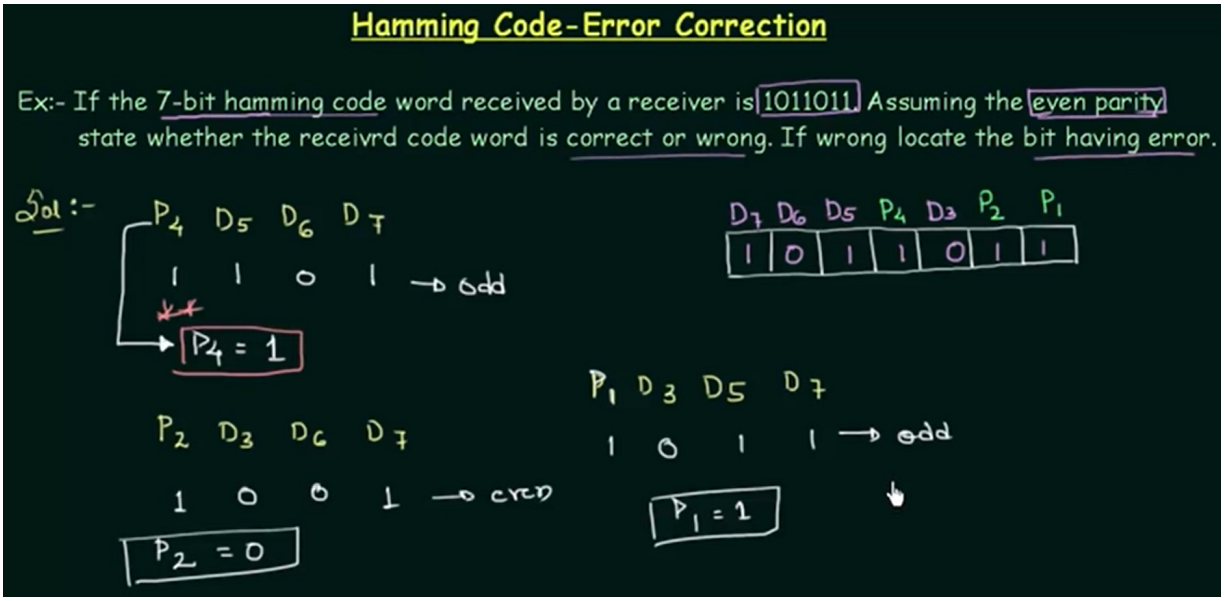


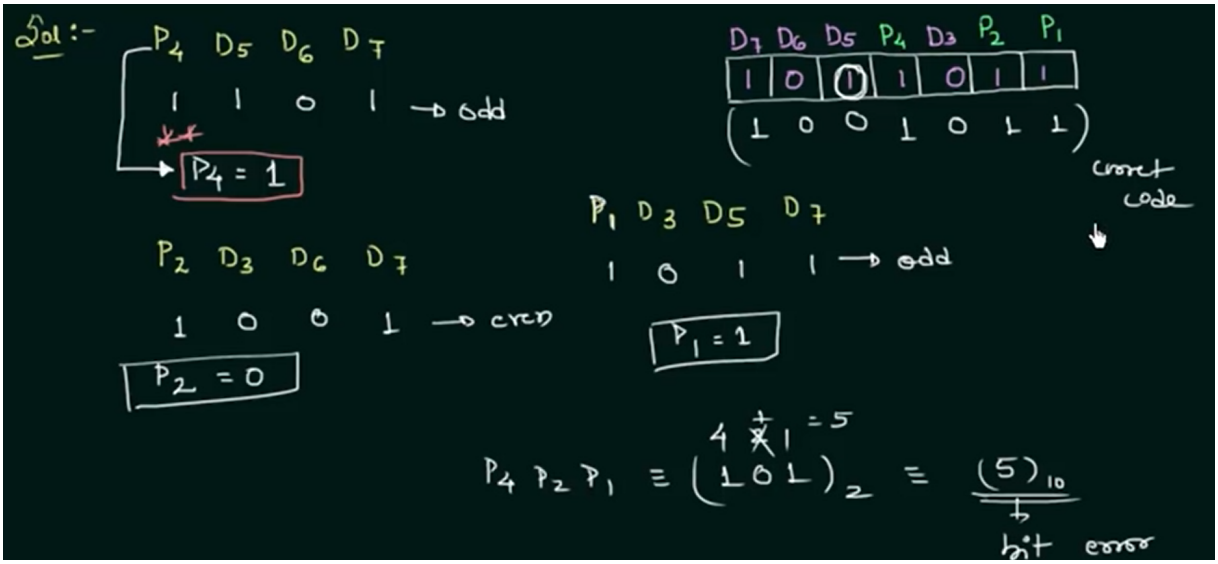
Parity Bit

1→ 3, 5,7

2→3,6,7

4→5 ,6 ,7

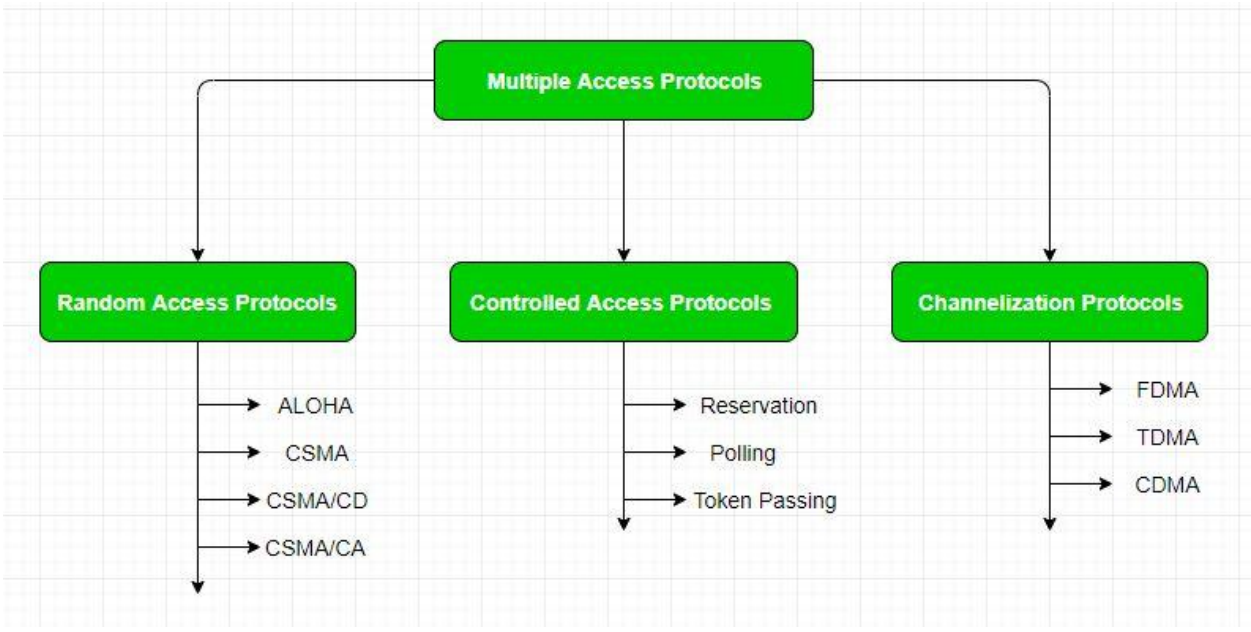




LLC = Logical Link Control

DATA LINK ke 2 layer = (LLC and MAC) ;

Multiple Access Protocol (MAC)

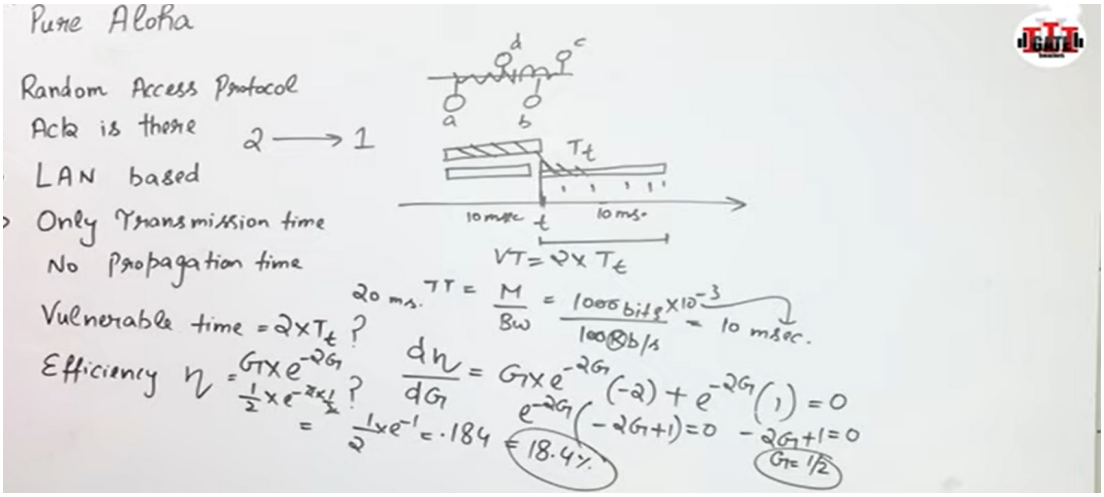


FDMA= frequency division multiple Access
TDMA= Time division multiple Access;

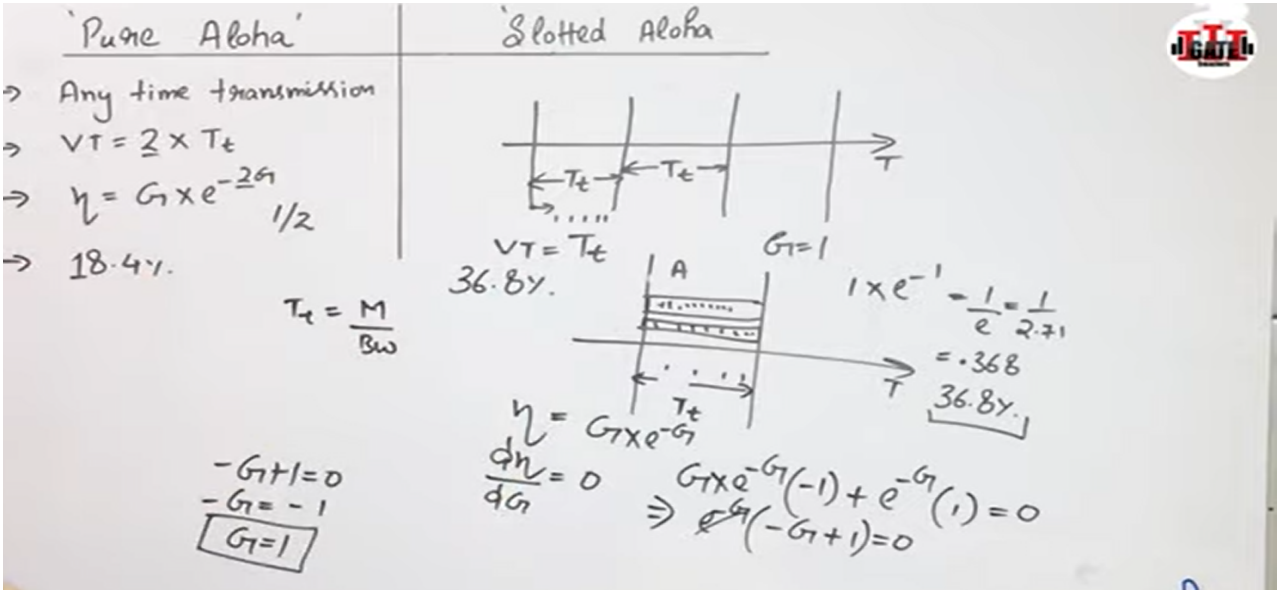
Pure Aloha

1. Random Access Protocol (like bus topology)

2. Ack is there
3. LAN based
4. Only Transmission time , no propagation time
5. Vulnerable time = 2*Tt(transmission time)
6. Efficiency n= G*e^(-2G)
   G= no of stations

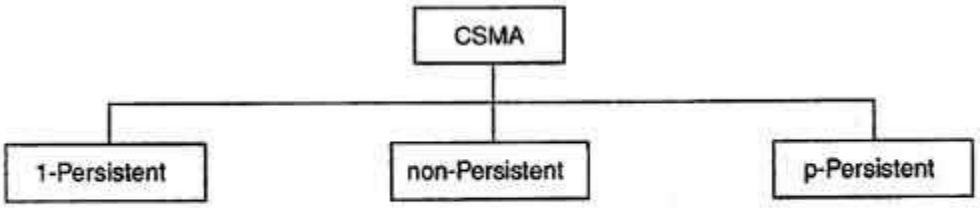


Difference between Pure aloha and Slotted Aloha

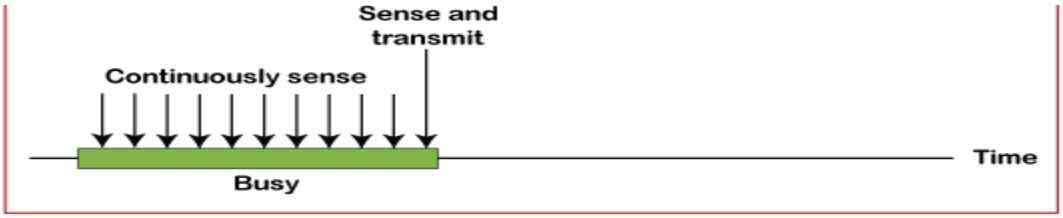


1. Agar hum 100kb data send karte hain to PURE ALOHA 18.4 kb hi data bhej payega baaki sab ka collision ho jayega
2. If we use Slotted Aloha then 36.8kb hi ja paayega out of 100 kb because of efficiency reasons .

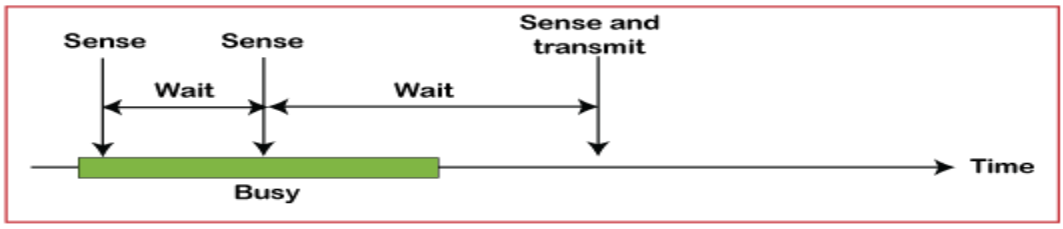
Carrier-Sensor Multiple Access (CSMA)



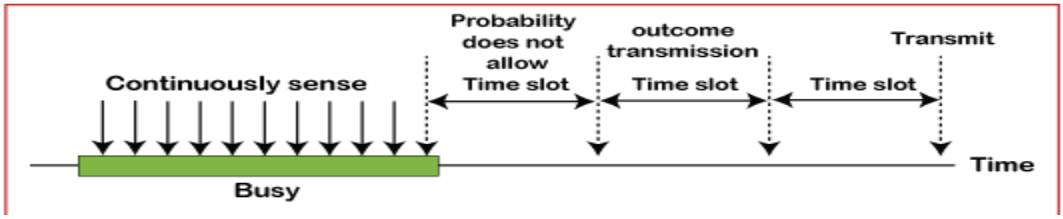
Types of CSMA



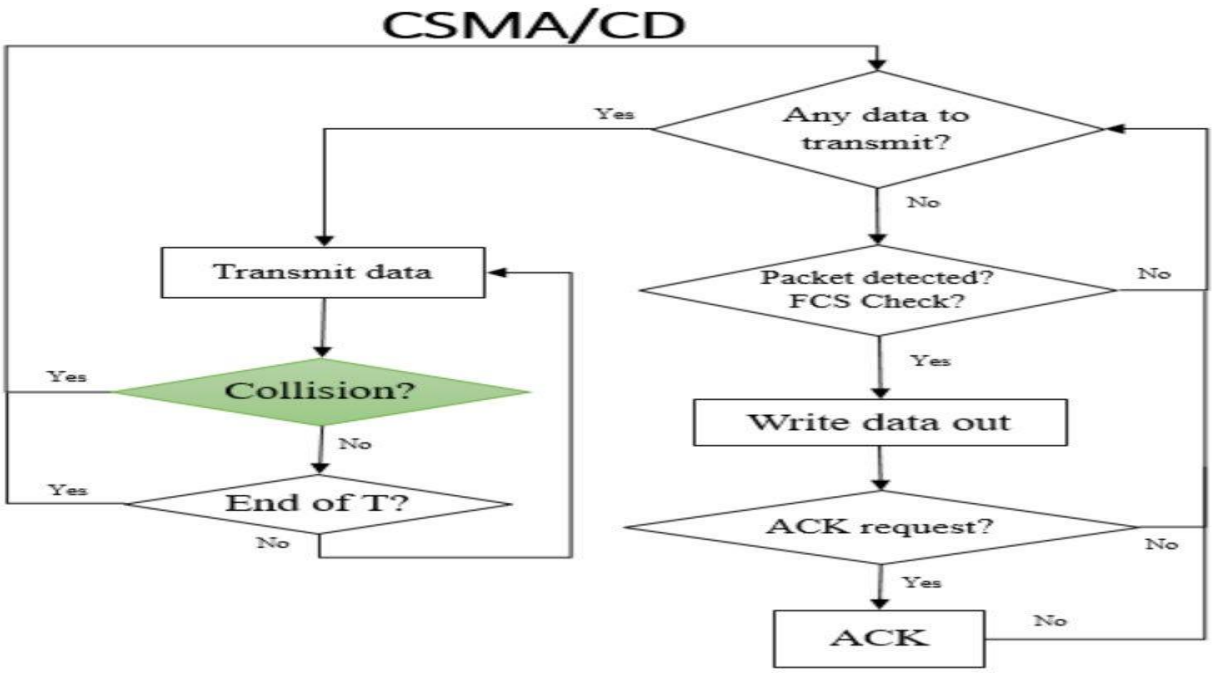
a. 1-persistent



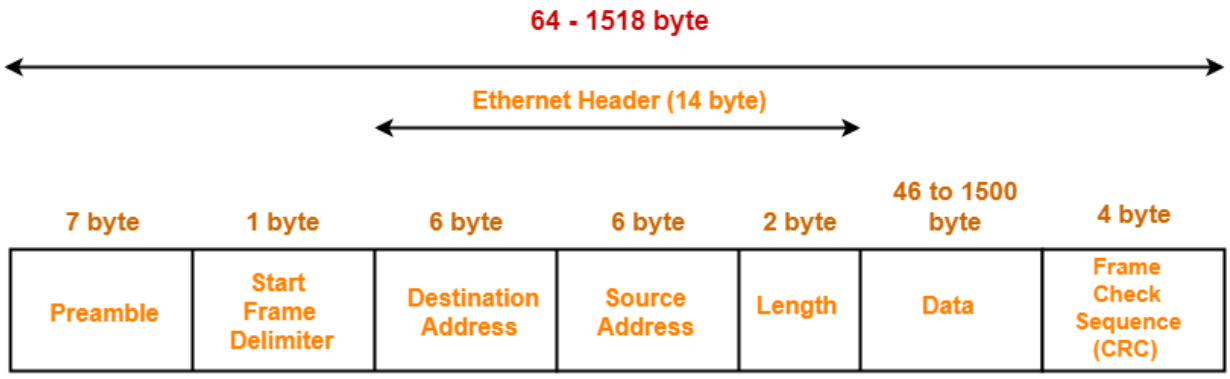
b. Nonpersistent



CSMA/CD



CSMA/CA



IEEE 802.3 Ethernet Frame Format

Token Ring

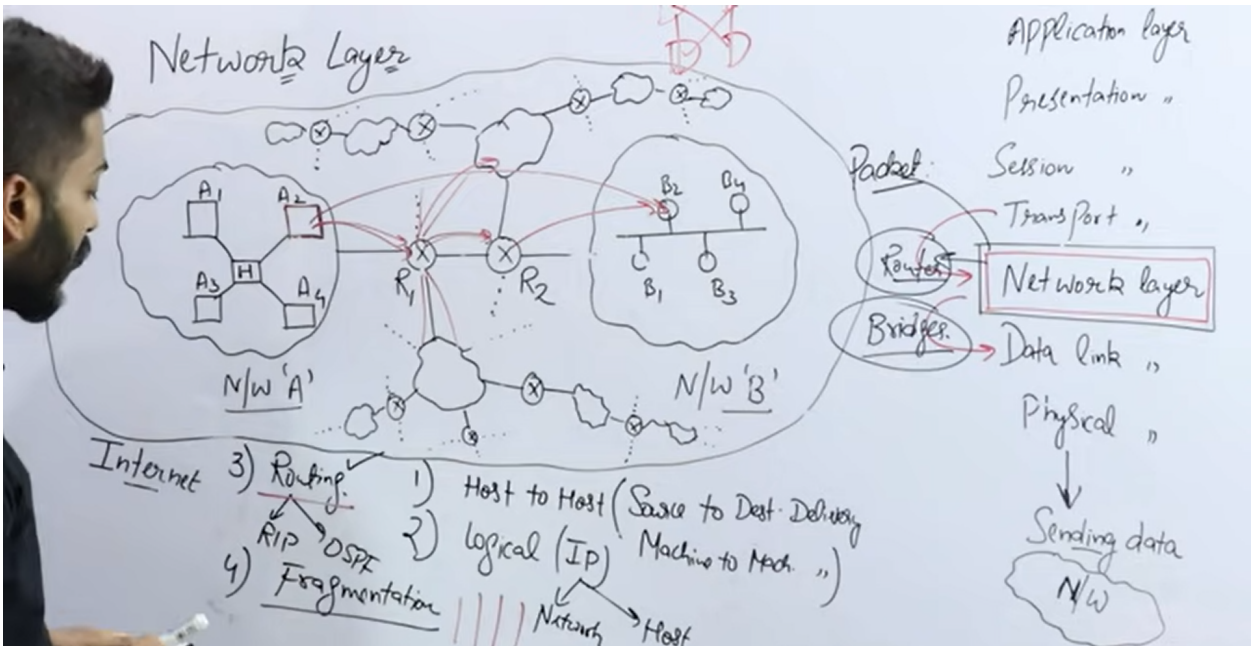
- *Ring Topology is used*
- *Access control method used is token passing.*

- *Token ring is unidirectional*
- *Data Rate used is 4Mbps & 16Mbps.*
- *Piggybacking acknowledgement is used.*
- *Differential Manchester encoding is used*
- *Variable size framing*
- *Monitor station is used.*

What is congestion?

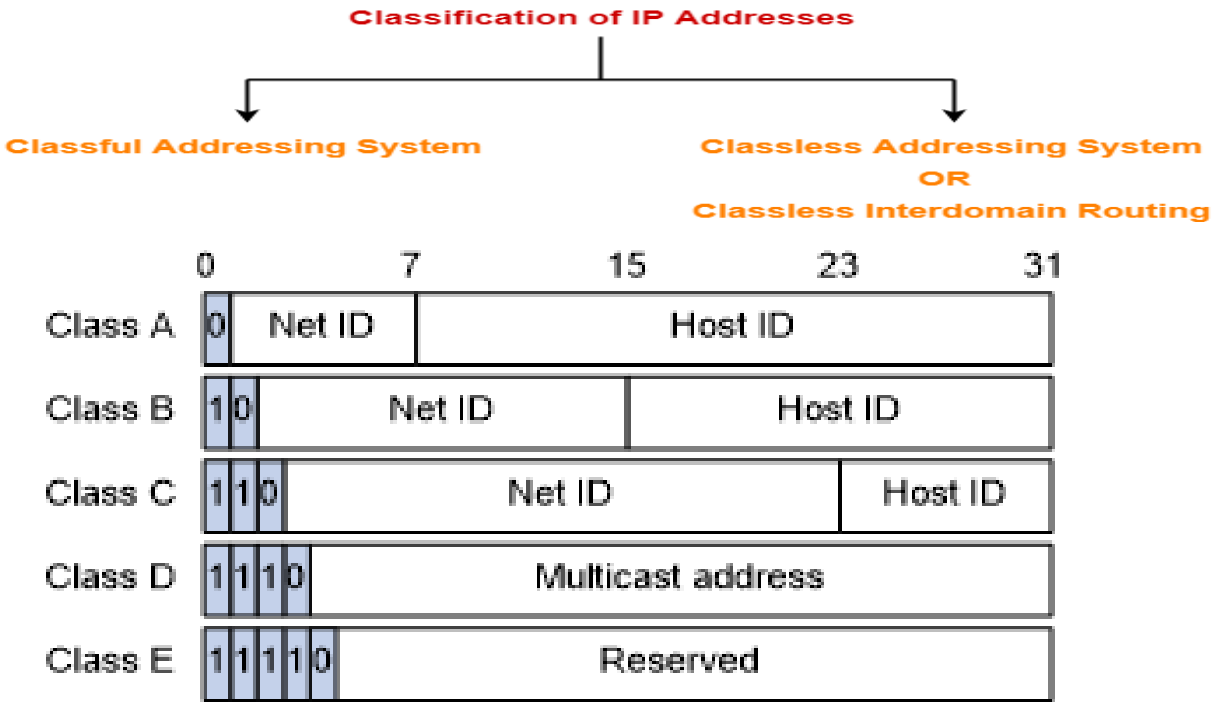
A state occurs in the network layer when the message traffic is so heavy that it slows down network response time.

Network layer (source to destination)



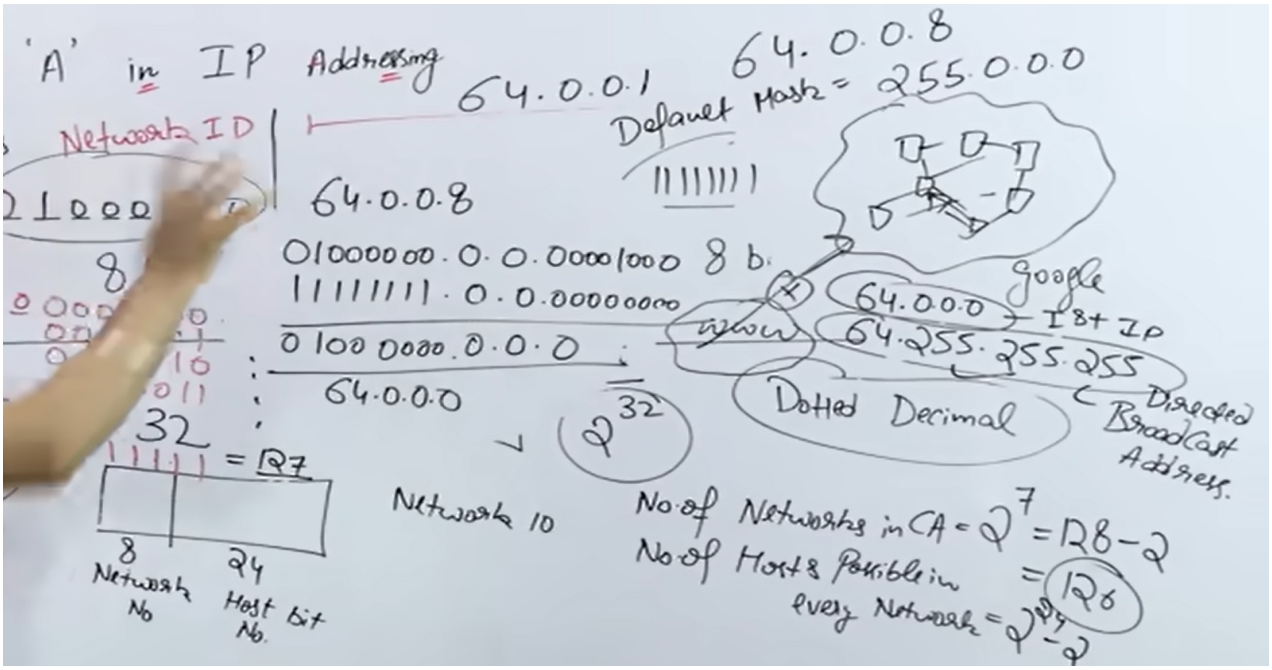
Bhejne ke liye shortest path lega

Class A in IP addressing



Class	*IP address range (1st Octet)*	*Network Mask*	*Prefix*	*Number of Networks*	*Number of Hosts*
A	1. - 127.	255.0.0.0	/8	125	16,777,214
B	128. - 191.	255.255.0.0	/16	16,382	65,534
C	192. - 223.	255.255.255.0	/24	2,097,150	254
D	224. - 239.	Multicast addresses			
E	240. - 254.	Restricted/Experimental			

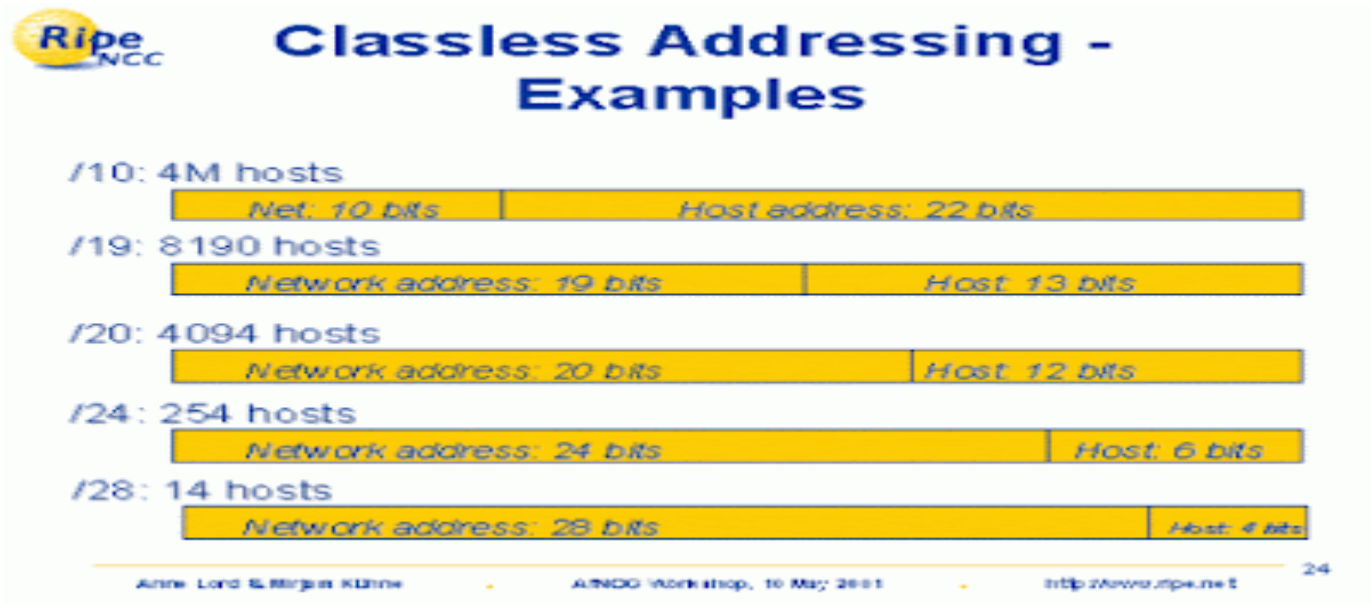
First and last reserved



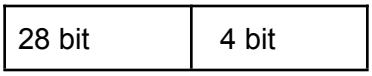
Problems with classful Addressing

- Wastage of IP addresses
- Maintenance is time consuming
- More prone to error
- Security ki problem

Classless IP addressing



- No class in this like A,B,C,D , it based on user requirement
- Only blocks



Block ID Host ID (2^4=16 IP address generate hoga)

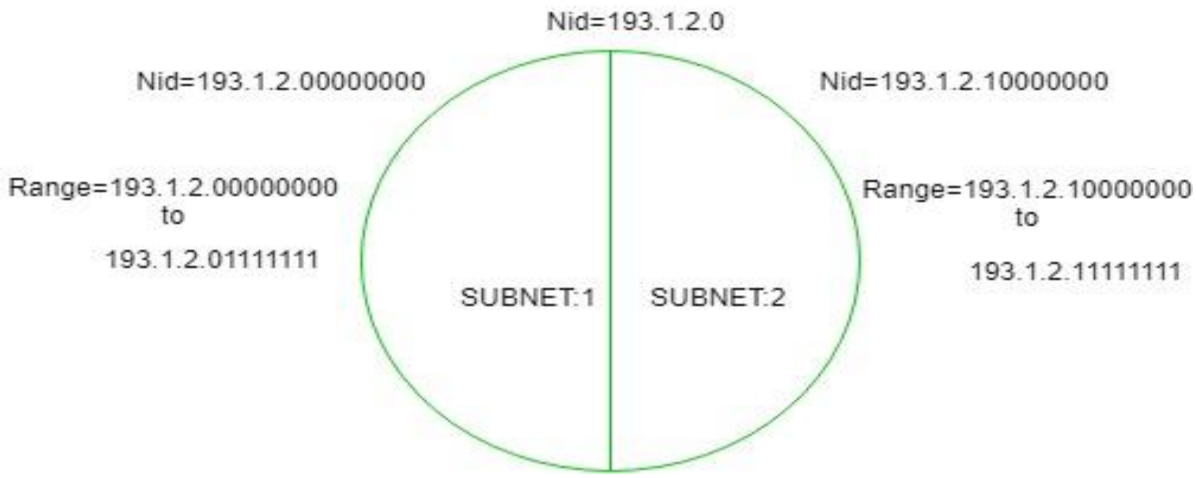
- Notation x.y.z.w/n
  Here n represents mask or no of bits represent block or network or no of 1's
  For example
  200.10.20.40/28 here
  For this IP address what will be the mask that means 28 times 1 and 4 time 0
  1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 11 1 1 1 1 .1 1 1 1 0 0 0 0
  255.255. 255. 240 = mask of this network
  For finding Network address
  First 28 bit ko chor denge as it because ye block ID hai unchangeable and last 4 bit ko 0 kar denge and calculate kar lenge then
  Here every block in 8 bit
  200.10.20.0 0 1 0 1 0 0 0 (8+8+8+8=32bit)
  200.10.20.0 0 1 0 0 0 0 0(conversion into network address by doing remaining 4 bit to 0)
  200.10.20.32/28 ⇒network id or block id
  ⇒ Another method doing this , mask of this network & IP address of the network

Subnetting

⇒Dividing the big Network into small networks

Class C me first 3 block Network Id hote hai to isme koi change nahi hoga agar hua toh problem aa jayega and only last octact ko open karna hai

First IP address subnet Id or network ID hote hain or Last waala Broadcast IP address hota hai

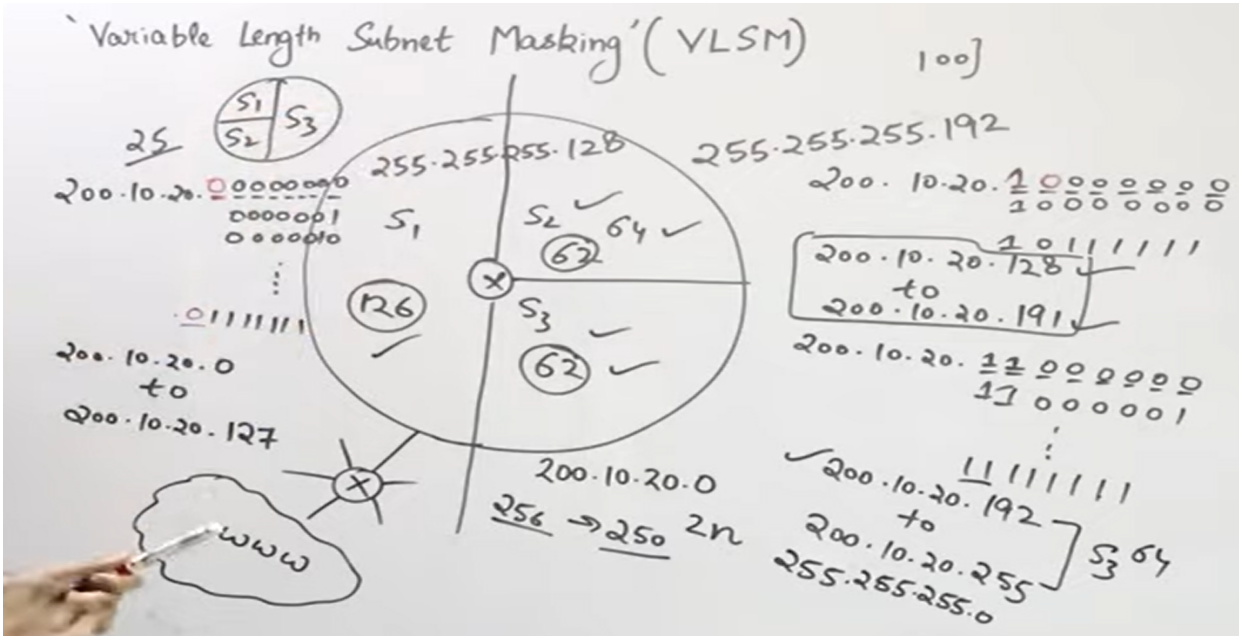


For Subnet mask , actually ye class C ka hai to class C ka subnet mask to use hoga hi
Like 255.255.255.(kitna bit ko fix kiya , 1 na) 1 0 0 0 0 0 0 0 that will be 255.255.255.128

255.255.255.128 = ye default subnet mask ho gaya
Jo v destination IP address aayega uska humlog default subnet mask ke sath and lenge and range ke according usko subnet 1 or subnet 2 me bhej denge

Variable length Subnet masking(VLS)

⇒ To make different size of subnet matlab according to our requirement



Subnetting in classless Interdomain Routing

For example

195.10.20.128/26 matlab issme (26 bit network id or remaining 6 bit host id hai)

Matlab 26 bit ko disturb nahi karna hai or remaining 6 bit ko change kar sakte hain

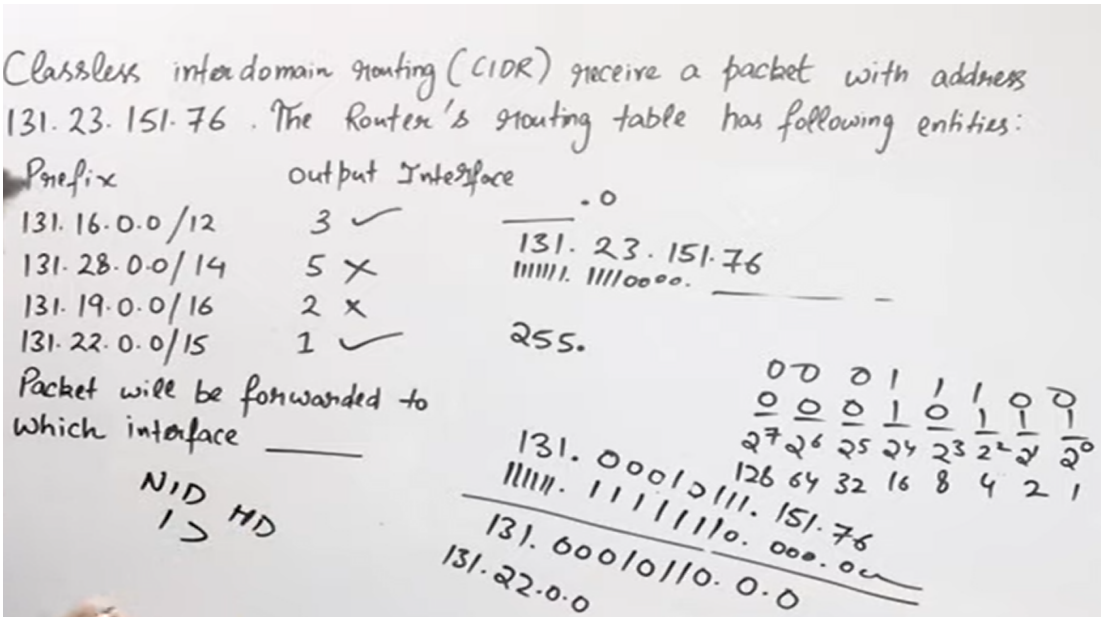
- Network id = first bit hota hai that means 26 bit ko chor sabko 0 karna padega tab to first IP address ban payega aapne subnet ka

195.10.20.1 0 0 0 0 0 0 0 (issme last 6 bit host Id ke liye hai)

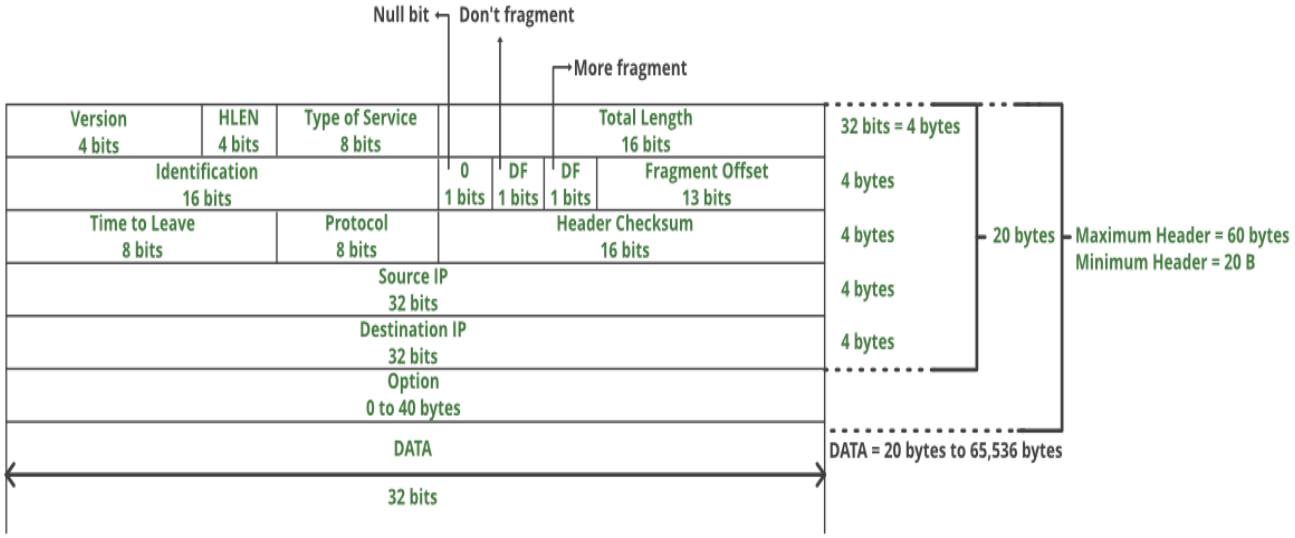
That means total 2^6=64 hots possible hai or usme se 2 use nahi karte hai 1st and last waala to baccha kitna (64-2=62)

To fix karne ke liye host id ke 1st bit ko fix karnege

Subnet 1	Subnet 2
195.10.20.1 0 **0** 0 0 0 0 0 (1 bit fix) And iska last ka address like 195.10.20.1 0 **0** 1 1 1 1 1 (128 to 159) 195.10.20.128/(26+1) because 1 bit fix kiye hain na to 195.10.20.159/(26+1) 32 addresses -2=30 usable	195.10.20.1 0 **1** 0 0 0 0 0 (1 bit fix) And iska last ka address 195.10.20.1 0 **1** 1 1 1 1 1 (160 to 191) 195.10.20.160/(26+1) because 1 bit fix kiye hain na to 195.10.20.191/(26+1) 32 addresses -2=30



IPV4 header format



VERSION: *Version of the IP protocol (4 bits), which is 4 for IPv4*

HLEN: *IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.*

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

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

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

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

Fragment Offset: *Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of the number of 8 bytes, which has the maximum value of 65,528 bytes.*

Time to live: *Datagram's lifetime (8 bits), It prevents the datagram from looping through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.*

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

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

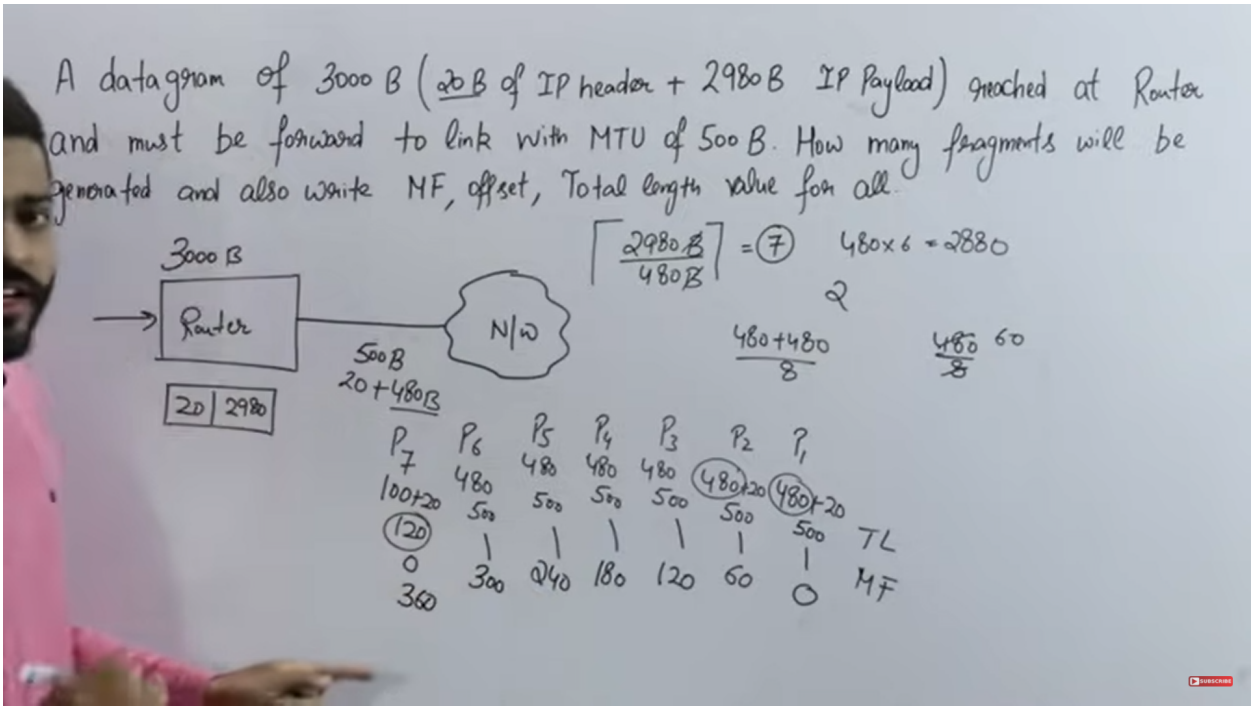
Source IP address: *32 bits IP address of the sender*

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

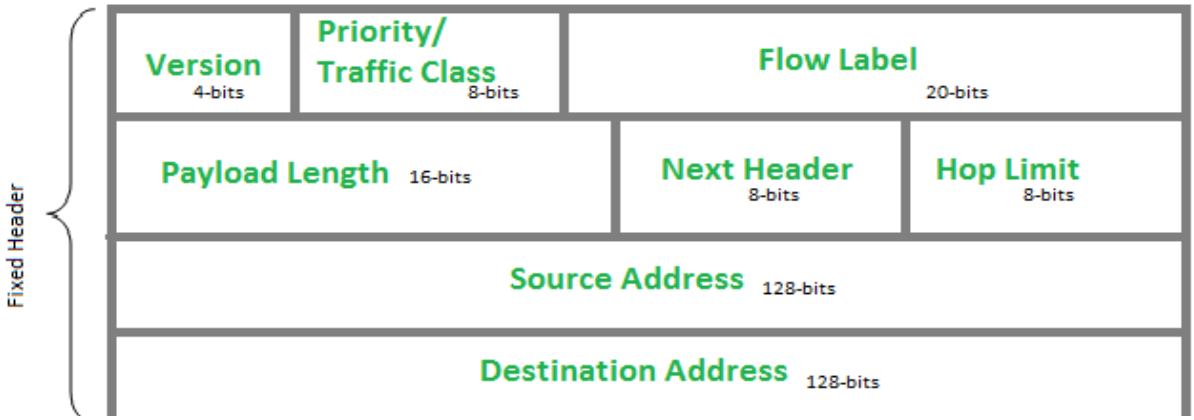
Option: *Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.*

Fragmentation in IPV4

IPv4 Datagram Fragmentation and Delays - GeeksforGeeks



IPV6 header format



- Base Headers = 40 Bytes (320 bits) fixed
- IPV4 me sirf 32 bit ka address the matlb 2^32 address possible hain
- IPV6 me 128 bit ka hota hai matlb 2^128 address possible hoga
- Version me 0110 = 6
- Next header contain Extension headers
  Extension Headers
  1. Routing Header(43) 2. Hop by hop Option (0) 3. Fragment Header (44) 4. Authentication Header (51) 5. Destination Options(60) 6. Encapsulation security payload(50)

Base Header(40B)	Extensions Header1	- - - -	Extensions Header N	Data

Difference between IpV4 and IpV6

Description	IPv4	IPv6
Address Length	32 bits	128 bits
Address representation	4 decimal numbers from 0-255 separated by periods	8 groups of 4 hexadecimal digits separated by colons
Address types	unicast, multicast, broadcast	unicast, multicast, anycast
Packet header	20 bytes long	40 bytes long, but simpler than the IPv4 packet header
Configuration	manual or through DHCP	auto-configuration of addresses is available
IPSec support	optional	Built-in

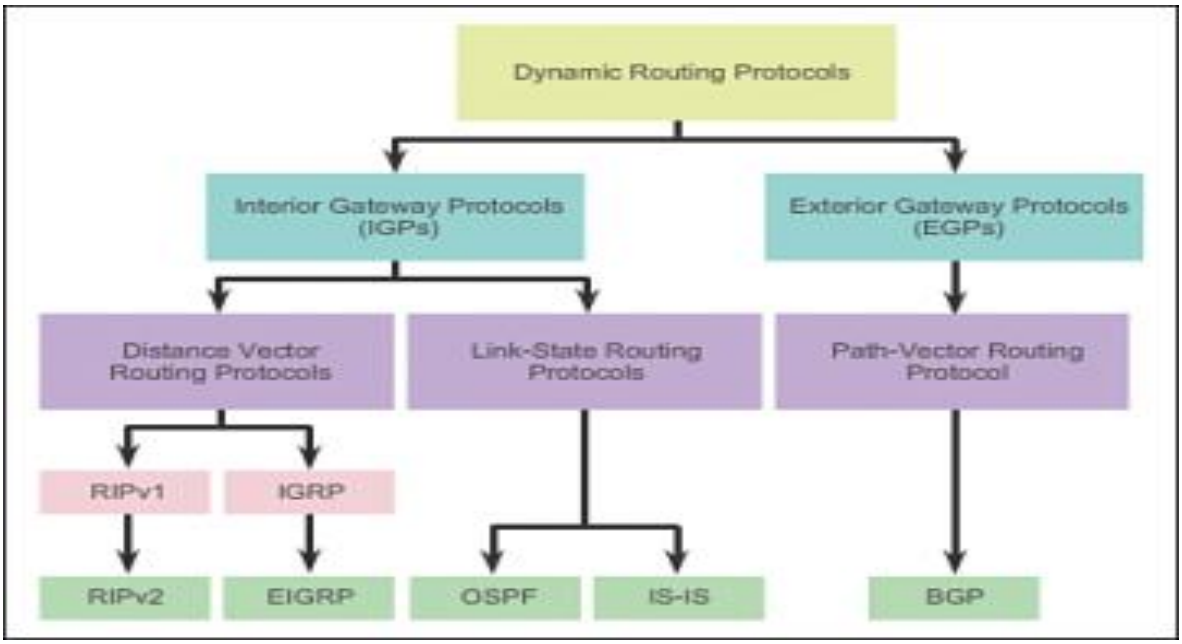
16 bit ka 8 block

[Differences between IPv4 and IPv6 - GeeksforGeeks]

Routing Protocol

Network layer ki major functionality is forwarding the packets

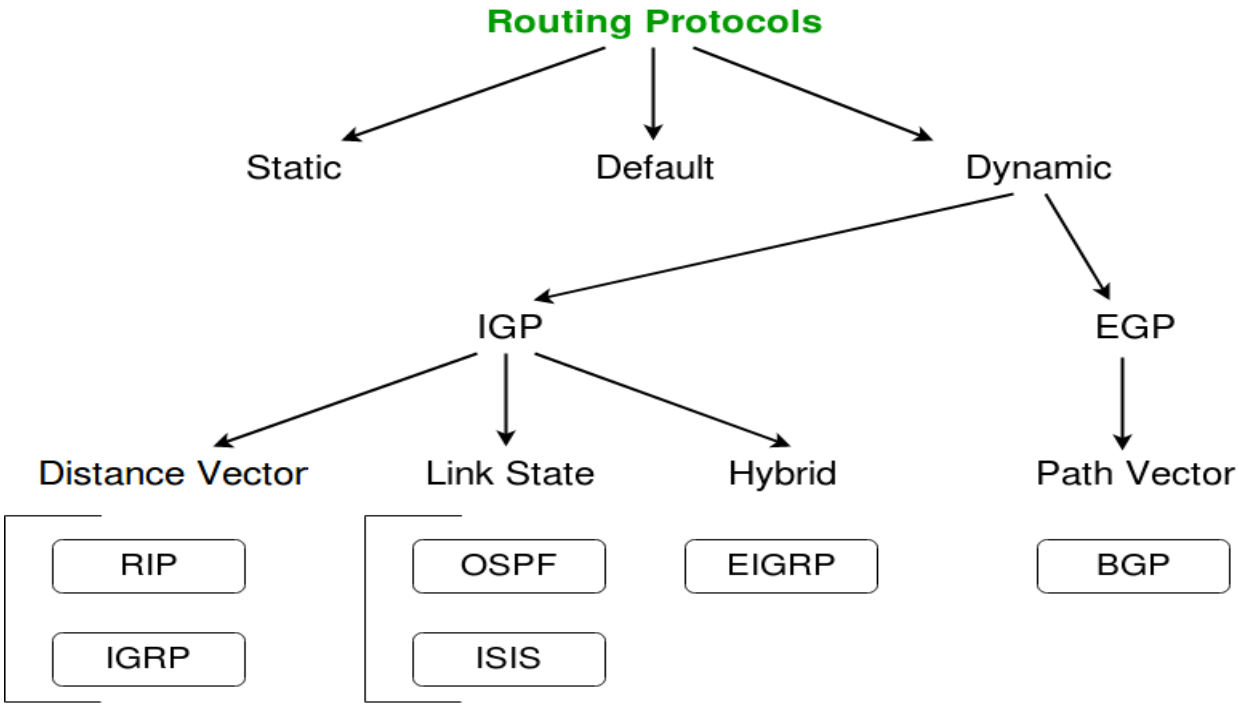
⇒A routing protocol **specifies how routers communicate with each other to distribute information that enables them to select routes between nodes on a computer network**



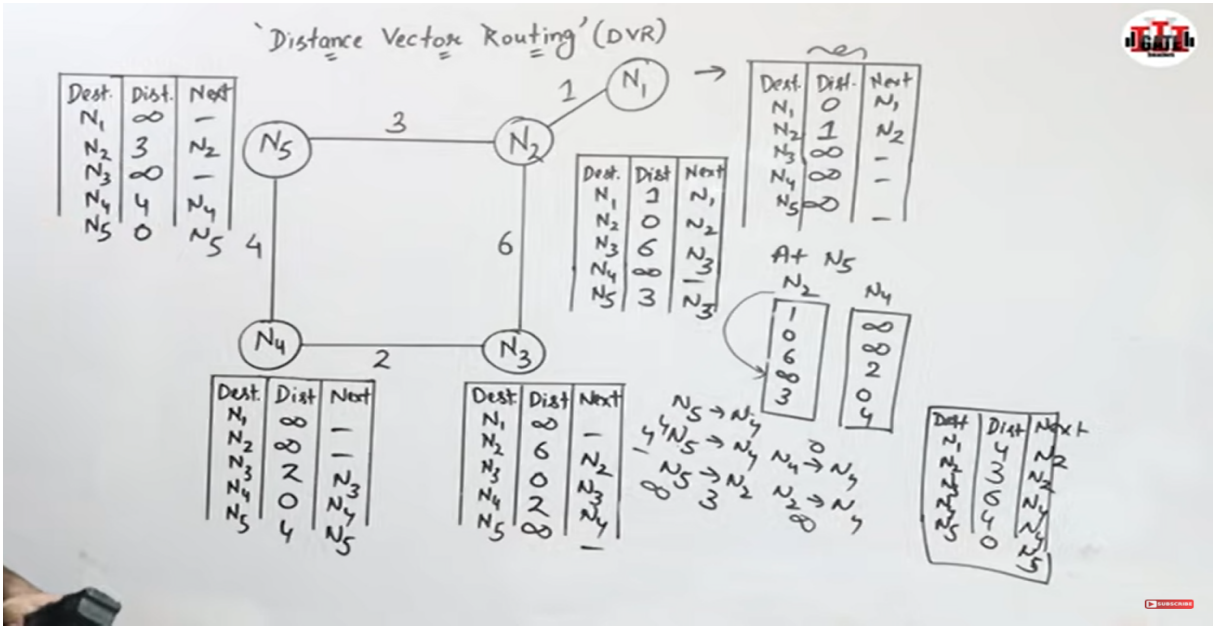
⇒ Routing table 2 types ke hote hain

1. Static Routing table
2. Dynamic Routing table (self update)

Dynamic Routing table more preferable



Distance Vector Routing Algorithm (DVR)



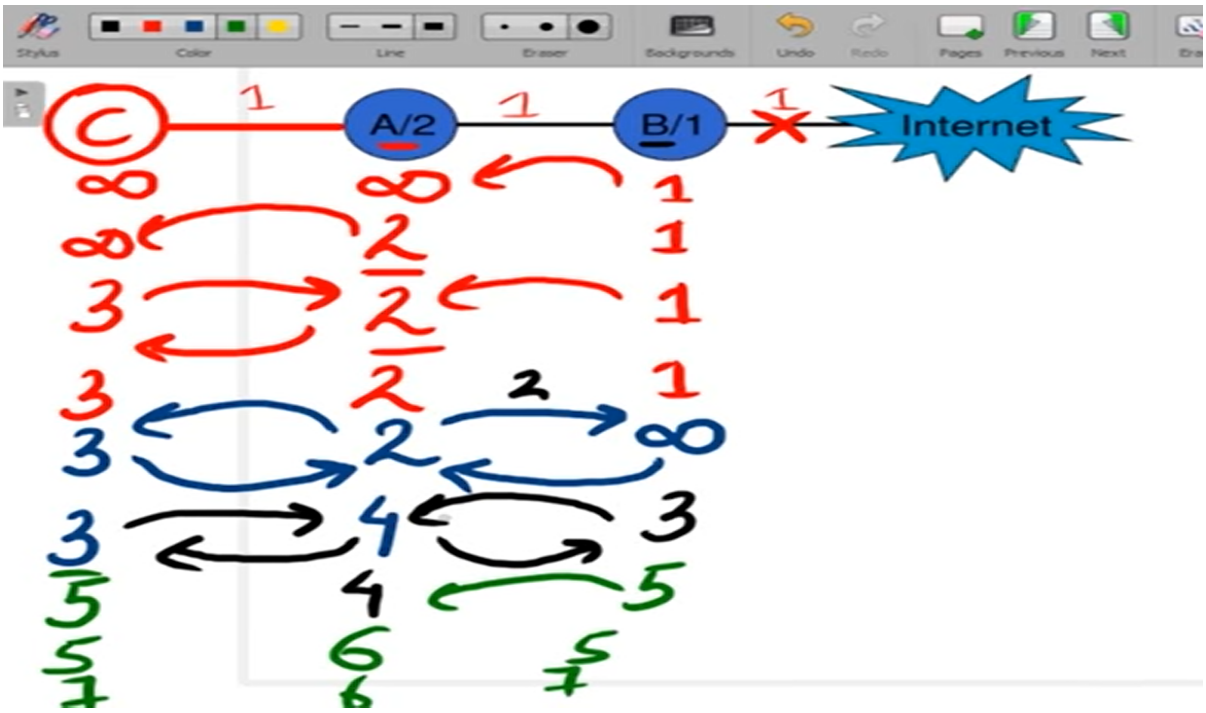
- Only Neighbors sharing
- Only Distance vector sharing
  For Example
  N2 ⇒ N1, N5,N3 ko distance vector sharing karega because of neighbors
  Agar N1 se N3 jaana hai then route will be
  N1->N2 and N2->N3 because N2 ka hi distance vector malum hai
  N1→N4 jaana hain
  N1→N2 and N2→N4
  1 + Infinity = infinity (sirf N2 ka hi distance vector use karna hai because of neighbors)

Count to infinity

Count-to-Infinity

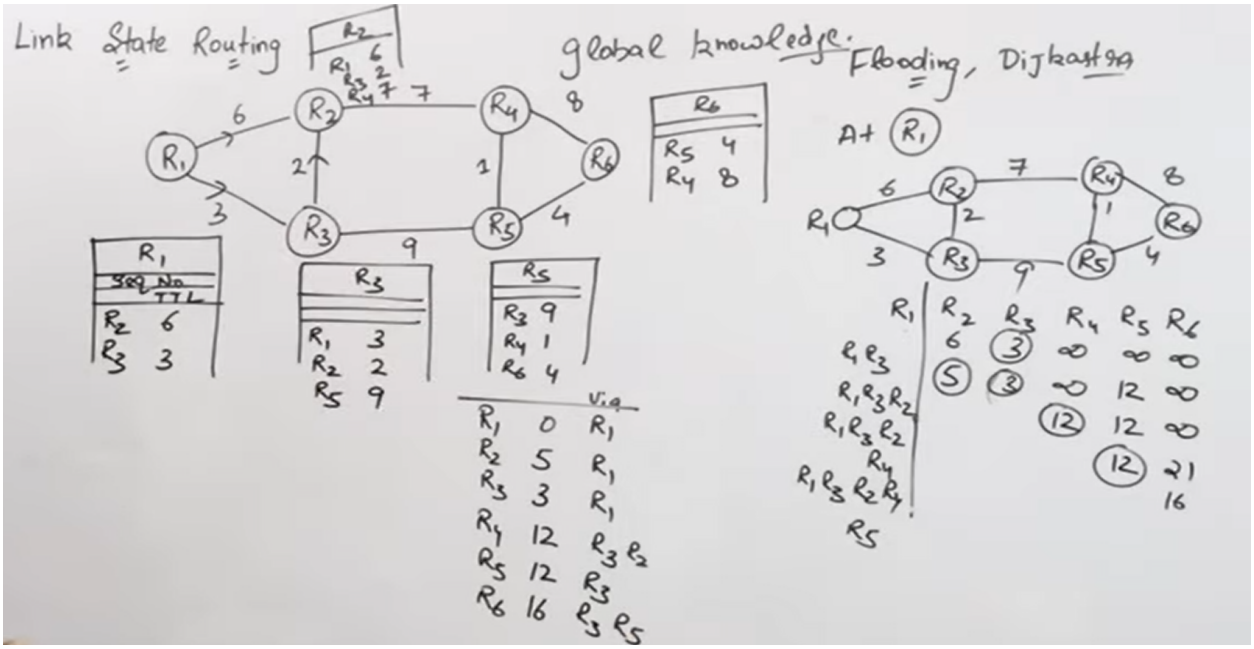
- The reason for the count-to-infinity problem is that each node only has a “next-hop-view”
- For example, in the first step, A did not realize that its route (with cost 2) to C went through node B

- How can the Count-to-Infinity problem be solved?
- **Solution 1:** Always advertise the entire path in an update message (**Path vectors**)
  - If routing tables are large, the routing messages require substantial bandwidth
  - BGP uses this solution

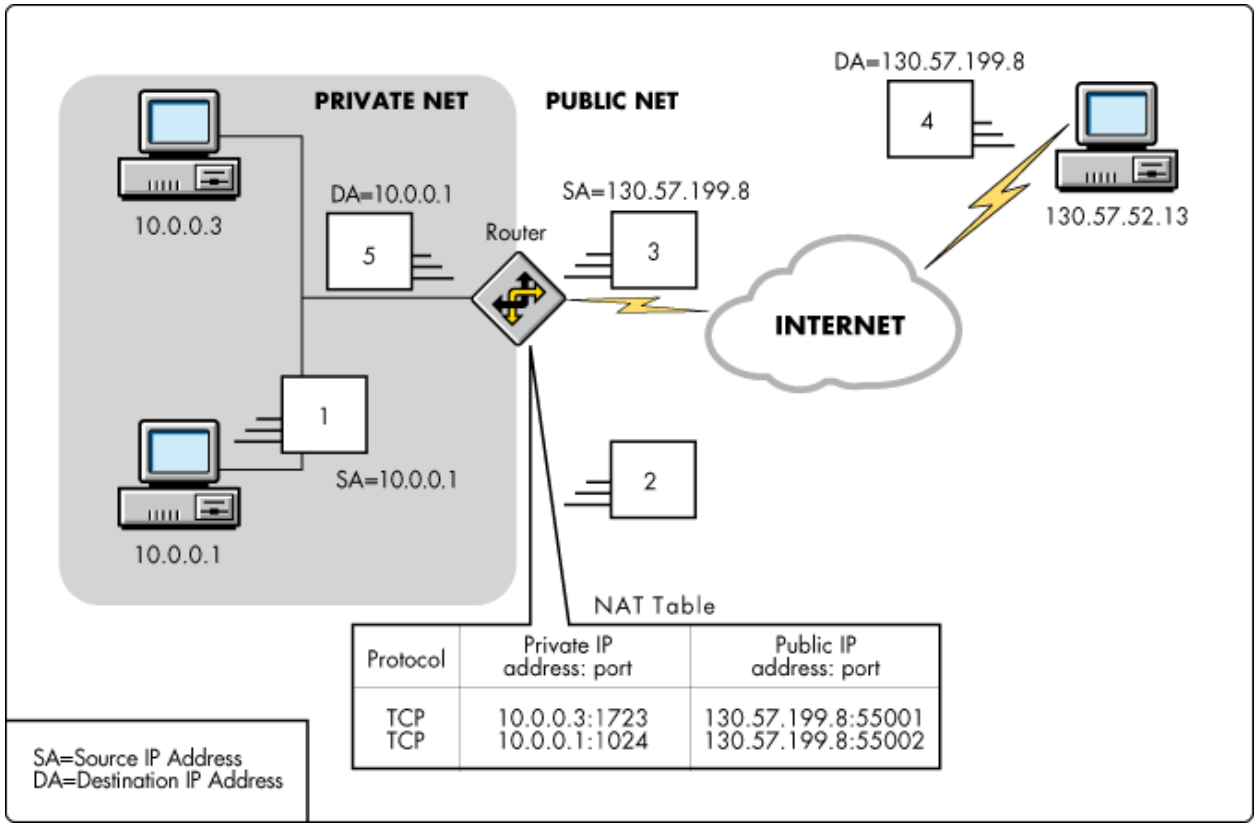


Link state routing Algorithms

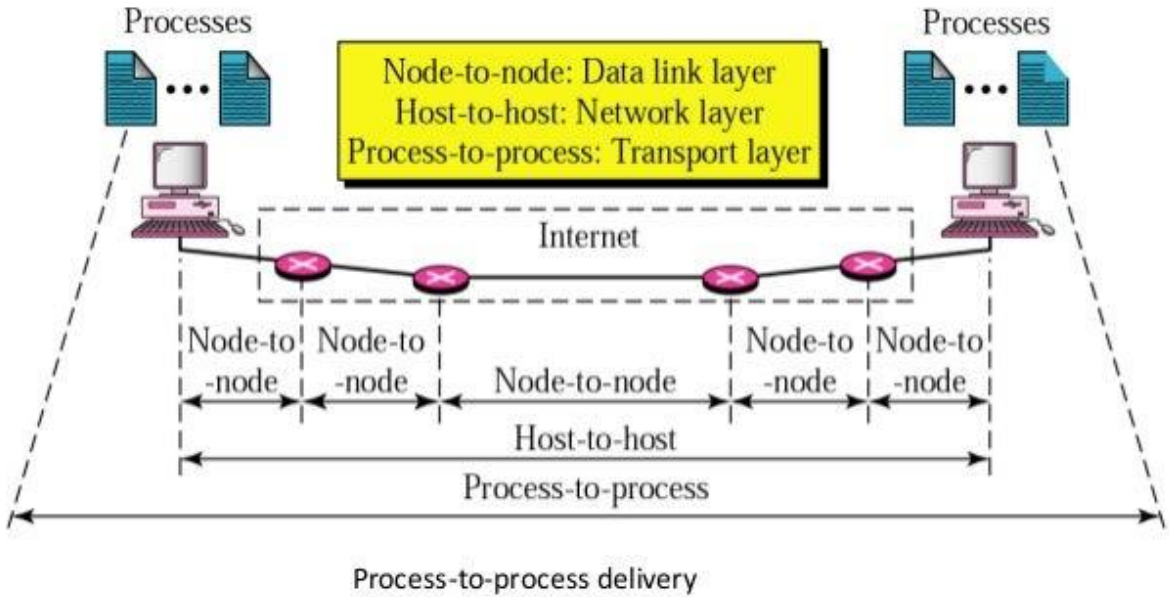
1. Each router is responsible for meeting its neighbors and learning their names.
   - Used a **Hello Protocol,** which send a data packet contains RID and address of the network on which the packet is being sent
2. Each router constructs a **LSP/LSA** which consists of a list of names and cost for each of its neighbors.
3. The **LSP/LSA** is transmitted to ***all other routers***. Each router stores the most recently generated **LSP/LSA** from each other router.
   - Link-state flooding: **Sequencing** and **Aging** procedures
   - Each routers store the identical **Link State Database**
4. Each router uses complete information on the network topology to compute the *shortest path route* to each destination node.
   - Use **SPF or Dijkstra's algorithm** to calculate the shortest path



NAT (Network addressing Translation)



Transport Layer

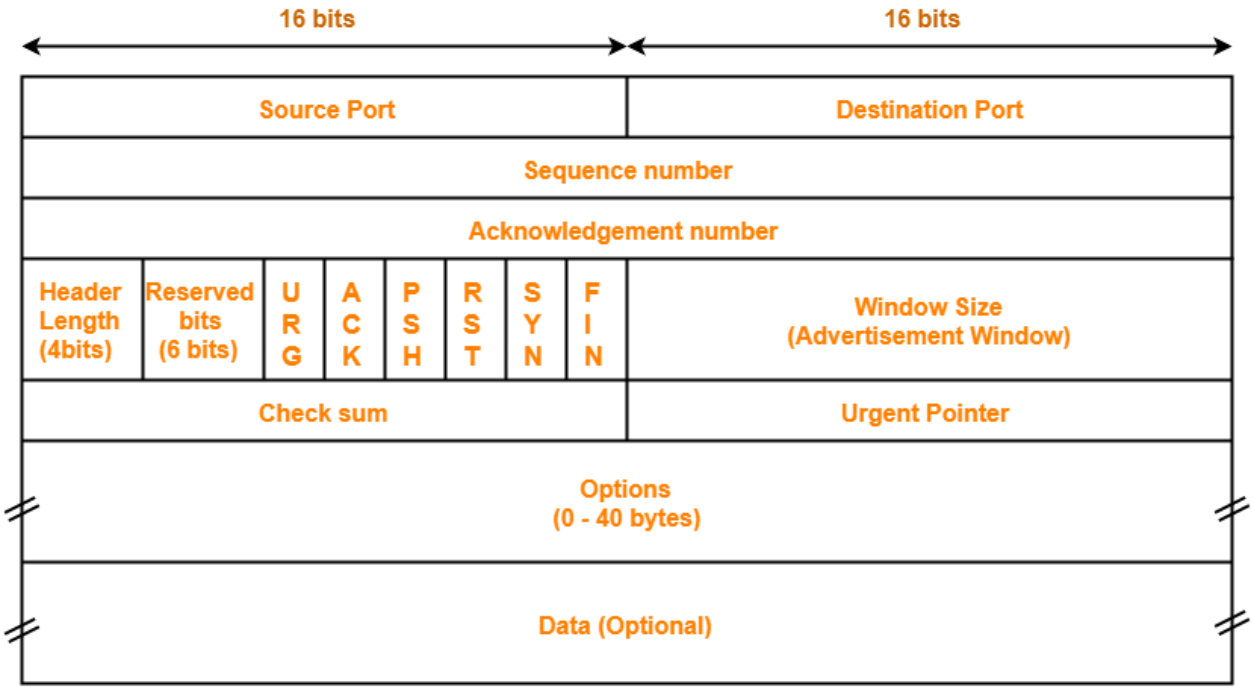


Process-to-process delivery

1. End to end Delivery (port to port)

2. Reliability (inorder , no loss of Data)
3. Error Control (checkSum)
4. Congestion Control
5. Flow control (SW , SR, GBN)

TCP (transmission control protocol)



TCP Header

FUNCTIONS

1. Byte Streaming
2. Connection Oriented
3. Full duplex
4. Piggybacking
5. Error Control
6. Flow control
7. Congestion Control

TCP maximum header size will be 20 to 60 Byte

ARP (Address Resolution Protocol)

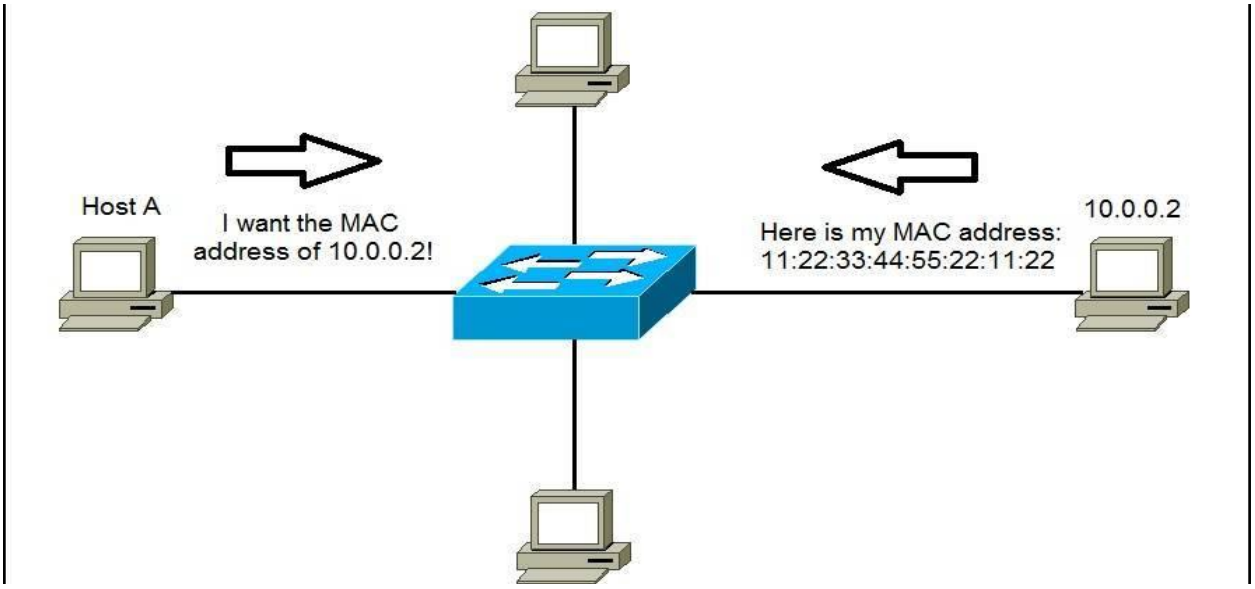
Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request 1, Reply 2
Sender Hardware address (For example, 6 bytes for Ethernet)		
Sender Protocol address (For example, 4bytes for IP)		
Target Hardware address (For example 6 bytes for Ethernet) (it is not filled in the address)		
Target Portocol address (For example ,4 bytes for IP)		

Ye level 3 ka protocol hai

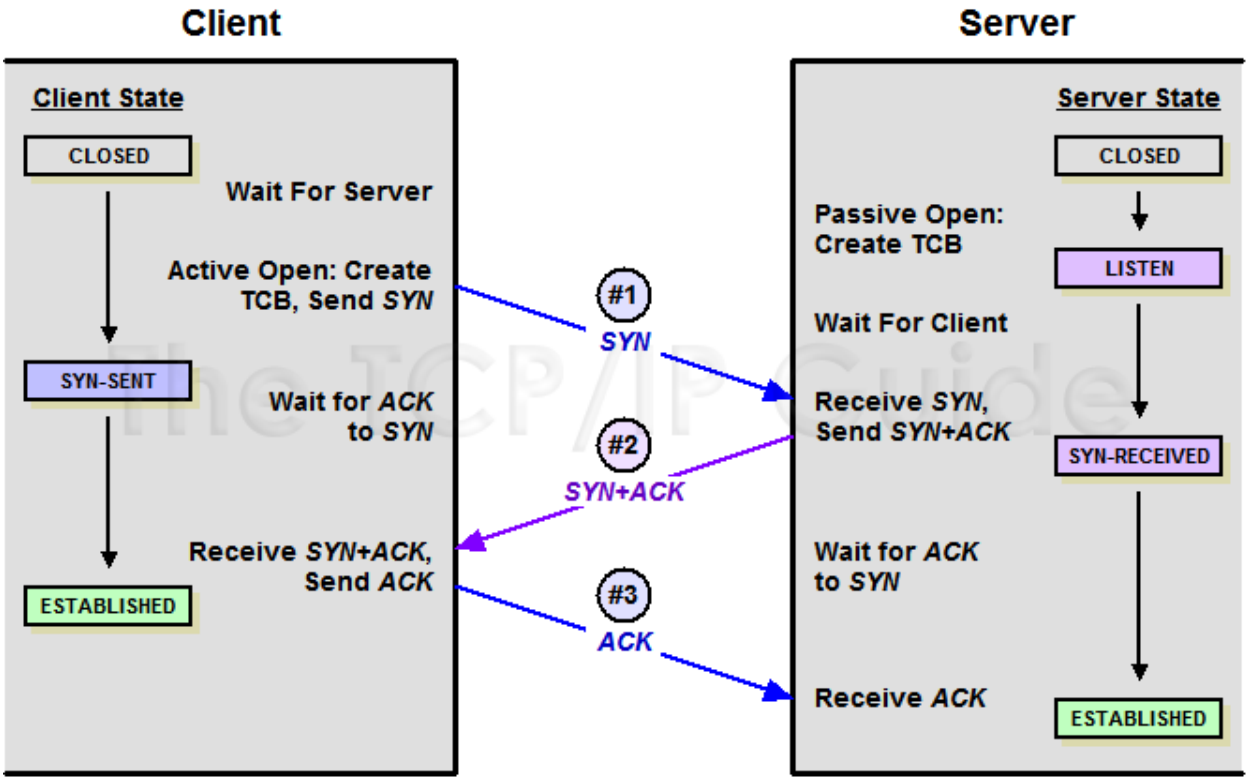
Works

1. IP ⇒ MAC
2. Logical ⇒ Physical me change karta hai
   Bina MAC address ke kisi v destination tak nahi pahucha ja sakta hai
   If A wants to communicate with B , and A doesn't know about the B's MAC address then A will broadcast this source and destination (All F as MAC) to all networks and after getting it B will unicast it .
   Request ⇒ broadcast
   Reply ⇒ Unicast

Source		Destination	
IP^A	MAC^A	IP^B	MAC^B Unknown



TCP connection Establishment

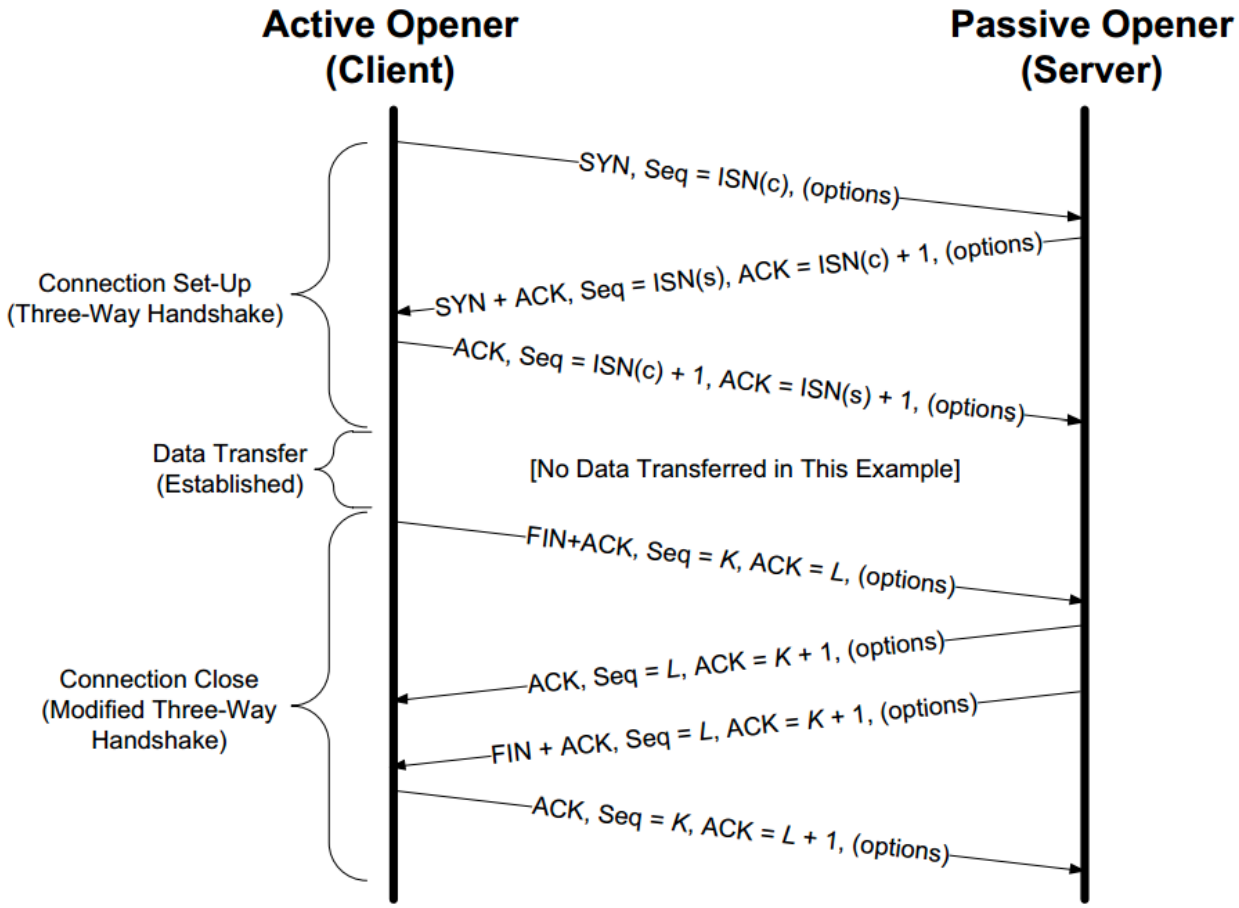


Key Concept: The normal process of establishing a connection between a TCP client and server involves three steps: the client sends a *SYN* message; the server sends a

message that combines an *ACK* for the client's *SYN* and contains the server's SYN; and then the client sends an *ACK* for the server's *SYN*. This is called the *TCP three-way handshake*.

Ek baar isko Open karke dekh lo saahi likha hua hai

TCP data Transfer



1. PiggyBacking (ACK + DATA)
2. Pure Ack(Only ACK)

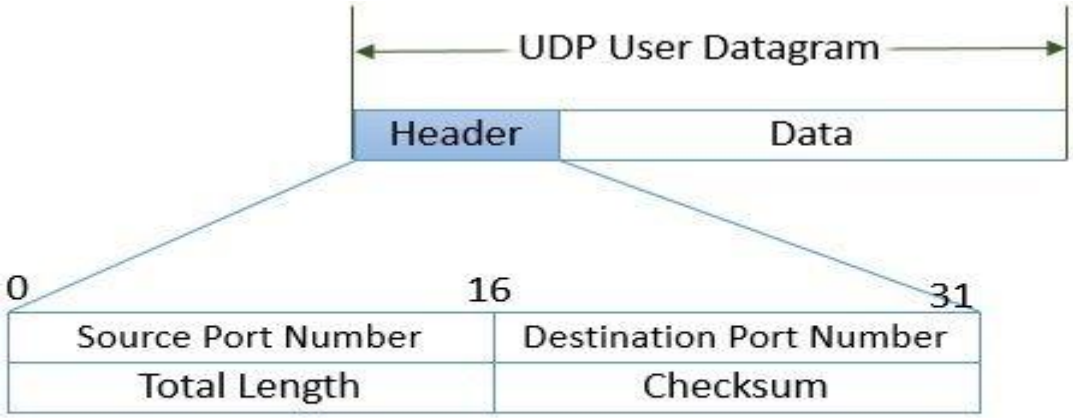
UDP (user Datagram protocol)

⇒ Connectionless
⇒ Unsynchronised
⇒no order

- Transfer layer me 2 protocol bahut important hai that is
    1. TCP 2. UDP

- CHECKSUM = UDP header + UDP Data + Pseudo header of IP
- TCP phale connection establishes karta hai then data bhejta hai but UDP koi connection nahi rakhta hai.
- UDP header me only 4 option hote hain 8 Byte fixed that means ($0\ to\ 2^{16}$-1 or 0 to 65535(16 times 1, toh ye maximum hoga port)
- Usme se 0 to 1023 well known port number hote hain

Header	Payload (data)
8 Byte	65535-8= 65527(max data can be)

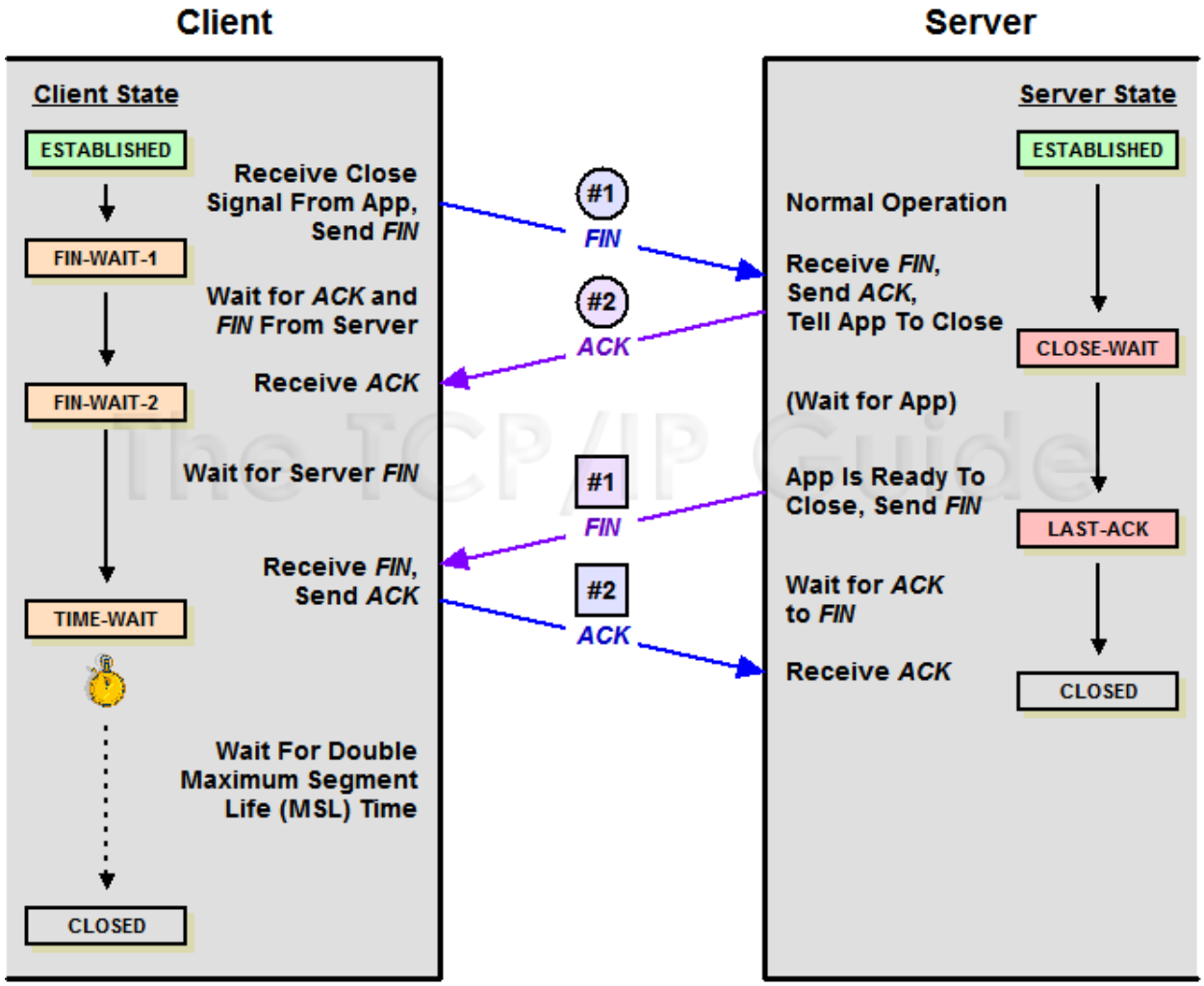


User Datagram Header Format

Table 4.1 Well-known port numbers used by UDP

Port	Protocol	Description
1	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
53	Name server	Domain Name Service
67	BOOTPs	Server port to download bootstrap information
68	BOOTPc	Client port to download bootstrap information
69	TFTP	Trivial File Transfer Protocol
111	RPC	Remote Procedure Call
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol
162	SNMP	Simple Network Management Protocol (trap)

TCP connection Termination

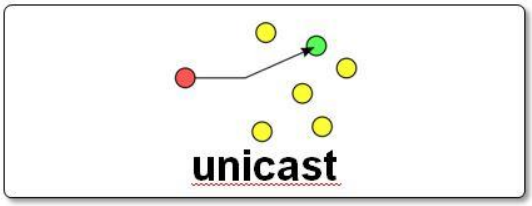


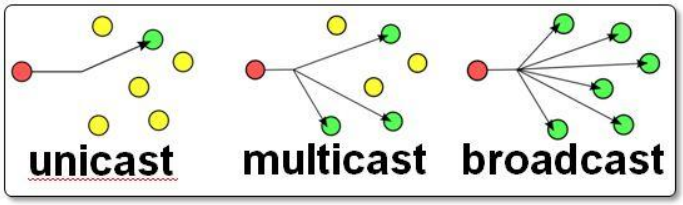
UDP application

1. Query Response Protocol (One request one reply)[DNS]
2. Speed (online games, Voice over IP)
3. Broadcasting / Multicasting[RIP]
4. Continuous Streaming [SkyPe, Youtube]

- Slower but reliable transfers
- Typical applications:
  - Email
  - Web browsing

- Fast but non-guaranteed transfers ("best effort")
- Typical applications:
  - VoIP
  - Music streaming



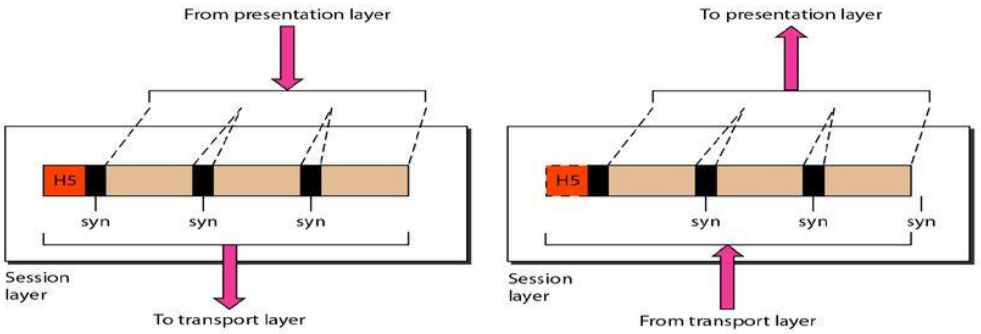


Difference between TCP and UDT

Protocol	TCP	UDP
Connection	connection-oriented	connectionless
Usage	high reliability, critical-less trans-mission time	fast, efficient transm-ission, small queries, huge numbers of clients
Ordering of data packets	rearranges packets in order	no inherent order
Reliability	yes	no
Streaming of data	read as a byte stream	sent and read indivi-dually
Error checking	error checking and recovery	simply error checking, no error recovery
Acknowle-dgement	acknowledgement segments	no acknowledgment

Session Layer

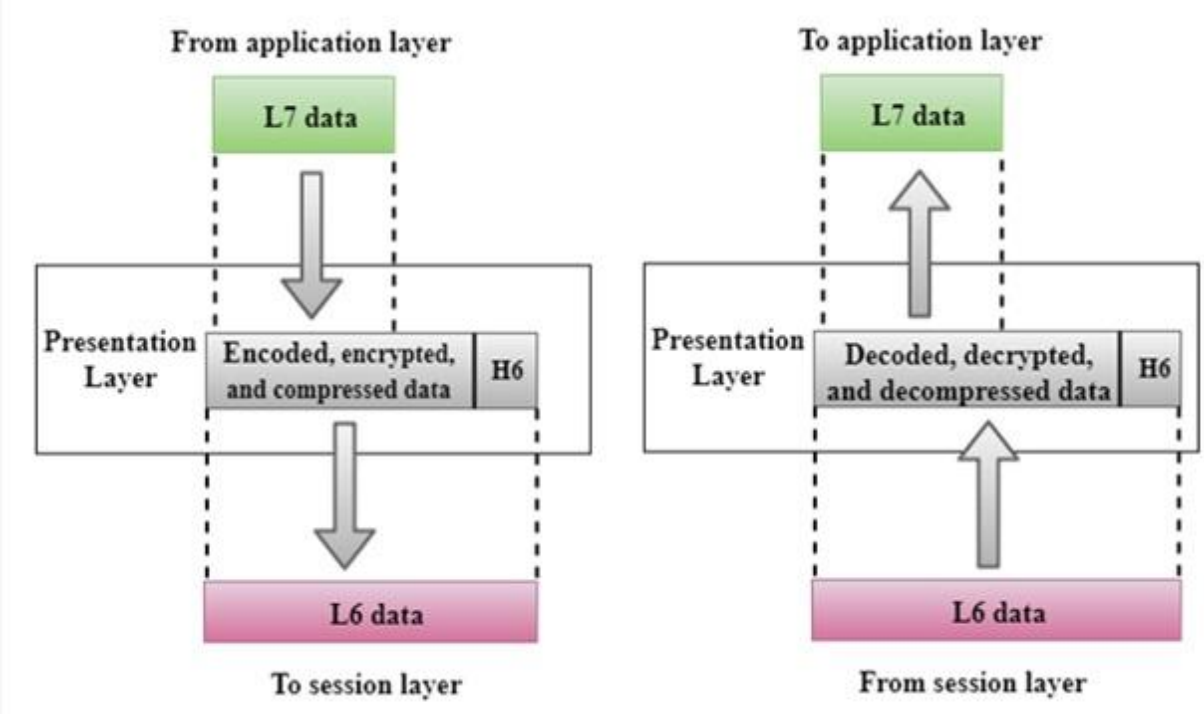
- This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.



:::Functions :::

1. Authentication 2. Session Restoration (check point) 3. Webinar (flow control sync)

Presentation Layer



FUNCTION OF PRESENTATION LAYER

1. Code conversion from ASCII to EBCDIC and vice-versa
2. Encryption / Decryption
3. Compression

Application layer

Service Name	Port	Comment
ftp	20	FTP - data
ftp	21	FTP - control
ssh	22	SSH Remote Login Protocol
telnet	23	TELNET
smtp	25	Simple Mail Transfer Protocol
domain	53	Domain Name Server
bootps	67	Bootstrap Protocol - server
bootpc	68	Bootstrap Protocol - client
tftp	69	Trivial File Transfer
http	80	World Wide Web
pop3	110	Post Office Protocol - version 3
sunprc	111	SUN Remote Procedure Call
Netbios-ssn	139	NETBIOS Session Service (SMB)
imap	143	Internet Message Access Protocol
snmp	161	Simple Network Management Protocol
bgp	179	Border Gateway Protocol
irc	194	Internet Relay Chat Protocol
ldap	389	Lightweight Directory Access Protocol
https	443	http secure
ipp	631	Internet Printing Protocol
wins	1512	Windows Internet Name Service
nfsd	2049	NFS server
squid	3128	Squid Web Proxy
mysql	3306	MySql

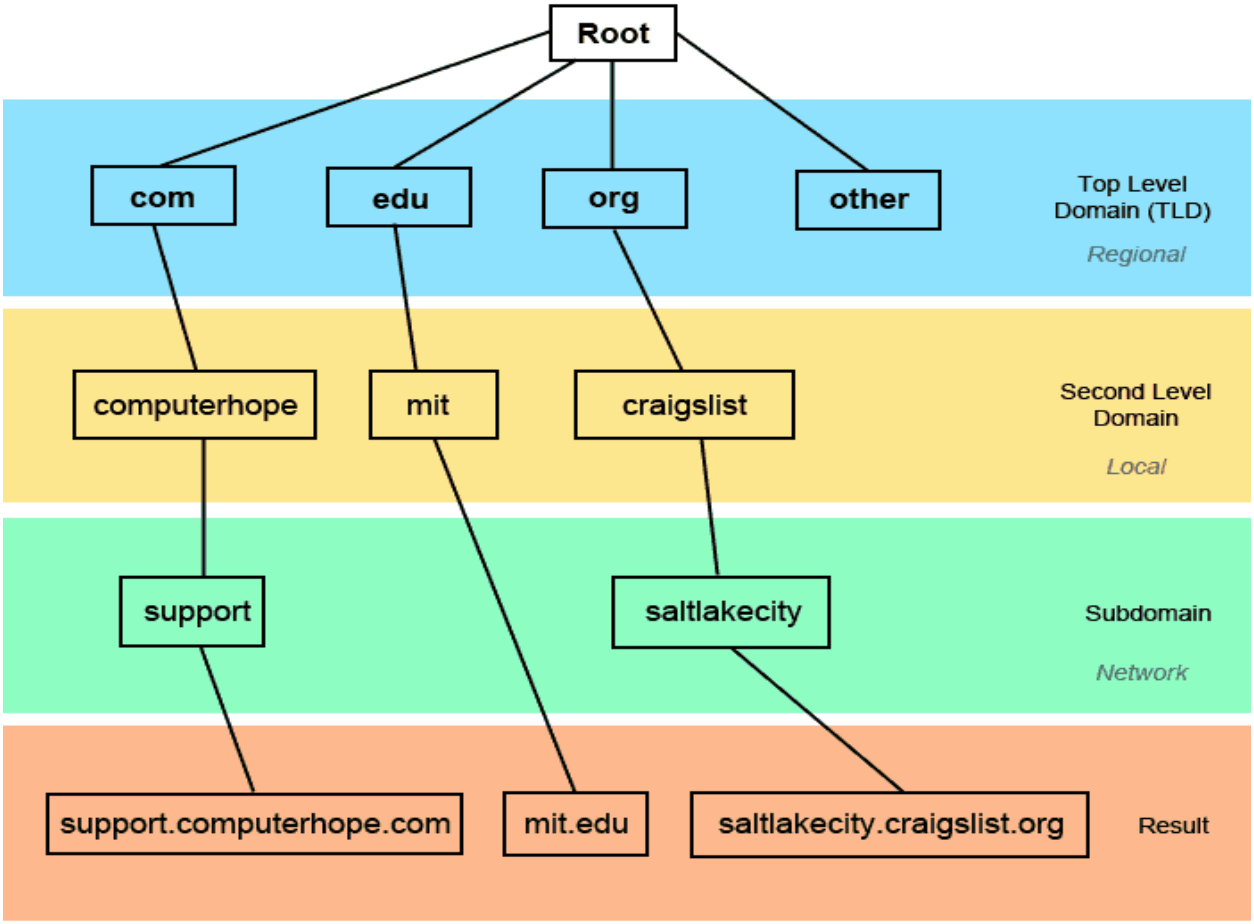
Feb 9, 2022

Domain Name System (DNS)

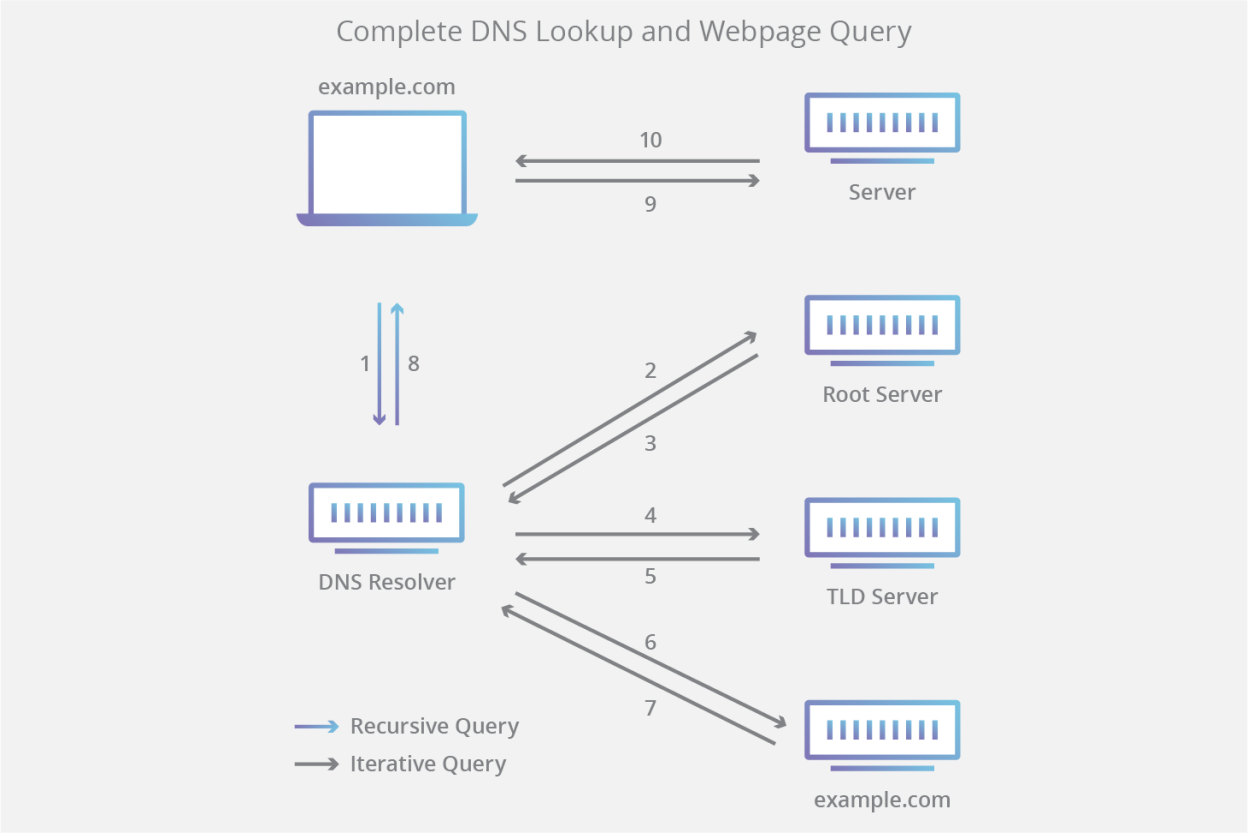
ISP isko cache karke rakhta hai mtlb mapping IP and DNS ko

- DNS use UDP protocol

Domain Naming Hierarchy



Iterative and Recursive mode



Application Layer Protocol

Important ⇒ DNS , HTTP, FTP , SMTP , POP

HTTP

- Port no 80
- Itself not reliable but use TCP to achieve reliability
- Inband Protocol
- Stateless
- HTTP 1.0 Non-Persistent
- HTTP 1.1 Persistent
- Commands(Head, Get, Post, Put, Delete, Connect)

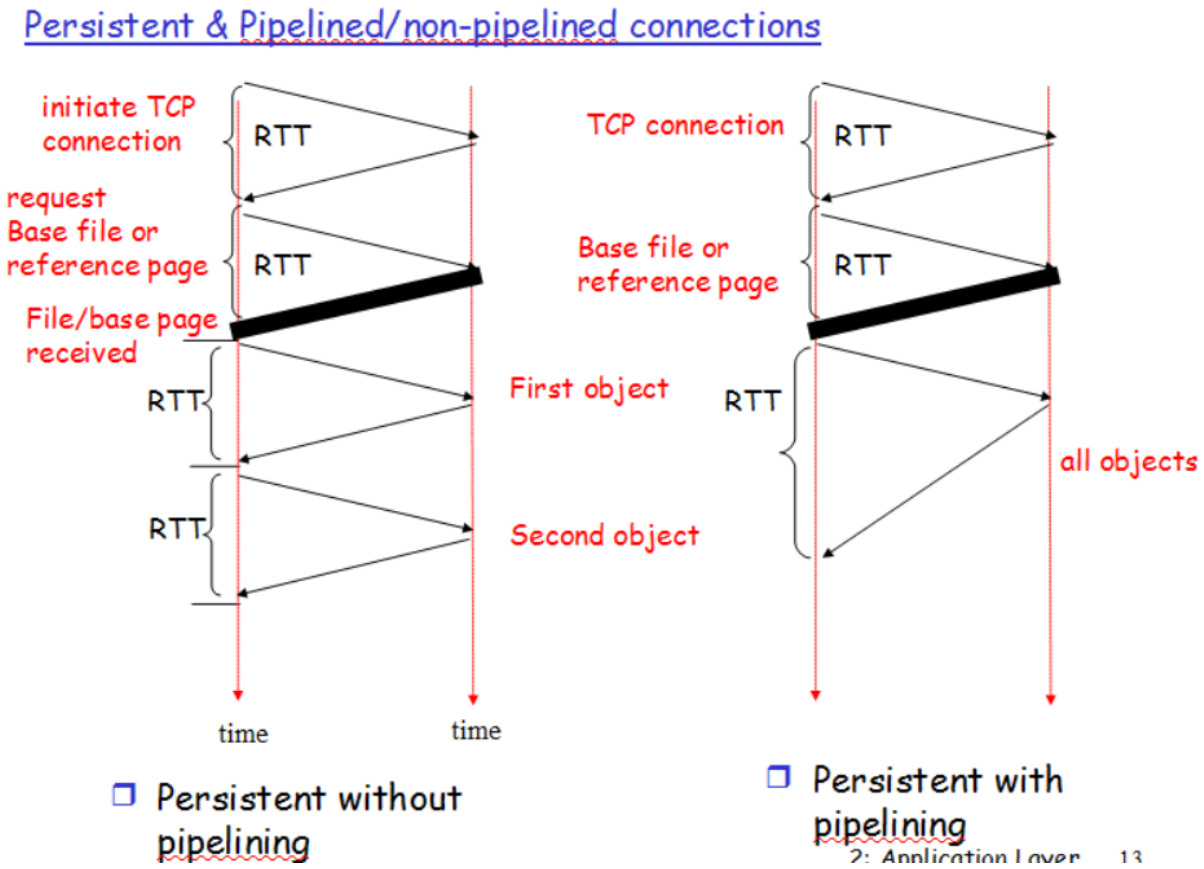
FTP

- Port no 20(DATA) & 21(Control)
- Data connection is non-persistent
- Control connection is persistent
- Not Inband
- Reliable
- Stateful

SMTP & POP

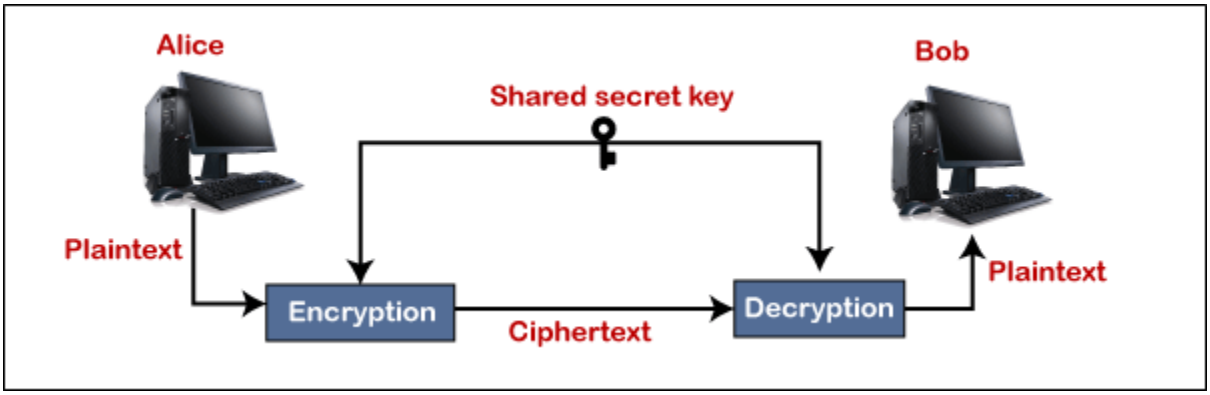
- FTP is synchronous but SMTP & POP is both synchronous & asynchronous
- SMTP Port no 25 for pushing the mail
- By default, the **POP3 protocol** works on **two** ports: Port **110** - this is the default **POP3** non-encrypted port. Port **995** - this is the port you need to use if you want to connect using **POP3** securely.
- MIME(**Multipurpose Internet Mail Extensions**)

Persistent and non-persistent HTTP

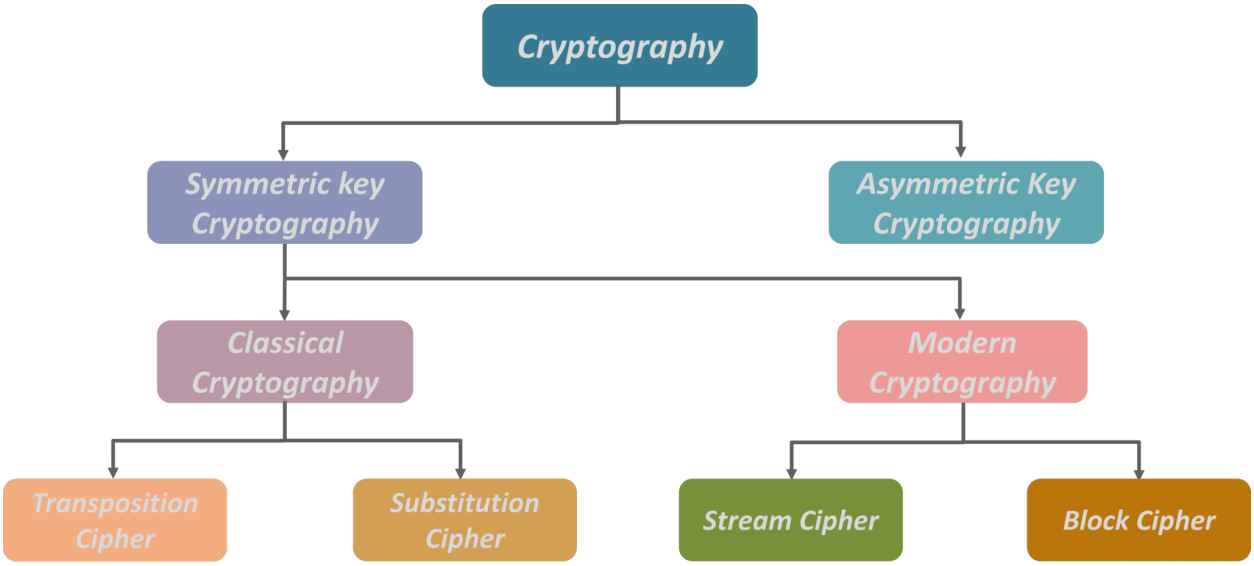


RTT= Round Trip time

Cryptography



Feb 10, 2022



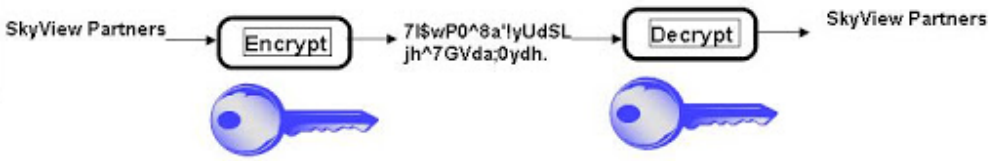
Symmetric Key

Types of Encryption

DES
TripleDES
AES
RC5

Symmetric Keys

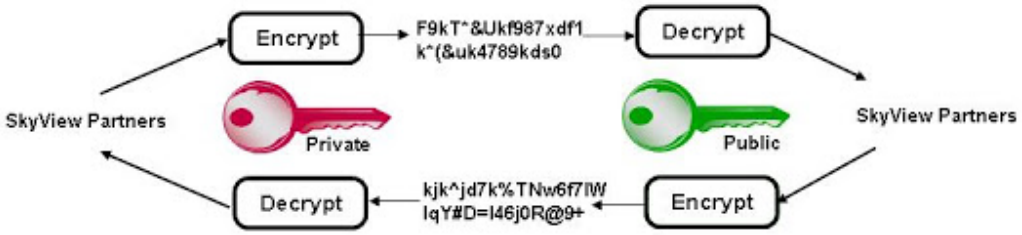
- Encryption and decryption use the **same key**.



RSA
Elliptic Curve

Asymmetric keys

- Encryption and decryption use different keys, a **public key** and a **private key**.

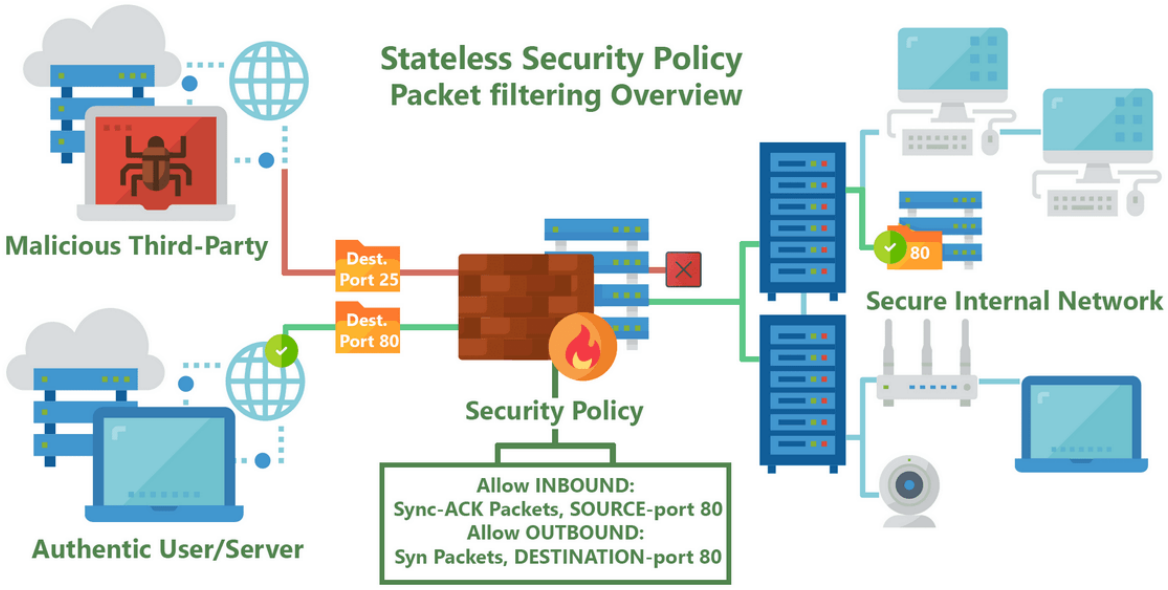


MD5
SHA-1

One-way hash

Firewalls (Network Security)

- Monitors and controls incoming and outgoing traffic based on predefined rules.
- Act like a barrier
- Host based and network based firewall



Packet Filtering Firewall (layer-4)

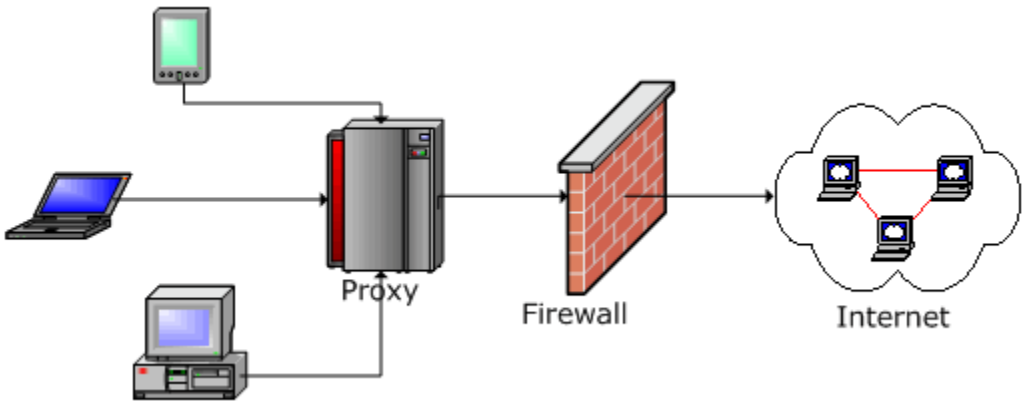
- Check IP header , TCP header
- Works on Network and Transport Layer
- Can block IP address, full Network
- Can block a service (http, ftp etc)

Default Allow Table

Rule No.	Source IP	Source Port	Destination IP	Dest. Port
1	179.2.4.80	Any	Any	Any
2.	152.32.0.0	Any	Any	Any
3.	Any	Any	172.9.0.3	Any
4.	Any	80	Any	Any
5.	Any	Any	Any	21

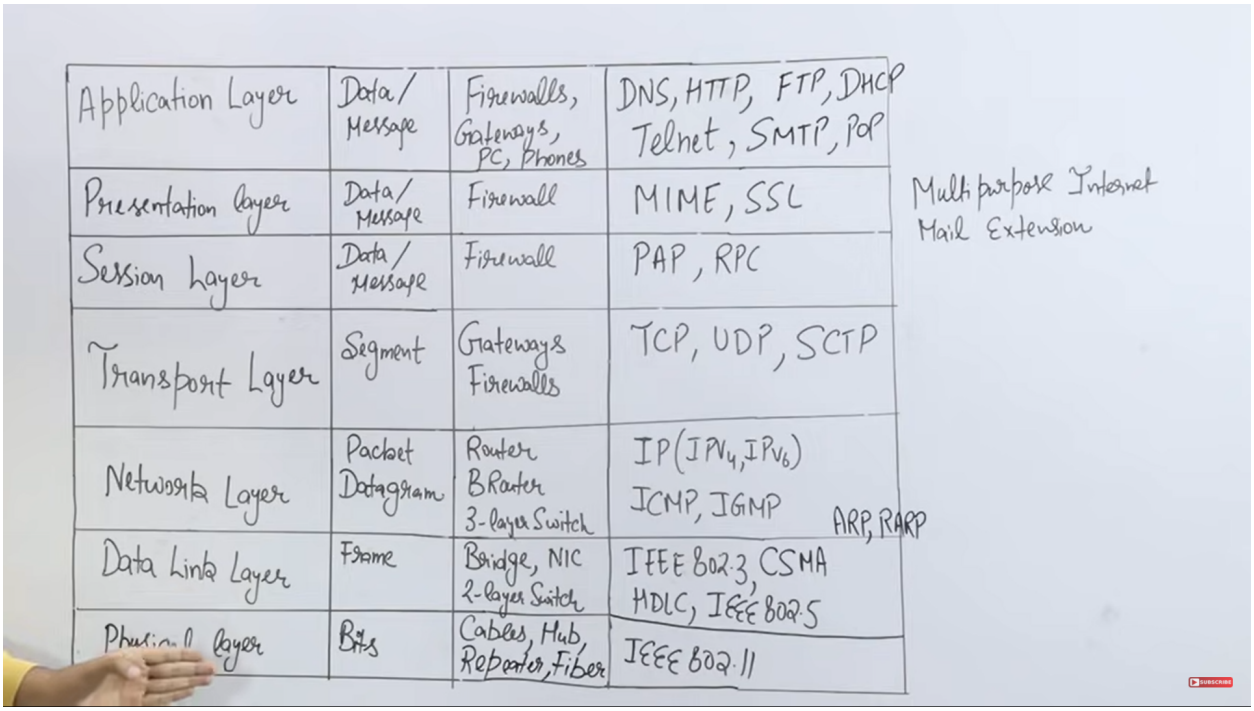
Isme jo hai oo nahi jaa payega or baaki sab jayega

Proxy Firewalls



- Proxy Firewall , ye user ka details check karta hai , har call me like https

Important Notes



ARP= use for finding the MAC address of the given IP address
Bits ke baad data Digital ya phir analog me change ho jata hain

Important Linux command

1. ***IFCONFIG*** ⇒ ifconfig(interface configuration) command is used to configure the kernel-resident network interfaces. It is used at the boot time to set up the interfaces as necessary. After that, it is usually used when needed during debugging or when you need system tuning.

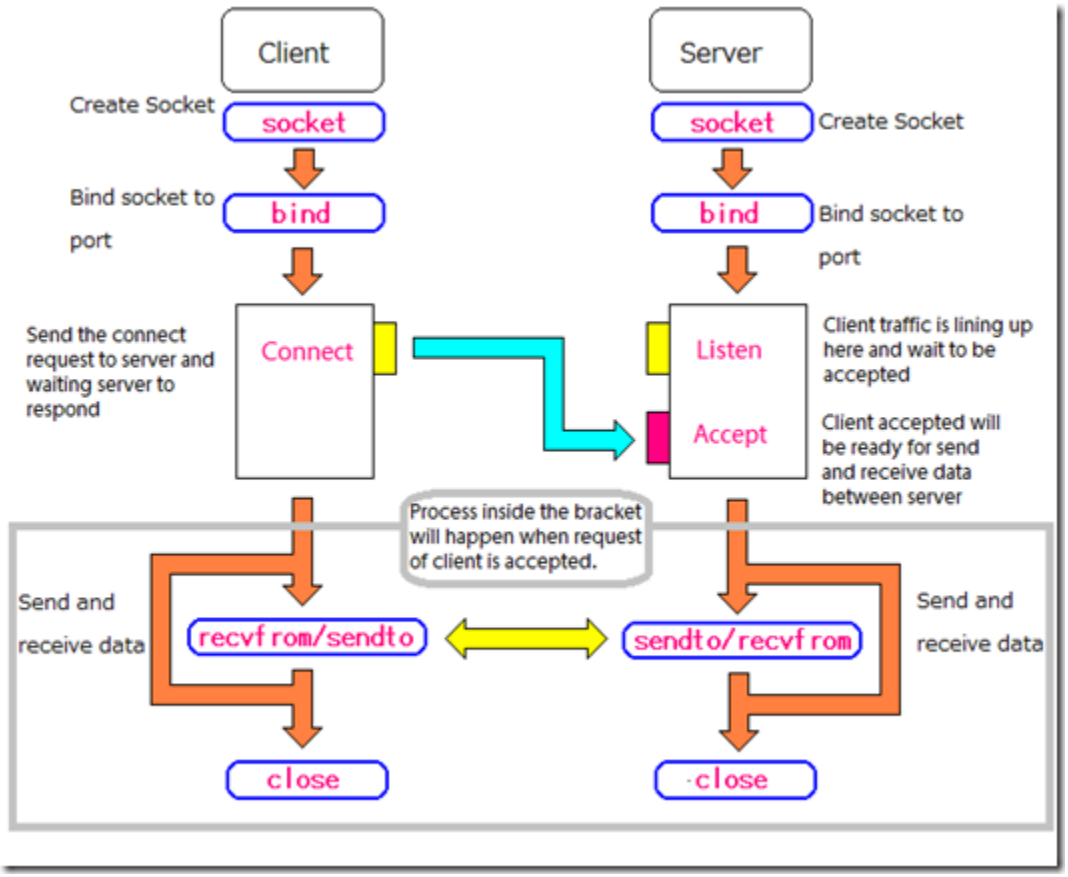
2. ***IP commands***⇒***i***p command in Linux is present in the net-tools which is used for performing several network administration tasks. IP stands for Internet Protocol. This command is used to show or manipulate routing, devices, and tunnels. It is similar to ifconfig command but it is much more powerful with more functions and facilities attached to it. ifconfig is one of the deprecated commands in the net-tools of Linux that has not been maintained for many years. ip command is used to perform several tasks like assigning an address to a network interface or configuring network interface parameters

3. ***Traceroute*** ⇒traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes

4. ***Tracepath command*** in Linux is used to traces path to destination discovering MTU along this path. It uses a UDP port or some random port. It is similar to traceroute, but it does not require superuser privileges and has no fancy options. tracepath6 is a good replacement for traceroute6 and a classic example of the application of Linux error queues. The situation with IPv4 is worse because commercial IP routers do not return enough information in ICMP error messages. It will change, when they will be updated. For now, it uses Van Jacobson's trick, sweeping a range of UDP ports to maintain trace history.

5. ***Ping command***⇒PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host. This command takes as input the IP address or the URL and sends a data packet to the specified address with the message "PING" and get a response from the server/host this time is recorded which is called latency. Fast ping low latency means faster connection. Ping uses ICMP(Internet Control Message Protocol) to send an ICMP echo message to the specified host; if that host is available then it sends an ICMP reply message. Ping is generally measured in milliseconds; every modern operating system has this ping pre-installed.

Socket Programming



Why there is need of IPv6(IPng)

- Limitation in IPv4 address
- 2^{32}=4,294,967,296
- $2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$
- Realtime data transmission
- Authentication
- Encryption enabled
- Fast Processing at routers

IP security (IPSec,3rd layer)

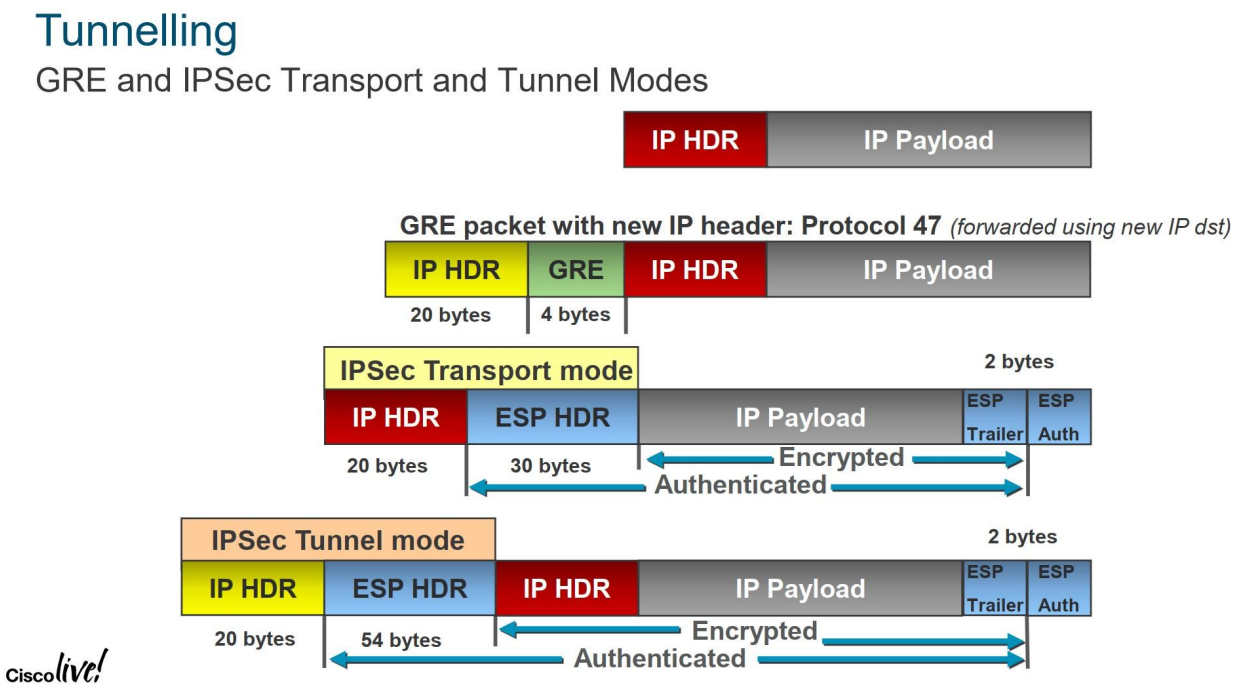
- IETF standard
- Network layer protocol (used both by IPv4 and IPV6)
- Uses of IP security
    1. Confidentiality
    2. Authentication/ Integrity
    3. Replay Attack Protection

Collection of protocols

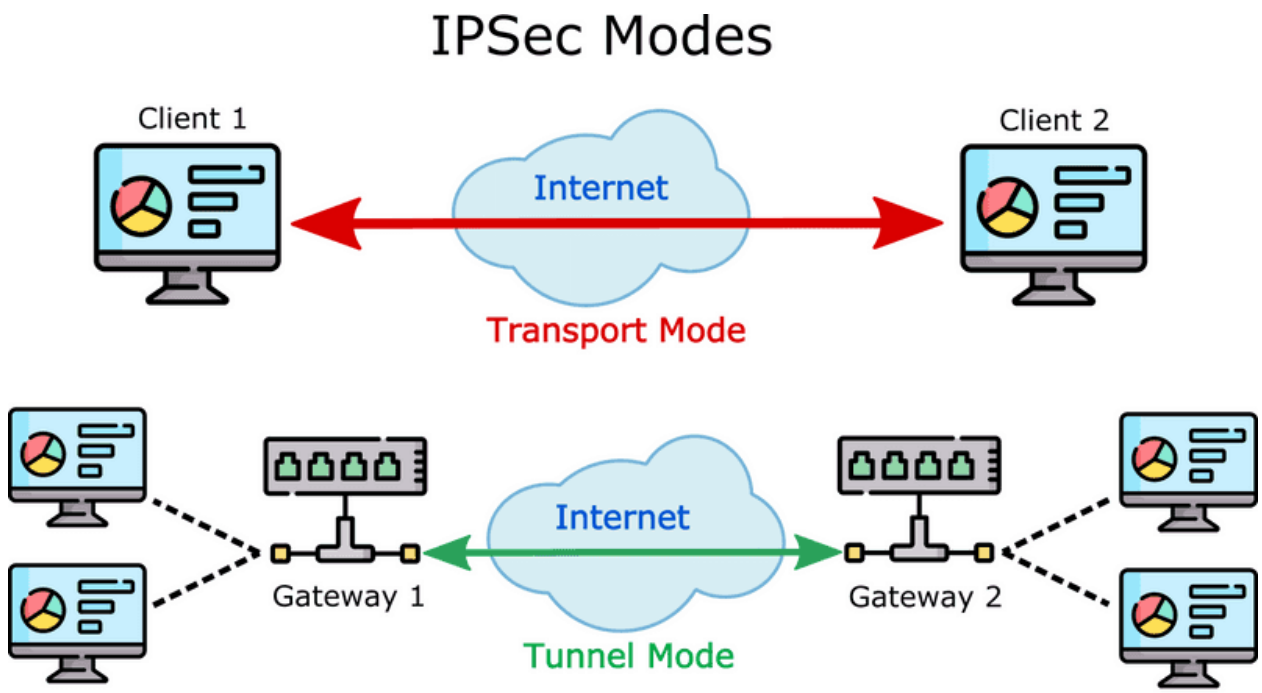
1. Encapsulation Security Payload (ESP)
2. Authentication Header(AH)
3. Internet Key Exchange (IKE)

Two modes of Operation (Transport Mode and Tunnel Mode)

Transport Mode vs Tunnel mode



Cisco live!



What is a Socket Address?

Socket Address⇒ ***IP address + PORT no (32 bit+16 bit) =46 bit***

- ***It is use to identify the connection Uniquely***

Why port no can not define a unique connection?

⇒ **The size of Port is 16 bit**
Then total possible of port number is from 0 to 2^16 (15 times 1)
⇒ **0 to 65535**
⇒ **0 to 1023 == well defined port no hai** (***like http , https , FTP……***)
⇒ **1024 to 49151 == Reserved by big corporate** (***like facebook , amazon …..)***
⇒ **49152 to 65535 == for real use (Local Machine)**, then ye bahut hua na , agar ek time me bahut saare log request kiye toh bahut saare device kar port number same ho jayega

Same for IP address , agar same local machine se bahut sare request bhej diye to IP address to same hai range but Port no alag rahega that is why (***IP address + PORT no***) use karte hain for uniquely identifying the connection .