COMPUTER NETWORKS

15 January 2025 19:00

The **OSI (Open Systems Interconnection**) Model is a conceptual framework that standardizes the functions of a communication system into seven distinct layers.

Application Layer: Applications create the data.

Presentation Layer: Data is formatted and encrypted.

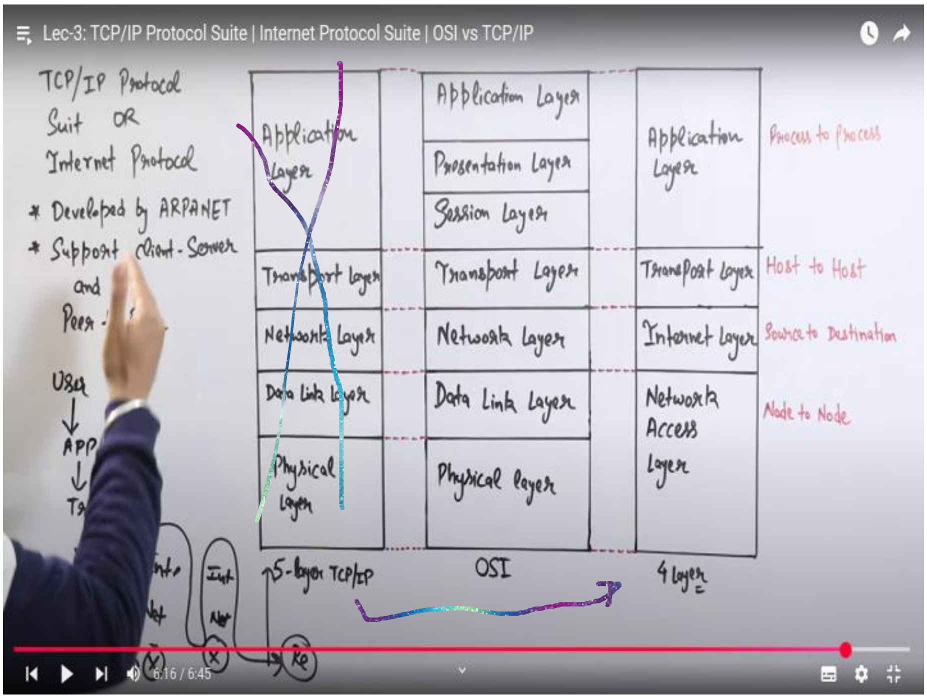
Session Layer: Connections are established and managed.

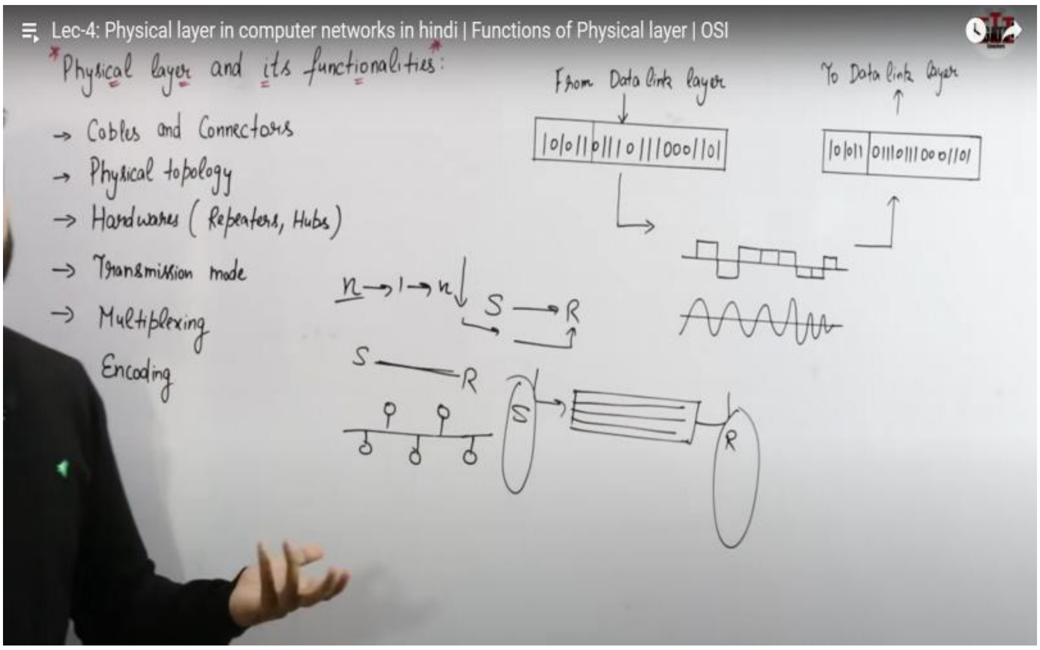
Transport Layer: Data is broken into segments for reliable delivery.

Network Layer : Segments are packaged into packets and routed.

Data Link Layer: Packets are framed and sent to the next device.

Physical Layer: Frames are converted into bits and transmitted physically.





--

DATA COME FROM THE DATA LINK LAYER IS IN THE BINARY FORMT IT WILL CONVERET THE DATA INTO THE SIGNALS

MULTIPLEXING AND DEMULTIPLEXING

N-->1-->N I.E WE PASS MULTIPLE SIGNALS IN THE ONE TIME BY COMBINING THE SIGNALS

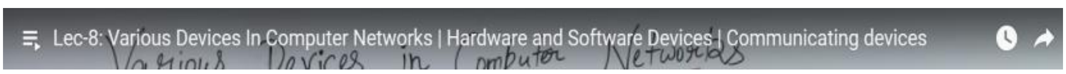
ENCODING

ANALOG -- > ANALOG
ANALOG TO DIGITAL

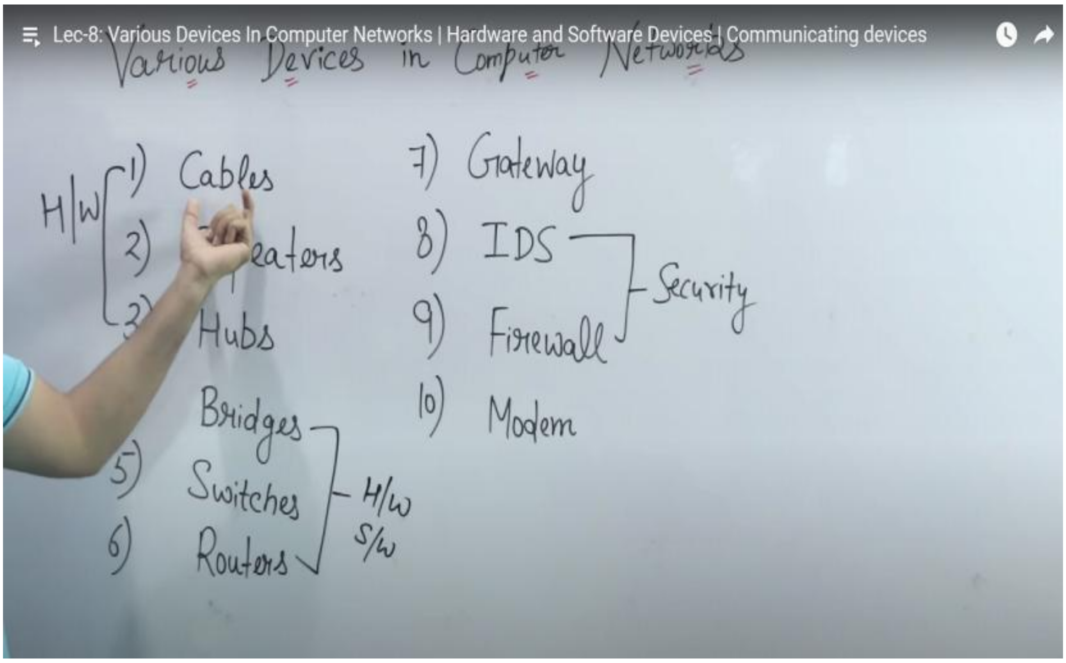
MANCHESTOR ENCODING AND DIFFERENTIAL MANCHESTOR ENCODING THESE ARE TWO TYPES OF THE ENCODING

TOPOLOGY

H/W



H/W



CABLES :-

Twisted pair cable
co-axial cable
Fiber optics

Repeaters

Repeater regenerates the strength that is loos by the attenuation
Repeater and Amplifier are not same their purpose is different
2 port device

HUBS

Multi Port Device
Forwarding
No Filtering

BRIDGE

USED TO CONNECT THE TWO DIFFERENT NODES

SWITCHES

THESE ARE THE SMART DEVICE

Hub, Switch, and Router are network devices used to connect devices and manage data communication within and between networks.

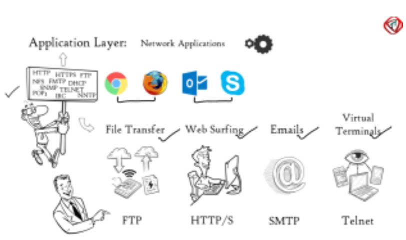
1. **Hub**
Definition: A basic networking device that *connects multiple devices in a network*, transmitting data to all connected devices.
How it Works:
When data arrives at one port, th**e hub copies it and sends it to every other port**.
It does not differentiate between devices or filter traffic.

2. **Switch**
Definition: A more advanced device that connects multiple devices in a network and forwards data only to the intended recipient.
How it Works:
A switch learns the **MAC addresses** of connected devices (CREATE THE TABLE).
It directs data packets to the specific device instead of broadcasting to all devices.

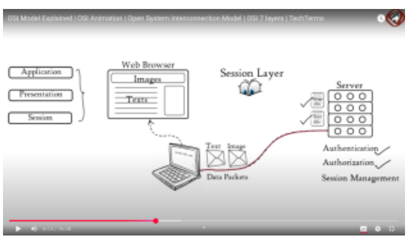
3.**Router**
Definition: A device that connects multiple networks and routes data between them.
How it Works:
Routers use IP addresses to determine the **best path for forwarding data** between networks.
They connect a **local network to the Internet** or other external networks.

TYPE OF CASTING (SENDING THE DATA)

UNICASTING ,MULTI,BROAD

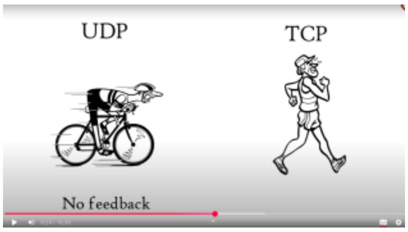


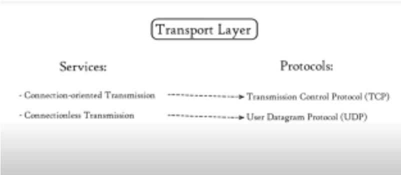
Presentation Layer
This layer is concerned with the syntax and semantics of the information transmitted

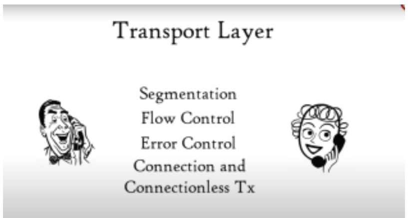


Session Layer
It deals with the concept of **Sessions** i.e. when a user logins to a remote server he should be **authenticated** before getting access to the files and application programs. Another job of session layer is to establish and maintain sessions. If during the transfer of data between two machines the session breaks down, it is the session layer which re-establishes the connection.

From <https://www.cse.iitk.ac.in/users/dheeraj/cs425/lec02.html#application>

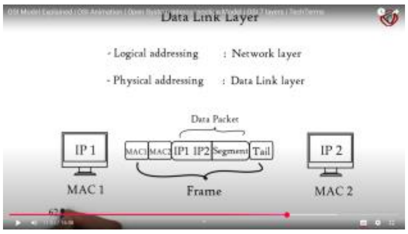






1. DATA LINK LAYER
2. Framing : Breaking input data into frames (typically a few hundred bytes) and caring about the frame boundaries and the size of each frame.
3. Acknowledgment : Sent by the receiving end to inform the source that the frame was received without any error.
4. Sequence Numbering : To acknowledge which frame was received.
5. Error Detection : The frames may be damaged, lost or duplicated leading to errors.The error control is on **link to link** basis.
6. Retransmission : The packet is retransmitted if the source fails to receive acknowledgment.
7. Flow Control : Necessary for a fast transmitter to keep pace with a slow receiver.

From <https://www.cse.iitk.ac.in/users/dheeraj/cs425/lec01.html#physical>

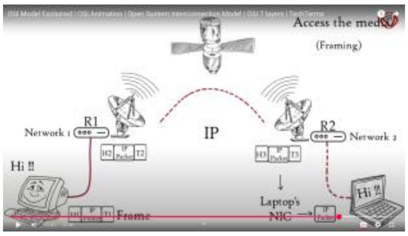


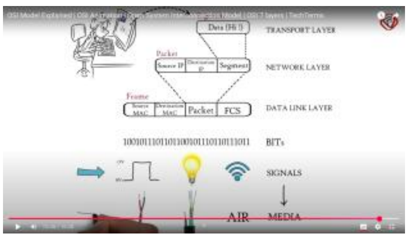
Its basic functions are routing and congestion control.
Routing: This deals with determining how packets will be routed (transferred) from source to destination.

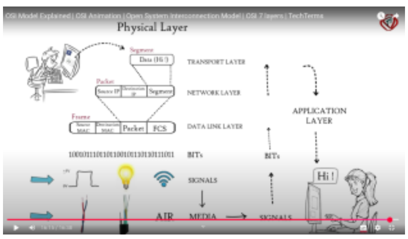
- **Connection less service:** Each packet of an application is treated as an independent entity. On each packet of the application the destination address is provided and the packet is routed.
Connection oriented service: Here, first a connection is established and then all packets of the application follow the same route.

Congestion Control: A router can be connected to 4-5 networks. If all the networks send packet at the same time with maximum rate possible then the router may not be able to handle all the packets and may drop some/all packets. In this context the dropping of the packets should be minimized and the source whose packet was dropped should be informed.

Internetworking: Internetworks are multiple networks that are connected in such a way that they act as one large network, connecting multiple office or department networks. Internetworks are connected by networking hardware such as routers, switches, and bridges



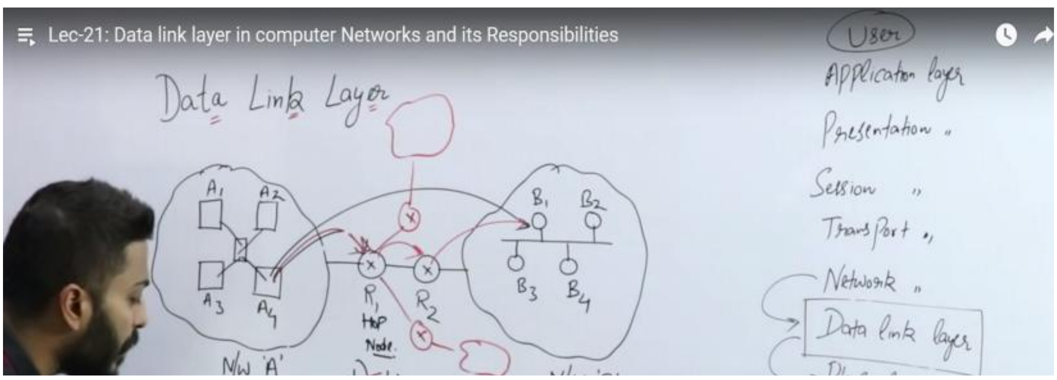


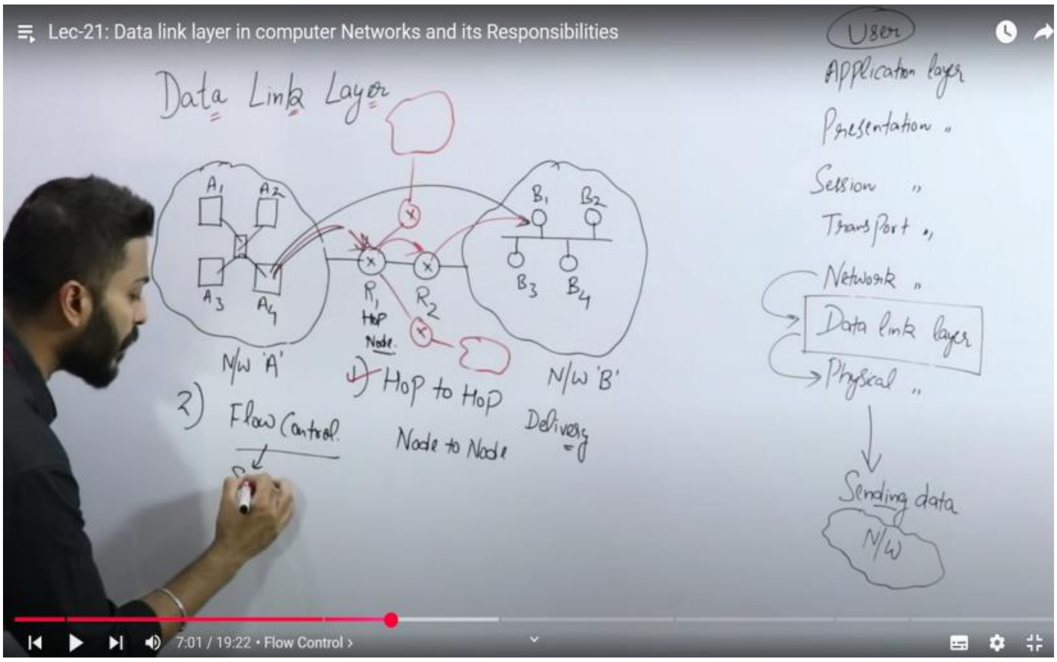


It helps in the transmission of data between two machines that are communicating through a physical medium, which can be optical fibres,copper wire or wireless etc.

From <https://www.cse.iitk.ac.in/users/dheeraj/cs425/lec01.html#physical>

DATA LINK LAYER





ITS RESPONSIBILITY IS THE ***HOP TO HOP DELIVERY***
THAT IS POINT TO POINT MEANS FROM HOP TO HOP DELIVERY THAT MEANS ***ONE ROUTER R1 TO ROUTER R2***

FLOW CONTROL :- WHILE ***PASSING THE DATA IT WILL MANAGE THE FLOW OF THE DATA I.E EKA SATH JADA DATA NAHI JANA CHAYIE***

1. STOP AND WAIT ARQ PROTOCOL
2. GO BACK N ARQ PROTOCOL
3. SELECTIVE REPEAT ARQ PROTOCOL

ERROR CONTROL :-
1.CHECKSUM
2.CYCLIC REDUDANCY CHECK (CRC)
3.HAMMING CODE ERROR DETECTION

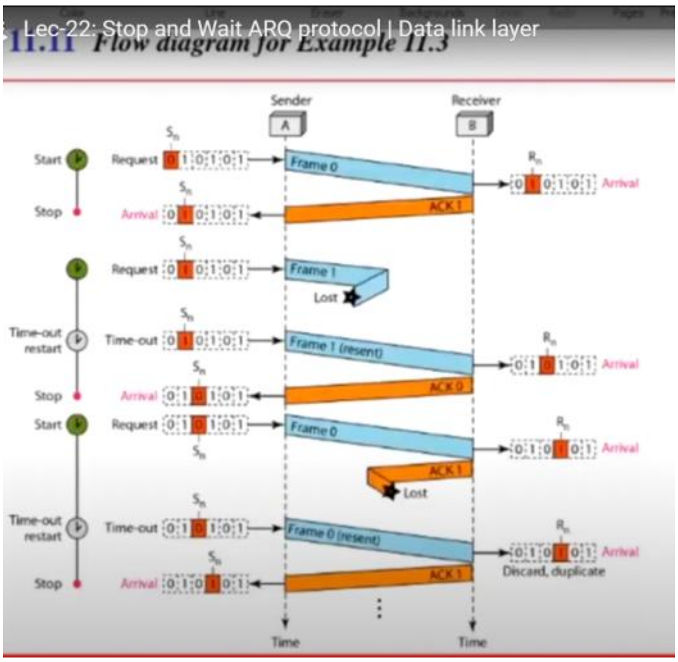
ACCESS CONTROL :-
to control access to a shared communication medium. It ensures that ***multiple devices can transmit data over the same network channel without interfering with each other.***
DATA LINK LAYER HAS MAINLY TWO LAYERS LLC (LOGICAL LAYER CONTROL) AND MAC (MULTIPLE ACCESS CONTROL)
1.PURE ALOHA
2.CSMA
CSMA/CD
CSMA/CA

ETHERNET FRAME FORMAT :-
1.IEEE 802.3 (FRAMES FOR)
2.IEEE 802.5 (RING TOPOLOGY USES)

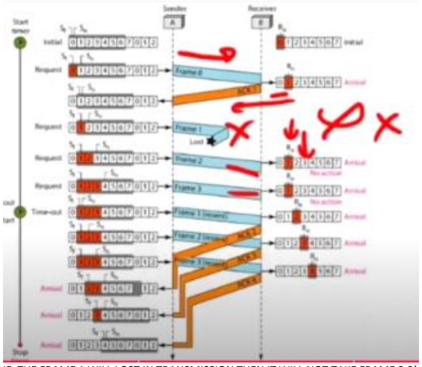
Feature	CSMA/CA	CSMA/CD
Purpose	Prevents collisions before they occur.	Detects collisions after they happen.
Operation	Devices send a request to transmit and wait for an acknowledgment before sending data.	Devices monitor the network, and if a collision occurs, they stop transmission and retry.
Usage	Used in wireless networks (e.g., Wi-Fi).	Used in wired Ethernet networks.
Efficiency	Less efficient due to waiting mechanisms.	More efficient in wired setups but limited in wireless environments.
Collision Handling	Avoids collisions proactively.	Resolves collisions reactively.

FLOW CONTROL IN DATA LINK LAYER

FLOW CONTROL :- WHILE PASSING THE DATA IT WILL MANAGE THE FLOW OF THE DATA I.E EKA SATH JADA DATA NAHI JANA CHAYIE

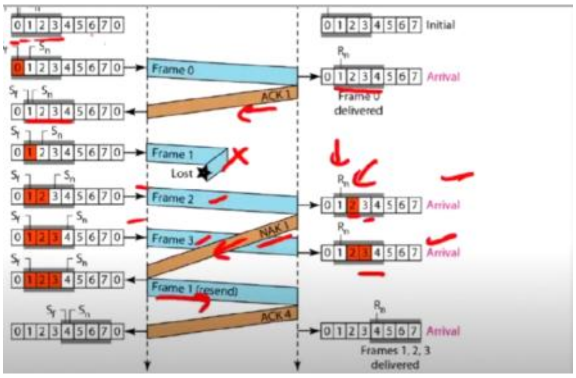


GO BACK-N ARQ



IF THE FRAME 1 WILL LOST IN TRANSMISSION THEN IT WILL NOT TAKE FRAME 2,3`

Selective Repeat ARQ (Automatic Repeat Request) | Data Link Layer



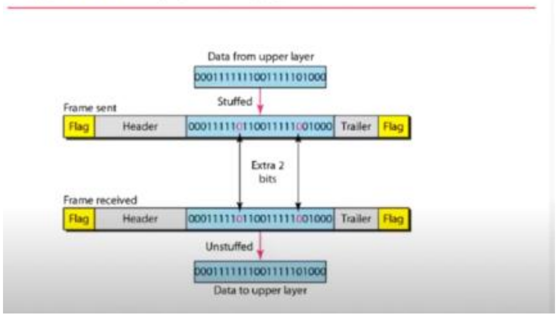
IN THIS IF ONE IS NOT COME THEN IT WILL ACCEPT OTHER FRAMES BUT AFTER COMPLETING THE ALL FRAMES THEN IT WILL SEND THE NEGATIVE ACK

Flow Control in Data Link Layer

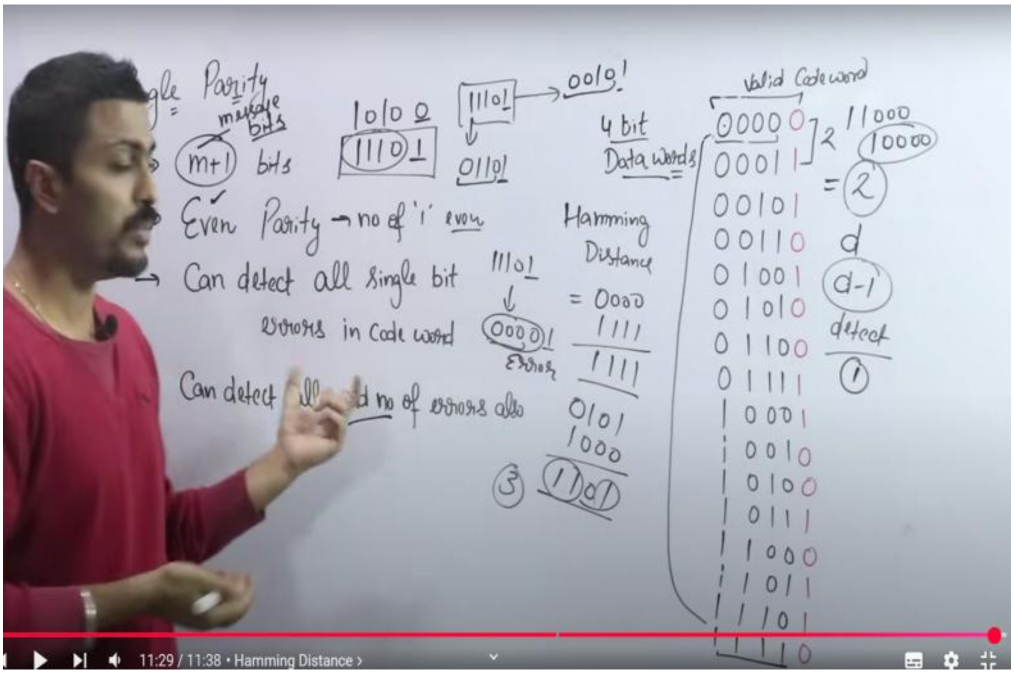
"Stop & Wait"	"Go back N"	"Selective Repeat"
→ Only 1 frame transmit	→ Multiple frames	→ Multiple frames
→ Sender Window = 1	→ Sender Window = $2^K - 1$	→ Sender Window = 2^{K-1}
→ Receiver Window = 1	→ Receiver Window = 1	→ Receiver Window = 2^{K-1}
→ $\eta = \frac{1}{1+2x}$ ∵ $x = \frac{T_p}{T_t}$	→ $\eta = (2^K - 1) * \frac{1}{1+2x}$	→ $\eta = 2^{K-1} * \frac{1}{1+2x}$
→ Retransmission = 1	→ Commulative ACK	→ Commulative & Independent ACK
	→ Retransmission = $2^K - 1$	→ Retransmission = 1

Framing in Data Link Layer

Figure 11.4 *Bit stuffing and unstuffing*



ERROR DETECTION

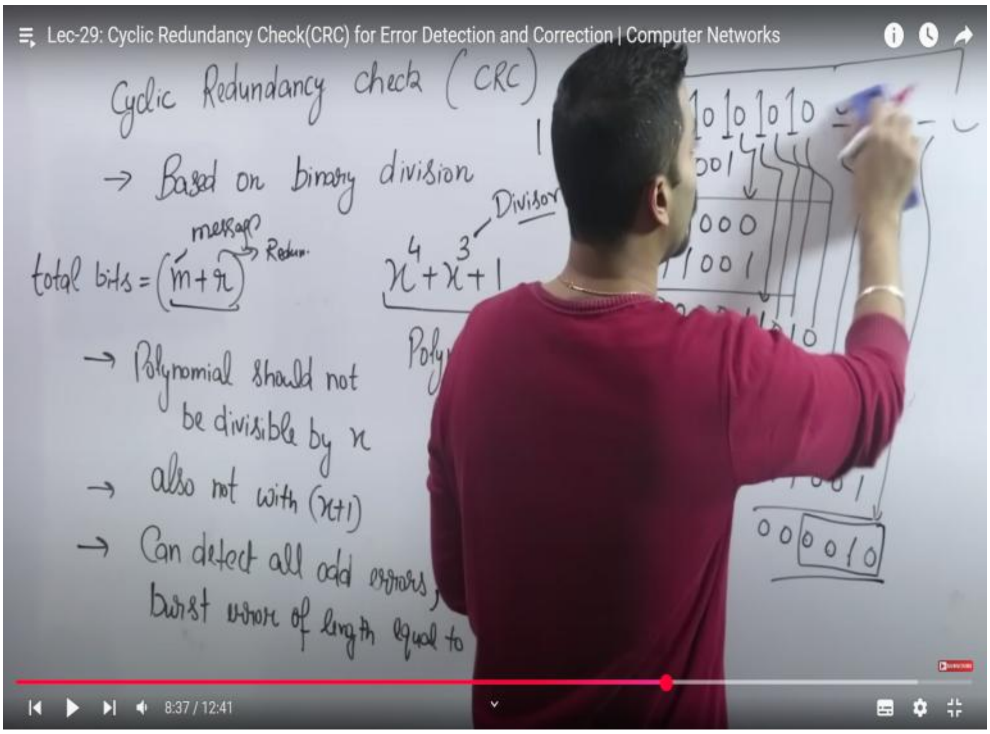


SINGLE BIT PARITY CHECK IS USED FOR THE ERROR DETECTION AS WELL AS THE ERROR CONTROL

WE WILL SEND THE DATA VY EVEN PARITY OR THE ODD PARITY

IF EVEN PARITY THEN THE NO OF THE DATA WORDS ARE ARE EVEN OTHERWISRE IT GIVES ERROR

CYCLIC REDANDENCY CHECK (CRC)



Example Walkthrough

Given:

- Data: 11010011101100
- Generator Polynomial: 1011 (degree = 3)

Steps:

1. **Append Zeros (JITANI DEGREE HAI UTNA)**
   Padded Data = 11010011101100000
2. **Perform Division**
   - Divide 11010011101100000 by 1011 using XOR.
   - Obtain the remainder (e.g., 100).
3. **Append Remainder**
   Transmitted Frame = 11010011101100100
4. **Receiver Verification**
   - Divide the received frame 11010011101100100 by 1011.
   - If the remainder is 0, the data is valid.

HAMMING CODE FOR ERROR DETECTION

Steps to Generate Hamming Code

1. Determine the Number of Parity Bits

- Let mmm be the number of data bits, and rrr be the number of parity bits.
- The total number of bits in the encoded data is n=m+rn = m + rn=m+r.
- rrr is chosen such that 2r≥m+r+12^r \geq m + r + 12r≥m+r+1.

2. Position the Parity Bits

- Place the parity bits in positions that are powers of 2: 1,2,4,8,…1, 2, 4, 8, \dots1,2,4,8,….
- Example: For 7 data bits, the positions of the parity bits are P1,P2,P4,P8P_1, P_2, P_4, P_8P1,P2,P4,P8.

3. Fill the Data Bits

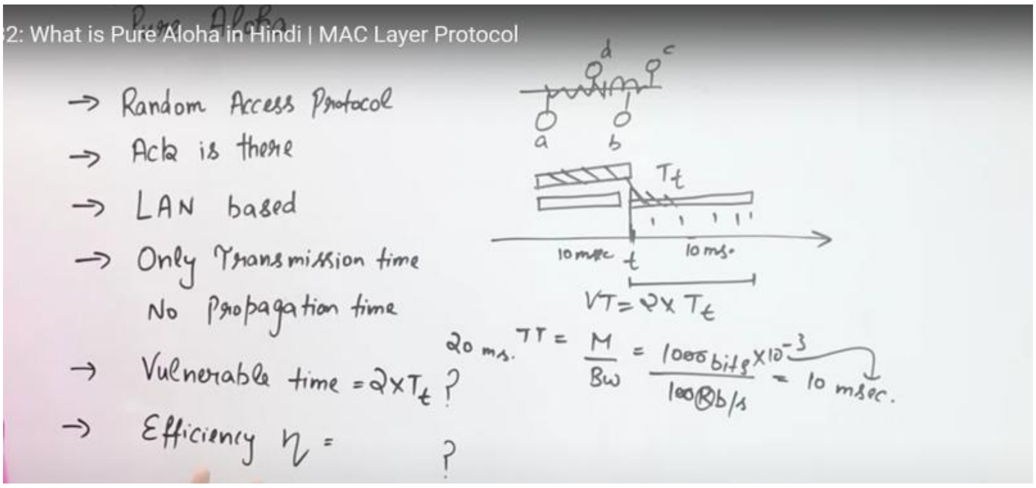
- Place the data bits in the remaining positions.
- Each parity bit PiP_iPi checks specific positions in the data, determined by the binary representation of the positions.
- Rule: A parity bit at position 2k2^k2k checks all bit positions where the kthk^{th}kth bit of the position (in binary) is 1.
- Use even parity (or odd parity, depending on the protocol):
  - **Even parity**: Ensure the total number of 1s (including the parity bit) is even.
  - **Odd parity**: Ensure the total number of 1s (including the parity bit) is odd.

4. Calculate the Parity Bits

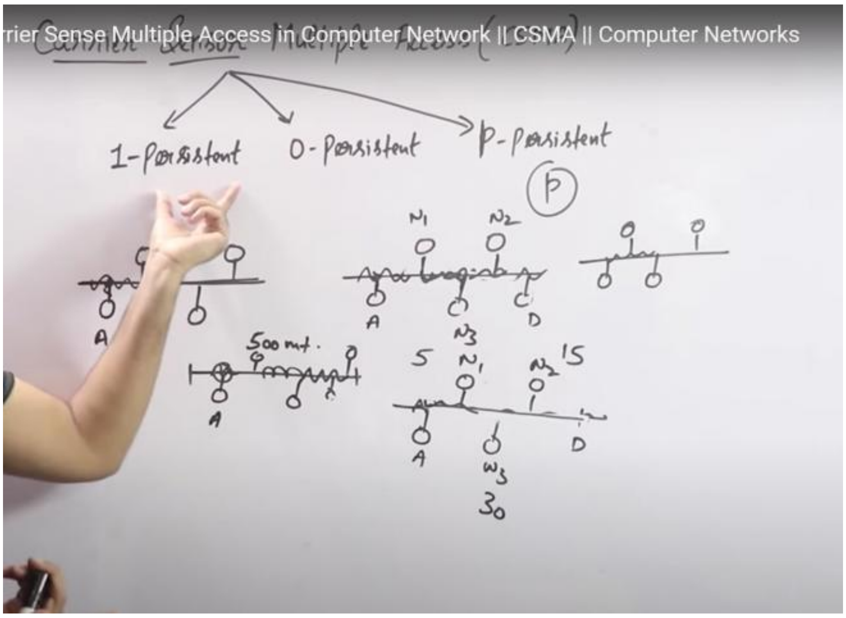
+-

Various Medium Access Control Protocols in Data Link Layer

DATA LINK LAYER HAS MAINLY TWO LAYERS **LLC (LOGICAL LAYER CONTROL) AND MAC (MULTIPLE ACCESS CONTROL)**



CSMA



-
- O-PERSISTANT:-

- When a device detects that the medium is idle, it does **not transmit immediately**.
- Instead, it waits for a random amount of time before checking again.

- **1-PERSISTANT**

- When a device detects the medium is idle, it transmits **immediately** without any delay.
- If the medium is busy, it continuously senses the medium until it becomes idle.

- **P-PERSISTANT**

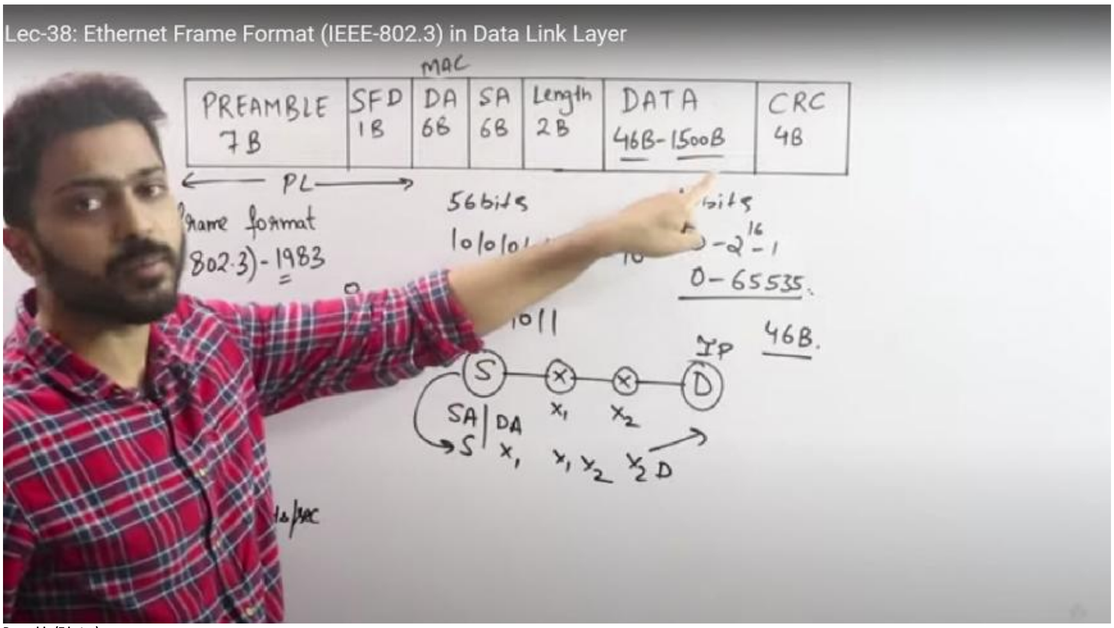
- This approach is used in **time-slotted systems**.
- When the medium becomes idle, a device transmits with a probability PPP.
- If it does not transmit (1−P1 - P1−P), the device waits for the next time slot and repeats the process.

to control access to a shared communication medium. It ensures that multiple devices can transmit data over the same network channel without interfering with each other.

In **CSMA**, before a device transmits data, it first **senses** (listens to) the channel to check if it is free (i.e., whether it is currently being used by another device). If the channel is clear, the device can transmit; if the channel is busy, the device waits until it is free.

- **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**: Used in Ethernet networks, devices detect if a collision occurs during transmission and stop transmitting if one is detected. After that, they back off for a random amount of time before attempting to retransmit.
- NO ACK
- ISME APAN APNE GHAR KE SAMNE KA DEKH SAKTE HAI USKE WAJA SE COLLISION KE CHANCES JADA HOTE HAI
- USED IN WIRED NETWORK
- **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**: Commonly used in wireless networks (e.g., Wi-Fi), CSMA/CA minimizes the chance of collision by waiting for a clear channel and using mechanisms like ACKs (acknowledgments) to confirm successful transmissions.
- USED IN THE WIRELESS NETWORK

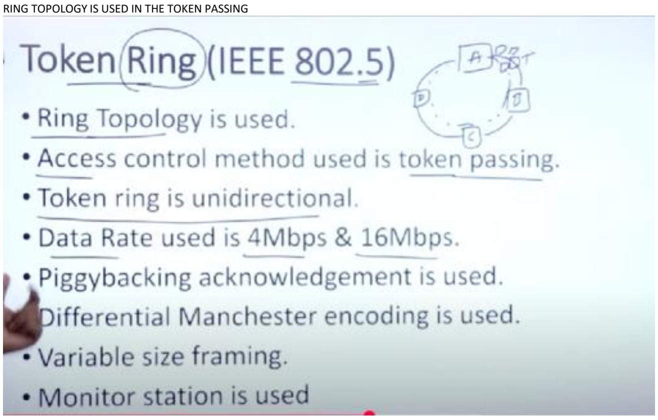
Ethernet Frame Format (IEEE-802.3) in Data Link Layer



- **Preamble (7 bytes):**
  - Contains a sequence of alternating 1s and 0s (101010...) used to synchronize the receiver's clock with the sender's clock.
- **Start of Frame Delimiter (SFD) (1 byte):**
  - Marks the end of the preamble and the start of the frame. Its value is 10101011.
- **Destination MAC Address (6 bytes):**
  - Specifies the MAC address of the device the frame is being sent to.
  - Can be a unicast, multicast, or broadcast address.
- **Source MAC Address (6 bytes):**
  - Specifies the MAC address of the device sending the frame.
- **Length/Type (2 bytes):**
  - **Length**: Specifies the length of the payload if the value is ≤ 1500 bytes.
  - **Type**: Specifies the protocol type (e.g., IPv4, IPv6) if the value is ≥ 1536 (0x0600 in hex).
- **Payload (Data) (46–1500 bytes):**
  - Contains the actual data being transmitted.
  - The size must be at least 46 bytes. If the payload is smaller, padding bytes are added.
- **Frame Check Sequence (FCS) (4 bytes):**
  - Provides error checking using a Cyclic Redundancy Check (CRC).
  - The receiver uses the FCS to verify the integrity of the frame.

Token Ring (IEEE 802.5)

UNI-DEIRECTION
RING TOPOLOGY IS USED IN THE TOKEN PASSING



NETWORK LAYER
CLASSFUL ADDERESING

- **CLASS A**
- The first octet (8 bits) ranges from 1.0.0.0 to 126.0.0.0.
- The full range of Class A IP addresses spans from 1.0.0.0 to 126.255.255.255.

Reserved Addresses:
  - 0.0.0.0 is reserved as a default route.
  - 127.0.0.0 to 127.255.255.255 are reserved for loopback testing and diagnostics.

Network and Host Division:
  - The first octet (8 bits) represents the **network ID**.
  - The remaining three octets (24 bits) represent the **host ID**.
  - This allows for a maximum of 27−2=1262^{7} - 2 = 12627−2=126 networks (excluding the reserved addresses 0 and 127).
  - Each network can have 224−2=16,777,2142^{24} - 2 = 16,777,214224−2=16,777,214 hosts (excluding the network and broadcast addresses).

GOOGLE SERVER IP :- 64.0.0.0

CLASS B

FIRST TWO -->NETWORK AND OTHER HOST

Address Range
  - **Default range:** 128.0.0.0 to 191.255.255.255
  - The first two octets (16 bits) represent the **network ID**, while the remaining two octets (16 bits) represent the **host ID**.

2. Subnet Mask
  - Default subnet mask: **255.255.0.0**
  - This means the first 16 bits are used for the network portion, and the last 16 bits are for hosts.

3. Number of Networks and Hosts
  - **Number of networks:** 16,384 (2^14)
  - **Hosts per network:** 65,536 (2^16) minus 2 (for network and broadcast addresses), so 65,534 usable addresses.

CLASS C

1. Address Range
  - **Default range: 192.0.0.0 to 223.255.255.255**
  - The first three octets (24 bits) represent the **network ID**, while the last octet (8 bits) represents the **host ID**.

2. Subnet Mask

- **Default subnet mask: 255.255.255.0**
- This means the first 24 bits are used for the network portion, and the last 8 bits are used for hosts.

3. Number of Networks and Hosts

- **Number of networks:** 2,097,152 (2^21)
- **Hosts per network:** 256 (2^8) minus 2 (for network and broadcast addresses), so **254 usable addresses per network.**

CLASS D

Address Range

- **Default range: 224.0.0.0 to 239.255.255.255**
- These addresses are used to deliver packets to a group of devices rather than a single device (multicast communication).

USED IN MULTICAST ADDRESSING

Key Characteristics

- **No Subnet Mask:** Class D does not have a default subnet mask since it does not divide into networks and hosts like Class A, B, or C.
- **Not for Standard Communication:** Devices in a multicast group do not have unique identifiers within the multicast address; instead, they all listen to the sam e group address.

The 5 Address Classes (A to E)

Class	Starting Bits	Range	Default Subnet Mask	Use
A	0xxxxxxx	1.0.0.0 to 126.0.0.0	255.0.0.0	Large networks (many hosts)
B	10xxxxxx	128.0.0.0 to 191.255.0.0	255.255.0.0	Medium networks
C	110xxxxx	192.0.0.0 to 223.255.255.0	255.255.255.0	Small networks (few hosts)
D	1110xxxx	224.0.0.0 to 239.255.255.255	N/A	Multicasting
E	1111xxxx	240.0.0.0 to 255.255.255.255	N/A	Reserved (research)

Class A

- **Range: 0.0.0.0 to 127.255.255.255**
- **Subnet Mask: 255.0.0.0**
- **Network ID Bits:** 8 bits
- **Host ID Bits:** 24 bits
- **Number of Networks:** 128 (2^7)
- **Number of Hosts per Network:** 16,777,214 (2^24 − 2)
- **Purpose:** Large networks like ISPs and large organizations.
- **First Bit Pattern:** Starts with 0.

Class B

- **Range: 128.0.0.0 to 191.255.255.255**
-
- **Subnet Mask: 255.255.0.0**
- **Network ID Bits:** 16 bits
- **Host ID Bits:** 16 bits
- **Number of Networks:** 16,384 (2^14)
- **Number of Hosts per Network:** 65,534 (2^16 − 2)
- **Purpose:** Medium-sized networks such as universities and corporations.
- **First Bit Pattern:** Starts with 10.

Class C

- **Range: 192.0.0.0 to 223.255.255.255**
- **Subnet Mask: 255.255.255.0**
- **Network ID Bits:** 24 bits
- **Host ID Bits:** 8 bits
- **Number of Networks:** 2,097,152 (2^21)
- **Number of Hosts per Network:** 254 (2^8 − 2)
- **Purpose:** Small networks, such as LANs (Local Area Networks).
- **First Bit Pattern:** Starts with 110.

Class D

- **Range: 224.0.0.0 to 239.255.255.255**
- **Subnet Mask:** Not applicable.
- **Used For: Multicasting** (sending packets to a group of devices).
- **Number of Networks/Hosts:** Not assigned to individual hosts.
- **Purpose:** Applications like live streaming, online gaming, and routing protocols.
- **First Bit Pattern:** Starts with 1110.

Class E

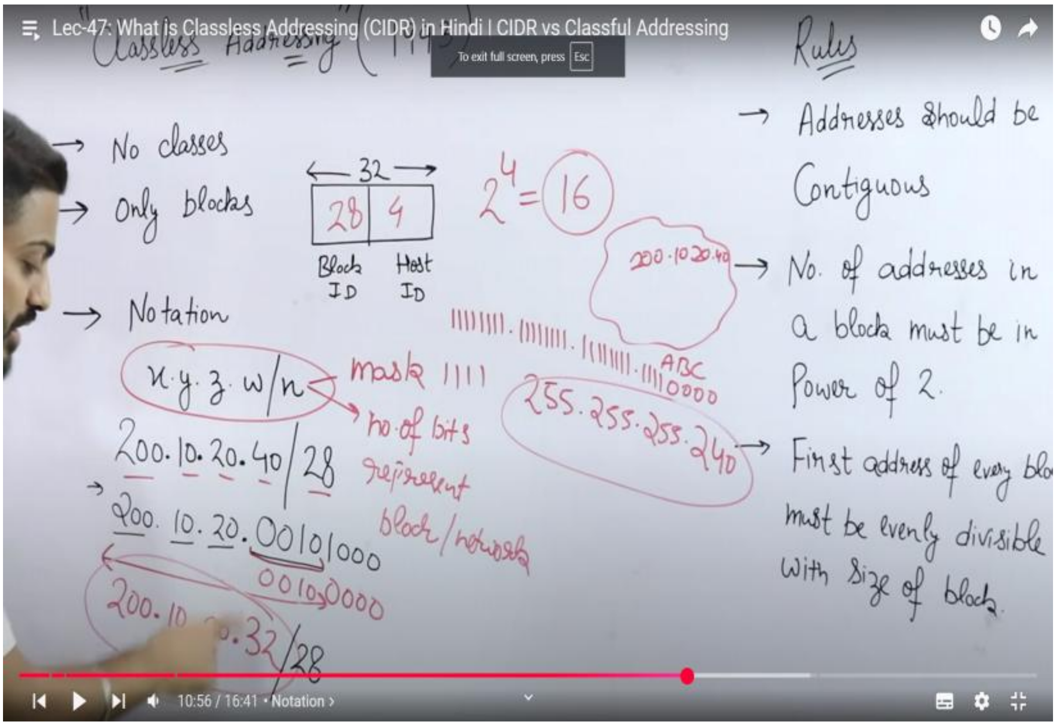
- **Range: 240.0.0.0 to 255.255.255.255**
- **Subnet Mask:** Not applicable.
- **Used For: Experimental and research purposes.**
- **Number of Networks/Hosts:** Reserved; not used for regular communication.
- **Purpose:** Future use and experimentation.
- **First Bit Pattern:** Starts with 1111.

LIMITED BROADCAST ADDRESS :- 255.255.255.255
DIRECT BROADCAST ADDRESS :- (LAST ADDRESS) ALLTHE ADDRESS HAS RESERVE THE LAST ADDRESS FOR DIRECT BROADCASTING
Disadvantage :-

1.wastage of ip address
2.lack of scalability
3.lack of flexibility

classless

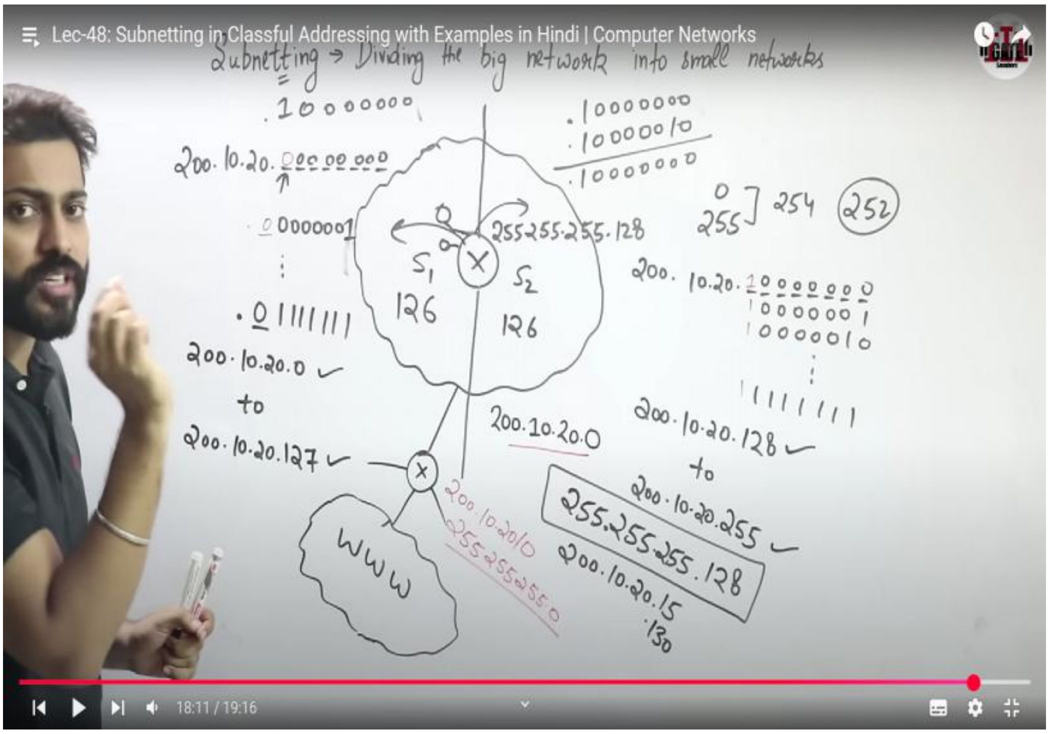
JITNA USER BOLENGA UTNA USKO ALLOT KIYA JAYENGA
NO CLASSES
ONLY BLOCK
/N -->MASK (NO OF BITS REPRESENT BLOCK/NETWORK)

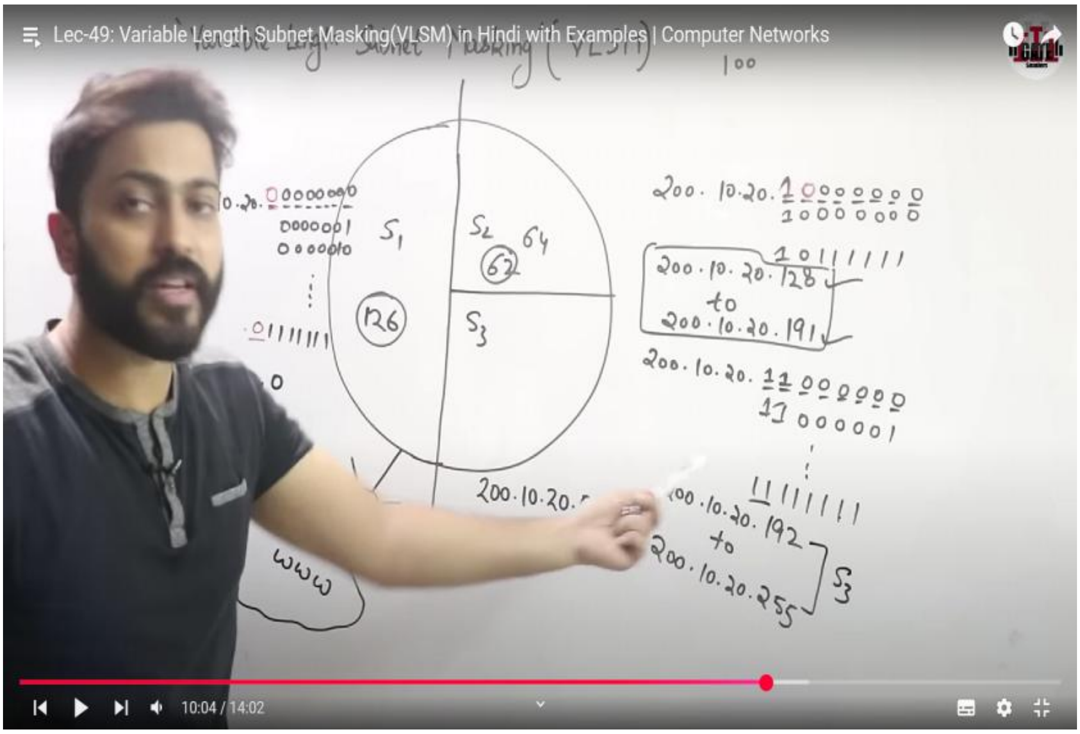


Subnetting is the process of dividing a large network into smaller, more manageable subnetworks (or subnets). It helps in efficient IP address management, better security, and reduced network traffic congestion.
For 192.168.1.0/24

- 192.168.1 is the network part.
- 0 is the host part (can range from 1 to 254 for 254 devices).

1. **Subnet Mask**:
   A subnet mask determines how much of an IP address is for the network and how much is for hosts.
   - For /24 (255.255.255.0), 24 bits are for the network, and the remaining 8 bits are for hosts.
2. **Creating Subnets**:
   - Borrow bits from the host part to create smaller subnets.
   - For instance, if you borrow 2 bits, you can create 22=42^2 = 422=4 subnets.



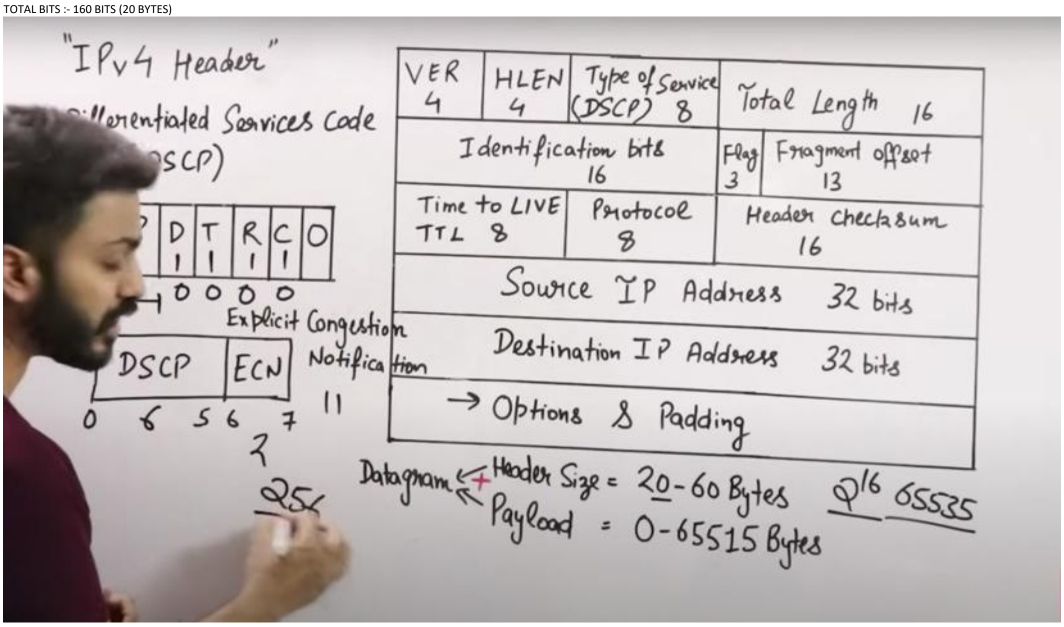


IPV4 HEADER

CONNECTIONLESS :- USED IN SOURCE TO DESTINATION TRANSMISSION

DATAGRAM SERVICE :- IT CAN BE GO FROM ANY PATH
datagram refers to a basic unit of data that is independently sent over a network. It is a self-contained packet that carries enough information for it to be routed from the source to the destination without relying on prior exchanges between the two endpoints or state information maintained by the network.

DATAGRAM = HEADER(20-60) + PAYLOAD (0-65515)
TOTAL FIELDS :- 13
MANDETORY FIELDS :- 12
TOTAL BITS :- 160 BITS (20 BYTES)



IPv4 Header Format

1. **Version (4 bits)**
   - Indicates the IP version being used. For IPv4, the value is 4.
2. **Internet Header Length (IHL) (4 bits)**
   - Specifies the length of the header in 32-bit words. Minimum value is 5 (20 bytes), and the maximum is 15 (60 bytes).
3. **Type of Service (TOS) / Differentiated Services (8 bits)**
   - Helps in prioritizing packets. It includes:
     - **DSCP (6 bits):** Differentiated Services Code Point for Quality of Service (QoS).
     - **ECN (2 bits):** Explicit Congestion Notification for congestion control.
4. **Total Length (16 bits)**
   - Indicates the total size of the IP packet, including the header and data. Maximum size: 65,535 bytes.
5. **Identification (16 bits)**
   - A unique value used to identify fragments of the same packet.
6. **Flags (3 bits)**
   - Control fragmentation:
     - **Bit 0 (Reserved):** Always set to 0.
     - **DF (Don't Fragment):** 1 if fragmentation is not allowed.
     - **MF (More Fragments):** 1 if more fragments follow.
7. **Fragment Offset (13 bits)**
   - Specifies the position of the fragment in the original packet. Measured in 8-byte blocks.
8. **Time to Live (TTL) (8 bits)**
   - Limits the packet's lifetime. Decreases by 1 at each hop; when it reaches 0, the packet is discarded.
9. **Protocol (8 bits)**
   - Identifies the protocol used in the data portion of the IP packet (e.g., 6 for TCP, 17 for UDP).
10. **Header Checksum (16 bits)**
    - A checksum for error-checking the header. Ensures integrity during transmission.
11. **Source Address (32 bits)**
    - IP address of the sender.
12. **Destination Address (32 bits)**
    - IP address of the receiver.
13. **Options (Variable, optional)**
    - Used for special features like record route, source routing, or timestamping. The field is optional and may not always be present.
14. **Padding (Variable)**

- Extra bytes added to make the header a multiple of 32 bits if options are present.

IPV6

Address Length and Format
- IPv4: Utilizes a 32-bit address scheme, allowing for approximately 4.3 billion unique addresses. Addresses are written in decimal format, typically as four octets separated by dots (e.g., 192.168.1.1).
- IPv6: Employs a 128-bit address scheme, which supports an astronomical number of unique addresses (about 3.4×10^{38} 3.4×10^{38}). IPv6 addresses are represented in hexadecimal format, consisting of eight groups of four hexadecimal digits separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Header Complexity
- IPv4: The header size can vary from 20 to 60 bytes and includes several fields such as checksum and options, which can complicate processing.
- IPv6: Has a fixed header size of 40 bytes with a simplified structure, making it more efficient for routers to process packets.

Security Features
- IPv4: Security features are not built into the protocol; they rely on external applications for encryption and authentication
- IPv6: Incorporates security features directly into the protocol with mandatory support for IPsec, providing encryption and authentication capabilities.

Fragmentation Handling
- IPv4: Both the sender and intermediate routers can perform fragmentation of packets.
- IPv6: Fragmentation is handled only by the sender, which reduces the processing load on routers.

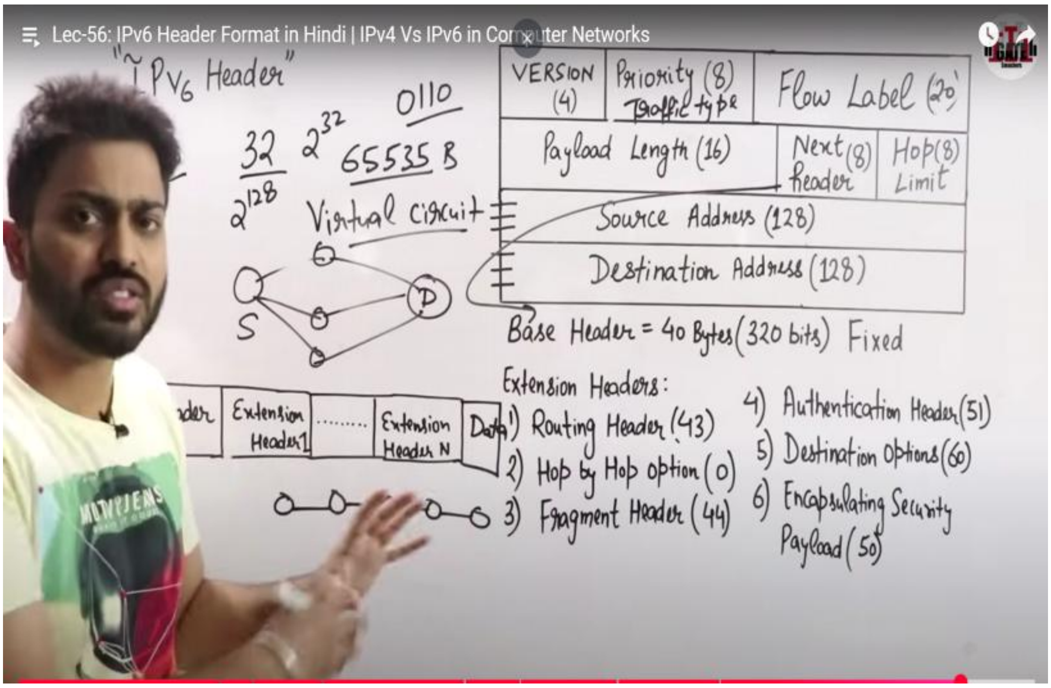
Address Configuration
- IPv4: Supports manual configuration and DHCP (Dynamic Host Configuration Protocol) for address assignment.
- IPv6: Supports automatic address configuration through Stateless Address Autoconfiguration (SLAAC) as well as DHCPv6 for more controlled environments.

Transmission Methods
- IPv4: Uses a broadcast method for packet transmission, where packets are sent to all devices on a network.
- IPv6: Eliminates broadcast in favor of multicast and anycast methods, which target specific groups or individual devices, thereby reducing unnecessary network traffic.

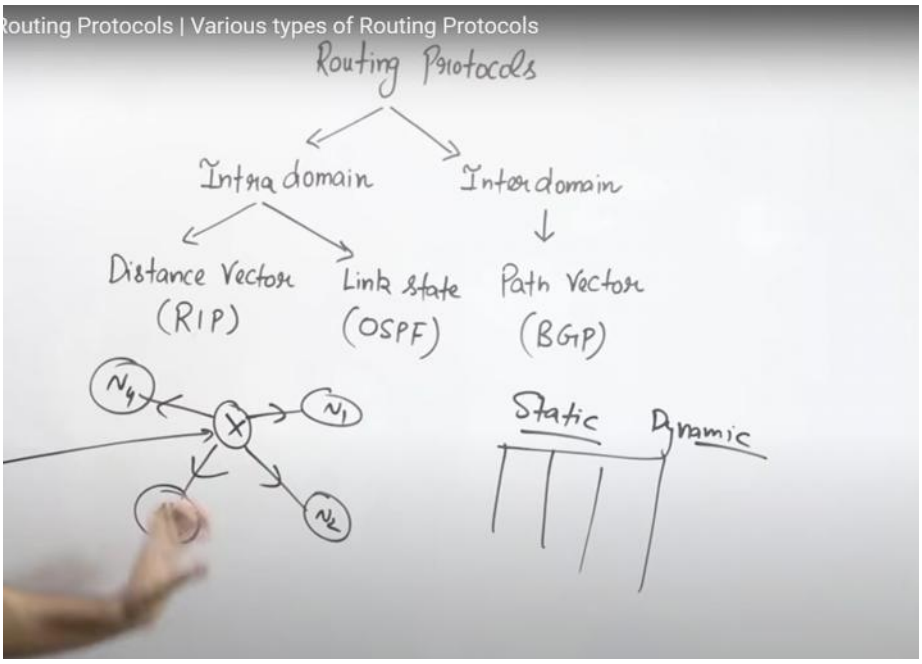
Checksum Field
- IPv4: Includes a checksum field in its header to verify data integrity.
- IPv6: Does not have a checksum field, relying instead on upper-layer protocols to ensure data integrity.

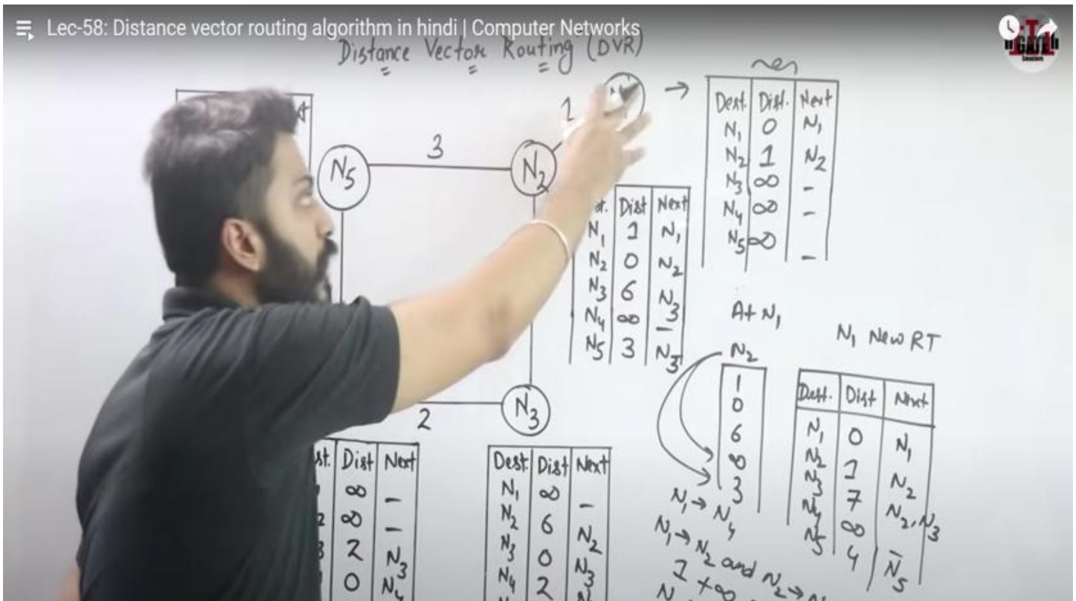
Classes of Addresses
- IPv4: Divided into multiple classes (A, B, C, D, E) based on the size and purpose of the network.
- IPv6: Does not use classes; instead, it allows for more flexible addressing without predefined categories.

From <https://www.perplexity.ai/search/what-is-diffreences-between-ip-7U1F4IlBSCuQnsOuHjLceQ>



ROUTING PROTOCOL :-





TCP & UDP

TCP CREATE THE CONNECTION BEFORE TRANSMISSION BUT UDP IS NOT CRETAE THE CONNECTION BEFORE SENDING DATA

UDP HAS NOT GUARANTEE THAT IT WILL REACH TO DESTINATION

. UDP also doesn't ensure the order of delivery or protect against duplicate packets12

Low Overhead: Because it doesn't require handshaking or error-checking mechanisms, UDP has lower overhead, making it faster and more efficient for certain applications2.

USED IN LIVE STREAMING , VEDIO CALLS

HTTP PROTOCL :-

HTTP stands for **Hypertext Transfer Protocol**. It's a foundational protocol used for data communication on the World Wide Web. Here are some key points about HTTP:

1. **Client-Server Model**: HTTP operates on a client-server model. The client, usually a web browser, sends a request to the server, which then responds with the requested resource, such as an HTML document, image, or video12.
2. **Stateless Protocol**: Each HTTP request is independent of others.
3. This means the server does not retain any information about previous requests from the same client12.
4. **Methods**: HTTP defines several request methods, the most common being:
- **GET**: Requests data from a specified resource.
- **POST**: Submits data to be processed to a specified resource.
- **PUT**: Updates a current resource with new data.
- **DELETE**: Removes the specified resource12.
5. **Status Codes**: HTTP responses include status codes to indicate the result of the request. Common status codes include:
- **200 OK**: The request was successful.
- **404 Not Found**: The requested resource could not be found.
- **500 Internal Server Error**: The server encountered an error12.
6. **Secure Version (HTTPS)**: HTTPS is the secure version of HTTP, where communications are encrypted using Transport Layer Security (TLS). This ensures data privacy and integrity12.

HTTP has evolved over time, with versions like HTTP/1.1, HTTP/2, and the latest HTTP/3, each bringing improvements in performance and security12.

Modem (Modulator-Demodulator)

A **modem** is a device that converts digital data from a computer into analog signals that can be transmitted over telephone lines or other analog media, and vice versa.

SONET (Synchronous Optical Networking)

SONET is a standardized protocol used to transfer multiple digital bit streams over optical fiber using lasers or LEDs.

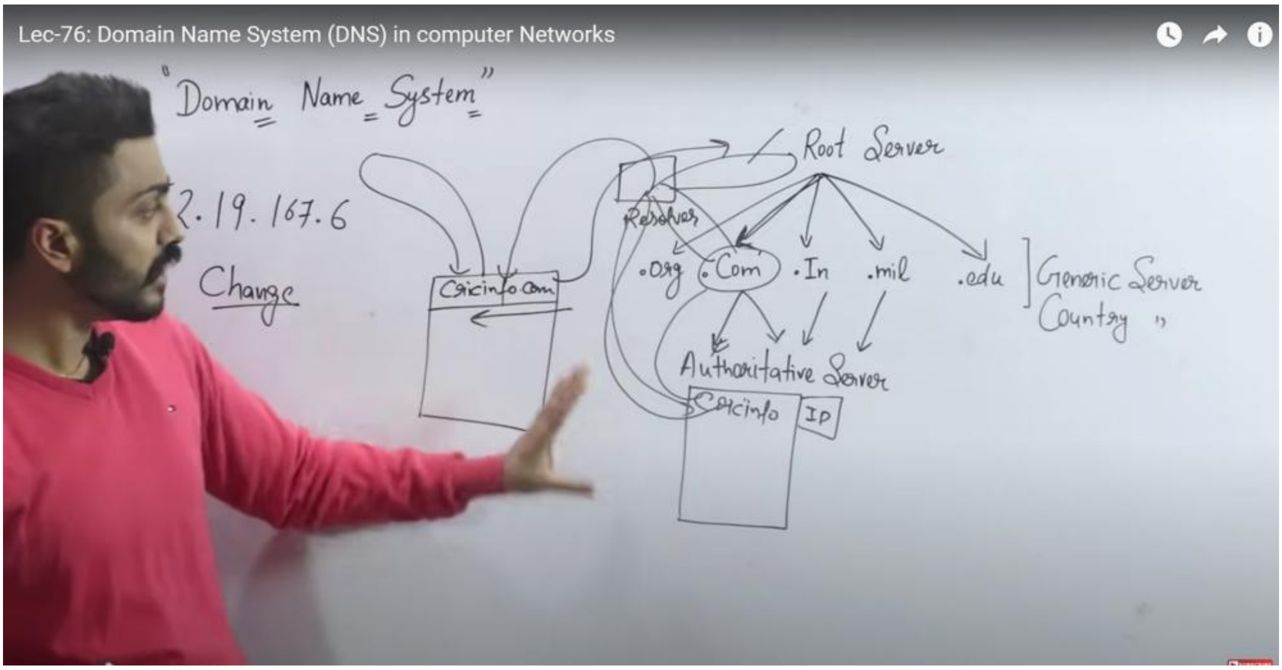
ROUTER LIVES IN NETWORK LAYER

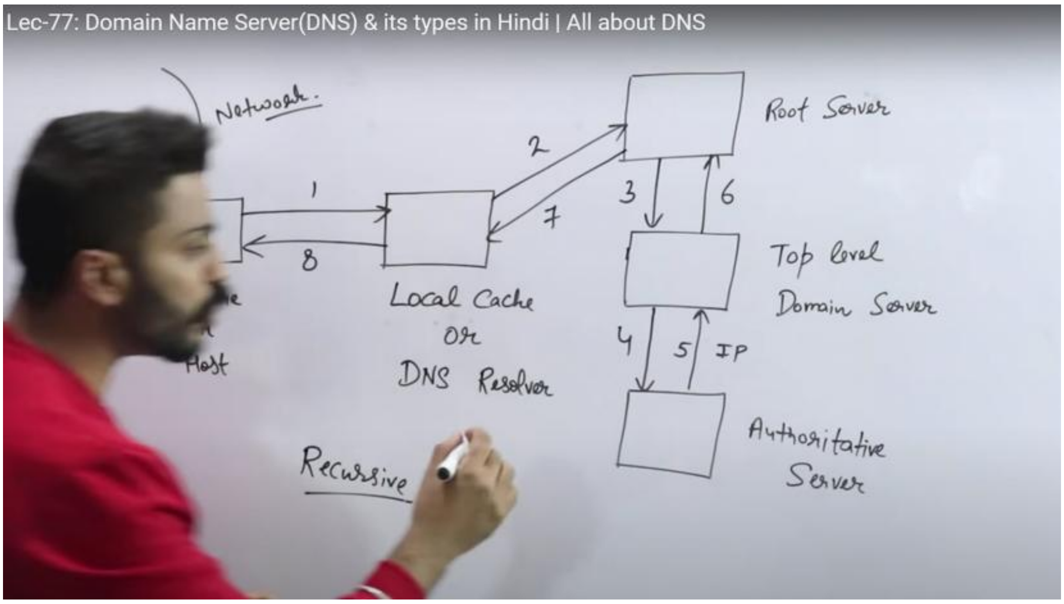
A **socket** is an endpoint for communication between two devices over a network. It acts as an interface between the application layer and the transport layer, enabling data exchange between programs running on different computers or even within the same system.

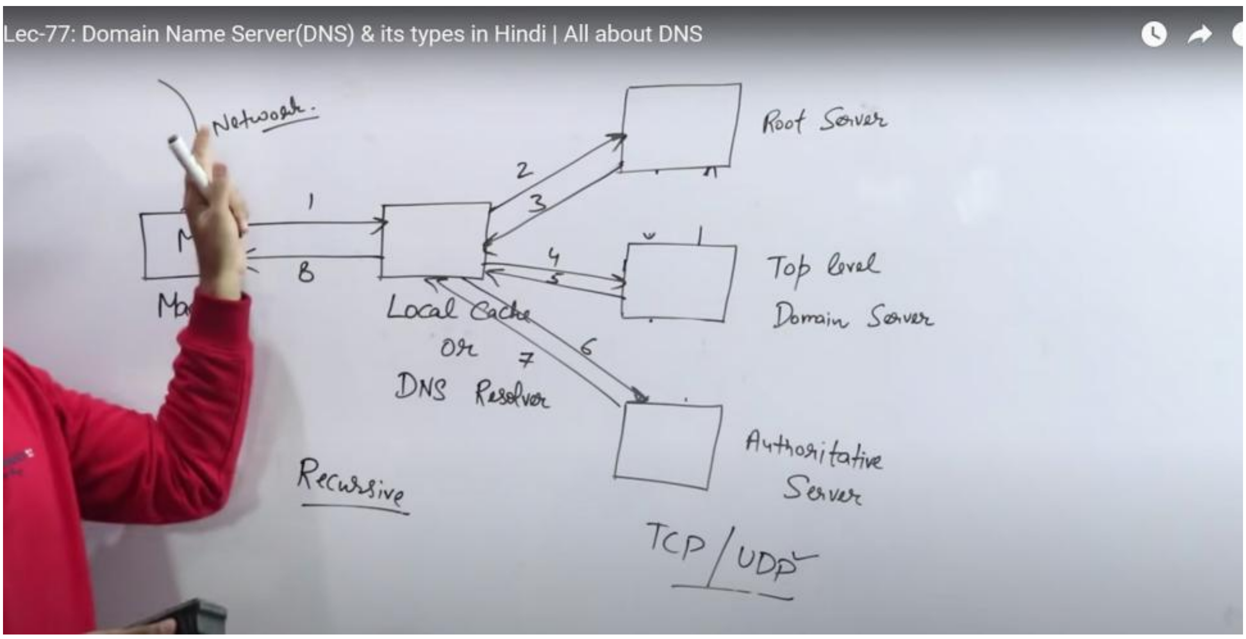
Socket Addressing

A socket is identified by:
- **IP Address** (e.g., 192.168.1.1)
- **Port Number** (e.g., 8080)

RESOLVER --> ROOT SERVER --> RESOLVER-->COMMERCIAL (.COM) --> AUTHORIATIVE SEREVR (CONTAINS THE TABLE WEBSITE NAME AND THE IP ADDRESS)
FIRST REQUEST COMES AT THE RESOLVER THEN IT PASSES TO THE ROOT SERVER







What is DNS?

DNS (**Domain Name System**) is a hierarchical system that translates human-readable domain names (e.g., www.google.com) into IP addresses (e.g., 142.250.183.206) that computers use to communicate over networks like the internet. It acts like a **phonebook** for the internet.

How Name Resolution Happens in DNS?

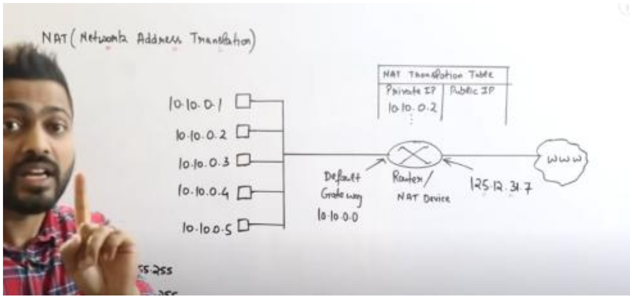
DNS name resolution is the process of converting domain names into IP addresses. The steps involved are:

1. **User Request:** When a user enters a domain name (www.example.com) in a browser, the request is sent to a **recursive DNS resolver** (usually provided by the ISP).
2. **Checking Cache:** The resolver first checks its **cache** to see if it has the IP address stored. If found, it returns the result immediately.
3. **Querying Root Server:** If the resolver doesn't have the record, it contacts a **Root DNS Server**, which directs it to the relevant **TLD (Top-Level Domain) server** (e.g., .com, .org).
4. **Querying TLD Server:** The **TLD DNS server** (e.g., .com server) points the resolver to the **Authoritative Name Server** for example.com.
5. **Querying Authoritative Server:** The **Authoritative DNS Server** holds the actual IP address of www.example.com and returns it to the resolver.
6. **Returning the Result:** The resolver caches the result and sends the IP address back to the user's device, which then connects to the website's serve r.

List of DNS Resource Records and Their Functions:

Record Type	**Function**
A (Address Record)	Maps a domain name to an IPv4 address.
AAAA (IPv6 Address Record)	Maps a domain name to an IPv6 address.
CNAME (Canonical Name Record)	Creates an alias for another domain name.
MX (Mail Exchange Record)	Specifies mail servers for email routing.
NS (Name Server Record)	Specifies the authoritative DNS servers for a domain.
PTR (Pointer Record)	Used for reverse DNS lookup (IP to domain).
SOA (Start of Authority Record)	Stores important domain details like admin email, refresh rate, etc.
TXT (Text Record)	Holds arbitrary text, often used for verification (e.g., SPF, DKIM for email security).
SRV (Service Record)	Specifies location of services (e.g., SIP, LDAP servers).
CAA (Certification Authority Authorization)	Defines which certificate authorities can issue SSL certificates for a domain.

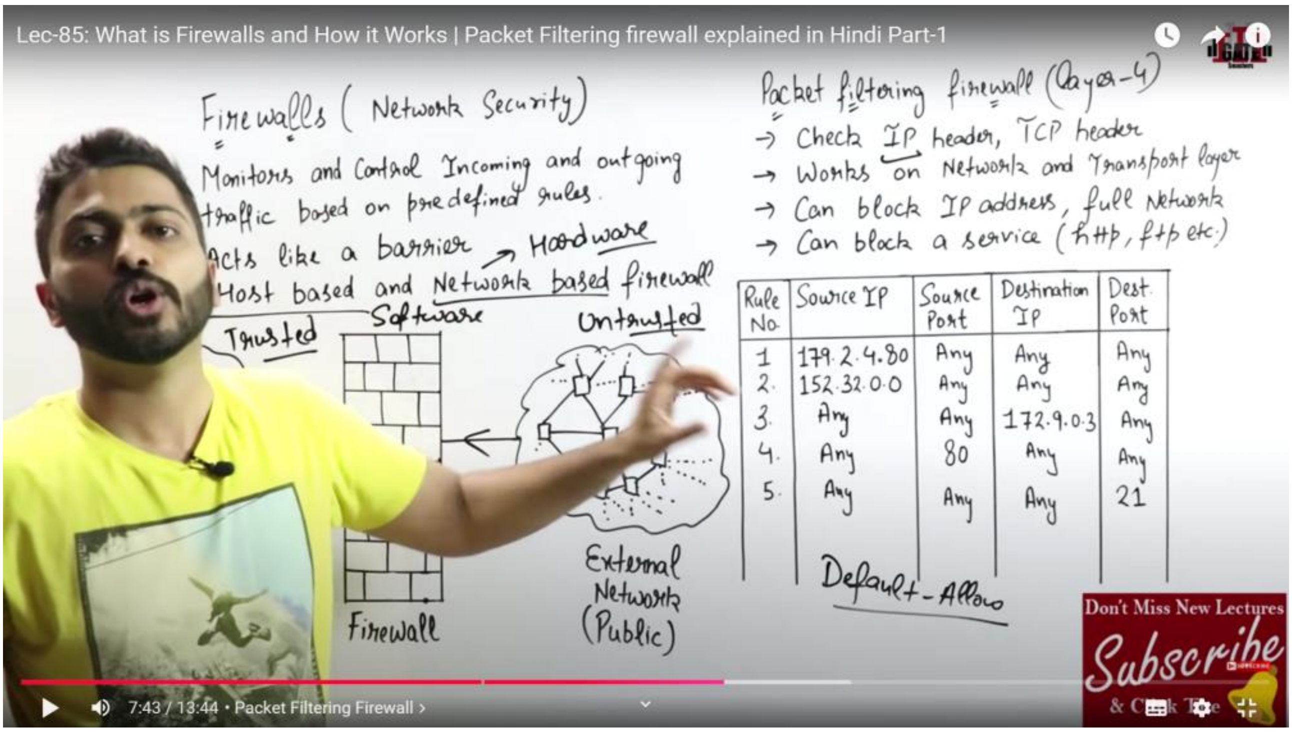
IT USES THE UDP PROTOCOL BECAUSE IT IS FAST



NAT :- USD IN THE UNIVERSITY

EXAMPLE :- IF THERE ARE 4 HOSTELS
IF HOSTEL 1 CONTAINS ROOM NO 101 THEN HOSTEL 2 CAN ALSO CONTAIN ROOM NO 101 THAT IS HOSTEL 1 HAS ITS OWN PRIVATE CONNECTION

THUS NAT IS USED IN THE NETWORK ADDRESS TRANSLATION (PUBLIC TO PRIVATE && PRIVATE TO PUBLIC)

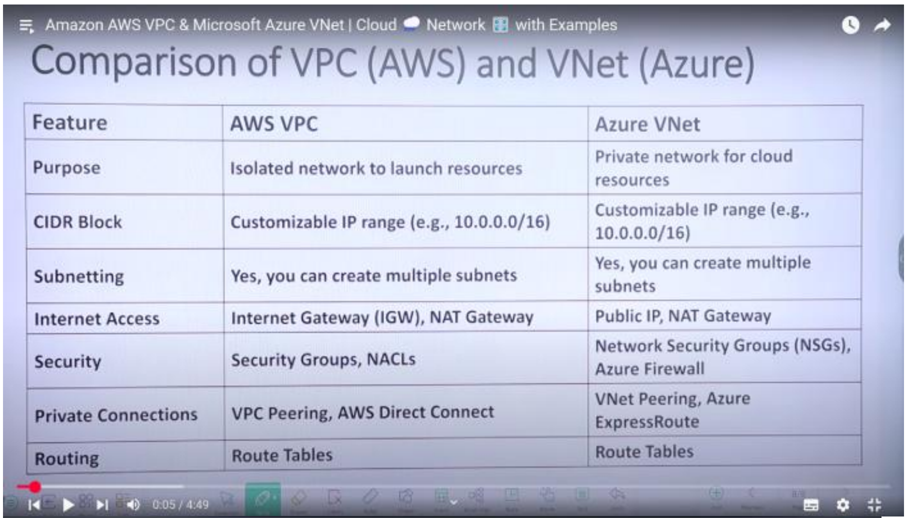


Access Control Lists (ACLs) and **Firewalls** are security mechanisms used to control and restrict network traffic, but they serve different purposes and operate at different levels.

-

A **firewall** is a security system that monitors and controls incoming and outgoing network traffic based on pre-defined security rules. It provides **advanced filtering, stateful inspection, and deep packet analysis**.

An **ACL** is a set of rules that control incoming and outgoing network traffic on a **router** or **switch** by permitting or denying packets based on source/destination IP addresses, ports, or protocols.



Comparison of VPC (AWS) and VNet (Azure)

Feature	AWS VPC	Azure VNet
Purpose	Isolated network to launch resources	Private network for cloud resources
CIDR Block	Customizable IP range (e.g., 10.0.0.0/16)	Customizable IP range (e.g., 10.0.0.0/16)
Subnetting	Yes, you can create multiple subnets	Yes, you can create multiple subnets
Internet Access	Internet Gateway (IGW), NAT Gateway	Public IP, NAT Gateway
Security	Security Groups, NACLs	Network Security Groups (NSGs), Azure Firewall
Private Connections	VPC Peering, AWS Direct Connect	VNet Peering, Azure ExpressRoute
Routing	Route Tables	Route Tables