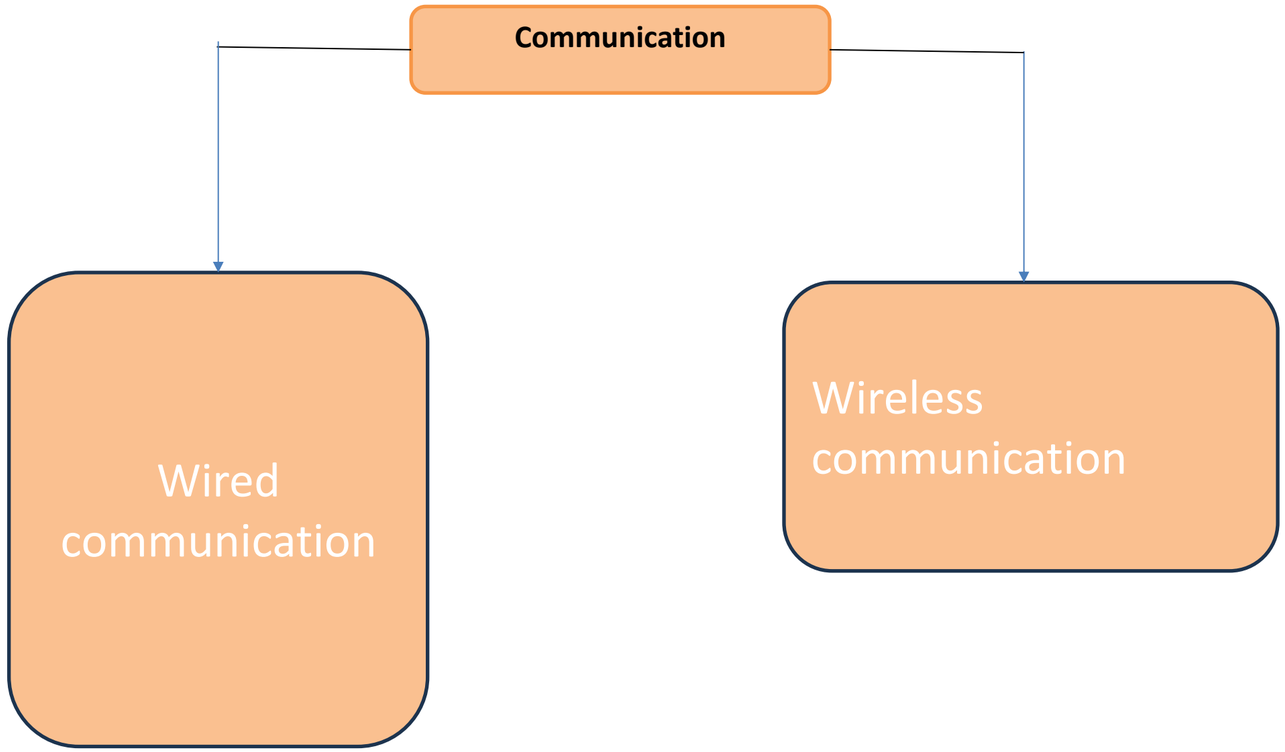
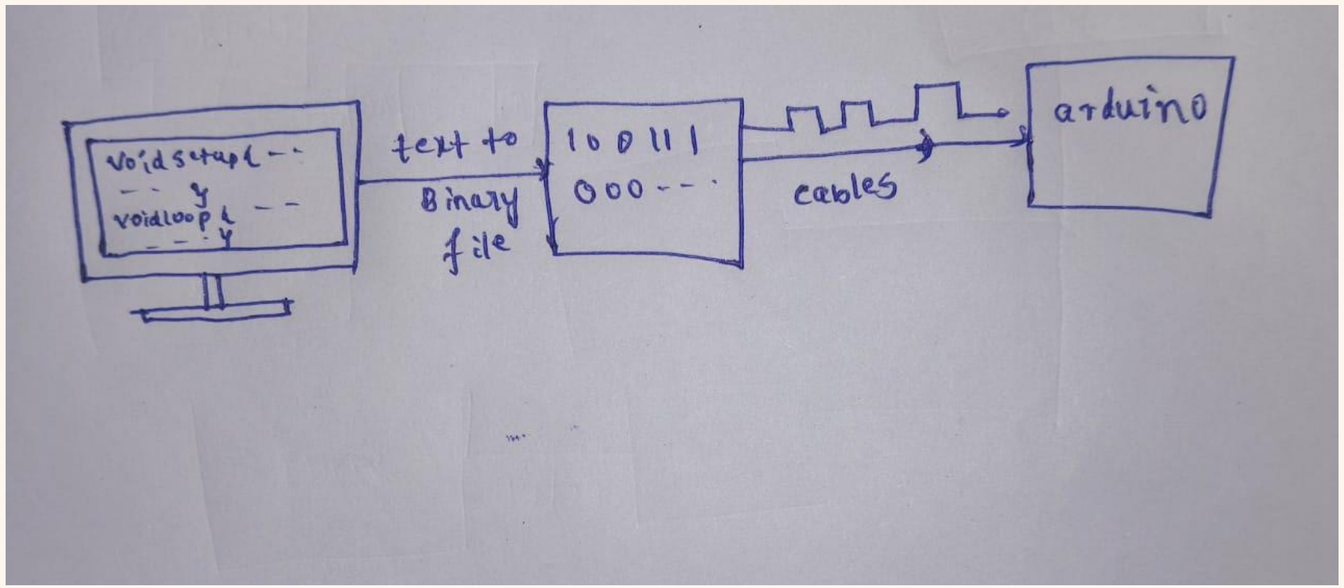
IOT SESSION-2


Communication
Wired communication
Wireless communication

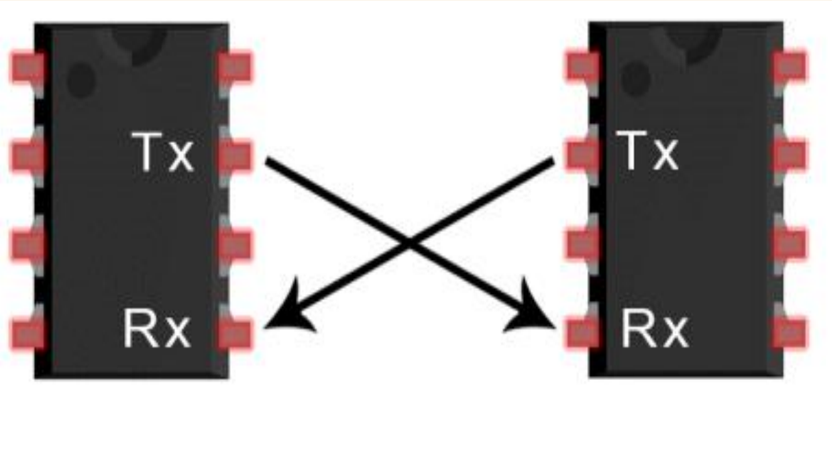
WIRED COMMUNICATION

How it actually happens ?

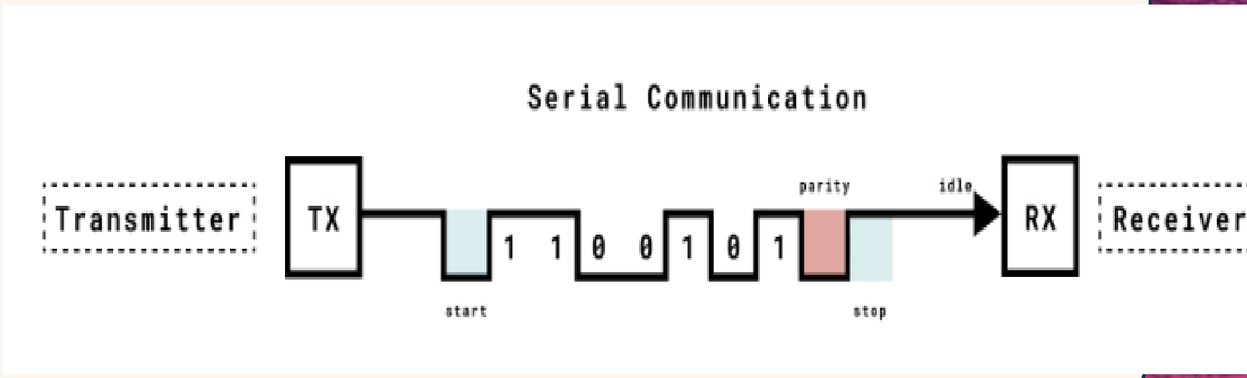
- Lets see how it happens in a simple example of



UART(Universal Asynchronous Receiver-Transmitter)

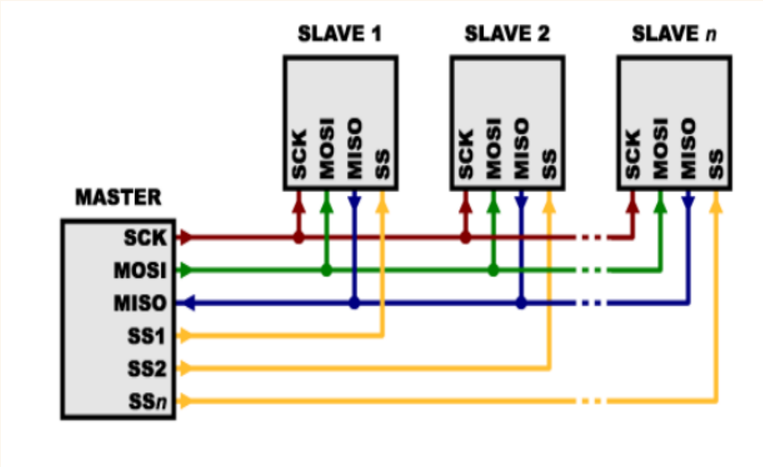


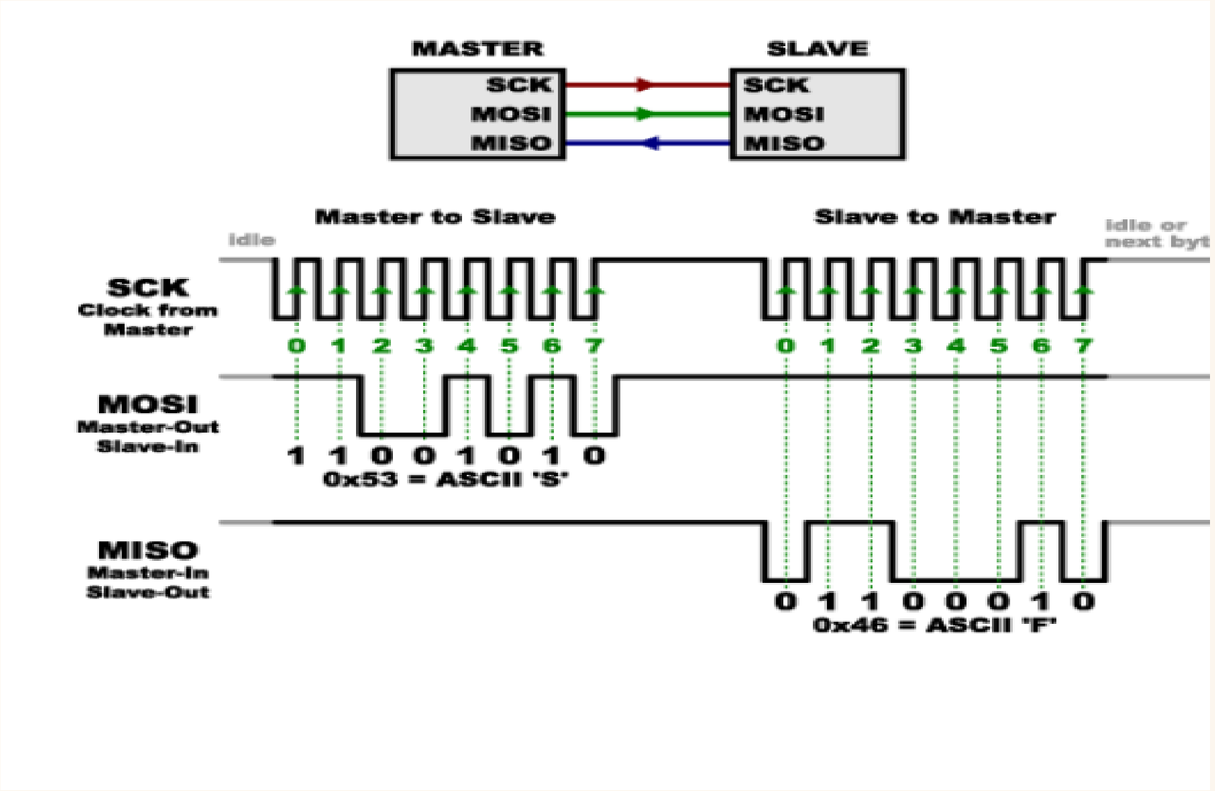
UART operates by transmitting data as a series of bits, including a start bit, data bits, an optional parity bit, and stop bit(s), As the name reveals the protocol operates asynchronous which means that it doesn't rely on a shared clock signal. Instead, it uses predefined baud rates to determine the timing of data bits. The baud rate is specified in bits per second (bps) and represents the number of bits transmitted in one second. In UART, both the transmitting and receiving devices must agree on the same baud rate to ensure successful communication.



SPI(Serial peripheral interface)

Pin Name	Description
MOSI	Master Out Slave In
MISO	Master In Slave Out
SCK	Synchronous Clock
SS	Slave Select (active Low)

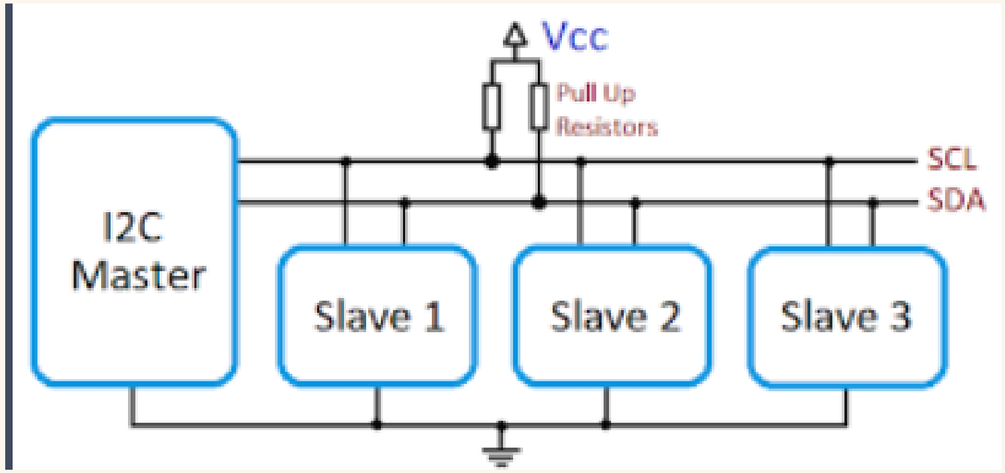


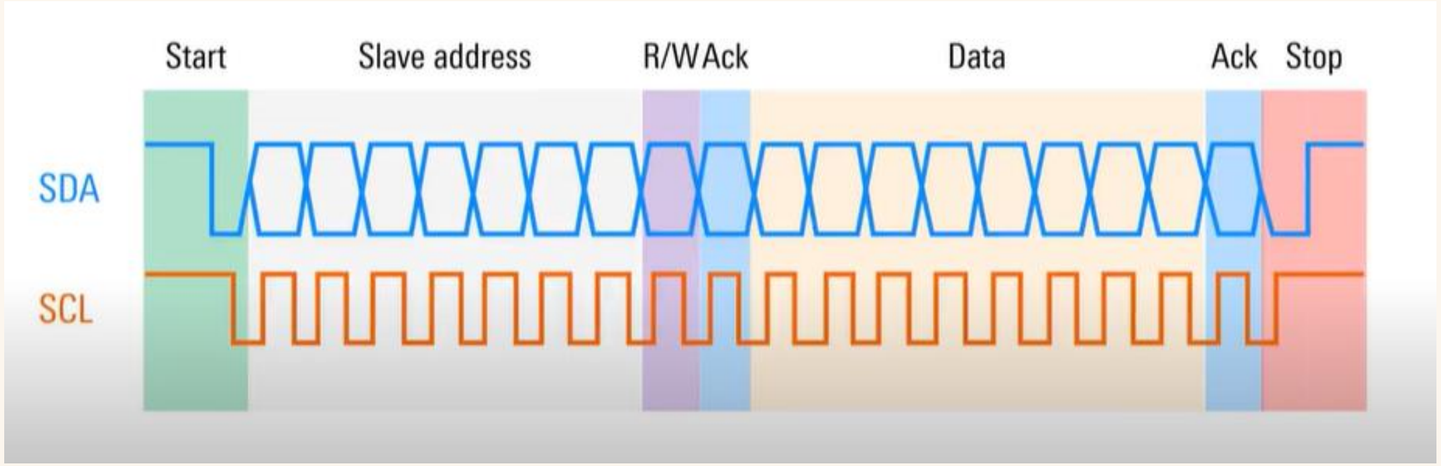


I2C:

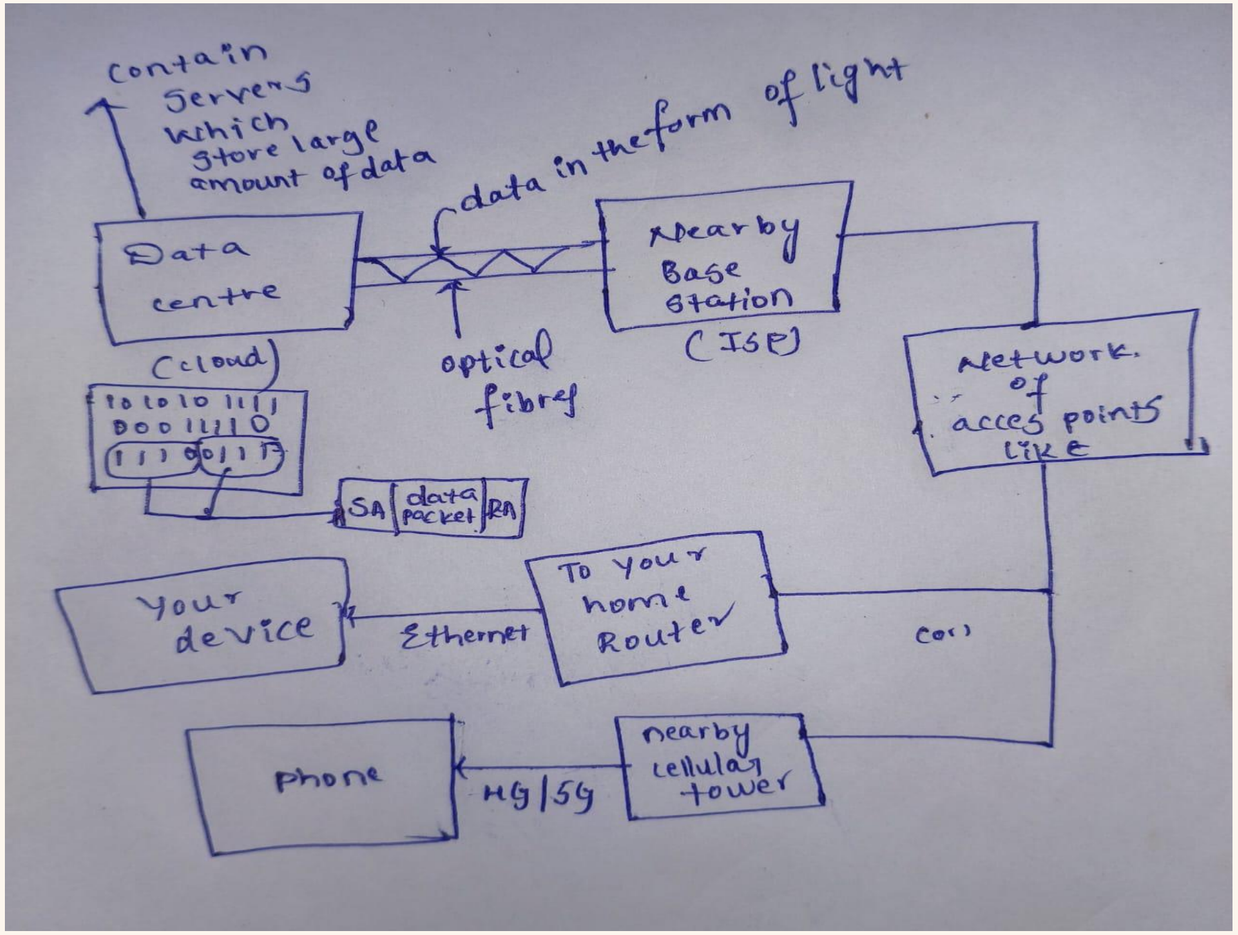
SDA: serial data line

SCL: serial clock signal





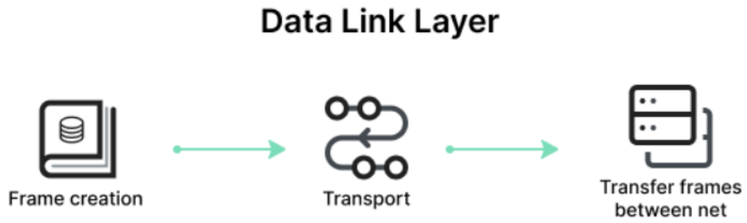
HOW THE INTERNET WORKS :



1. Physical Layer

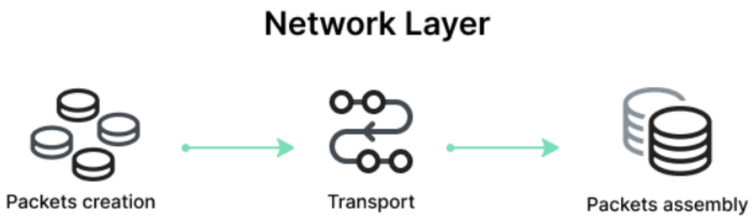
The Physical Layer is responsible for the physical connection between devices. It defines the hardware elements involved in the network, including cables, switches, and other physical components. This layer also specifies the electrical, optical, and radio characteristics of the network.

2. Data Link Layer



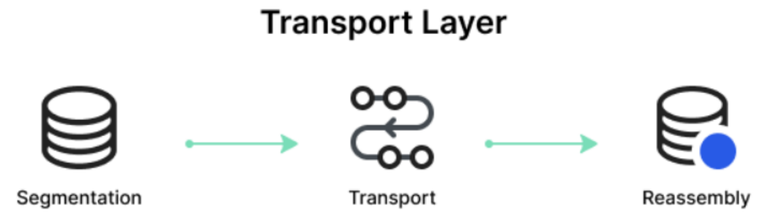
The Data Link Layer is responsible for node-to-node data transfer and error detection and correction. It ensures that data is transmitted to the correct device on a local network segment. This layer manages MAC (Media Access Control) addresses and is divided into two sublayers: Logical Link Control (LLC) and Media Access Control (MAC).

3. Network Layer



The Network Layer is responsible for data routing, forwarding, and addressing. It determines the best physical path for data to reach its destination based on network conditions, the priority of service, and other factors. This layer manages logical addressing through IP addresses and handles packet forwarding.

4. Transport Layer

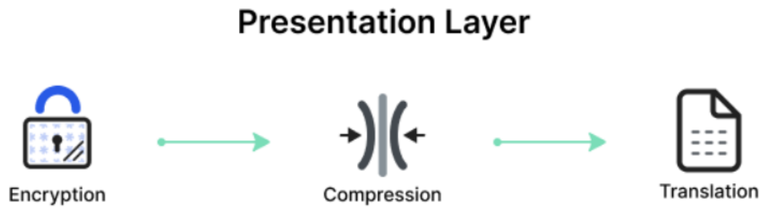


The Transport Layer provides end-to-end communication services for applications. It ensures complete data transfer, error recovery, and flow control between hosts. This layer segments and reassembles data for efficient transmission and provides reliability with error detection and correction mechanisms.

5. Session Layer

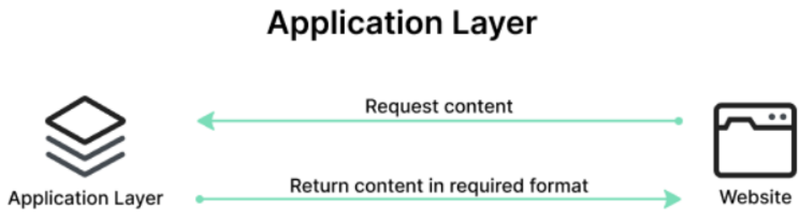
The Session Layer manages and controls the connections between computers. It establishes, maintains, and terminates connections, ensuring that data exchanges occur efficiently and in an organized manner. The layer is responsible for session checkpointing and recovery, which allows sessions to resume after interruptions.

6. Presentation Layer

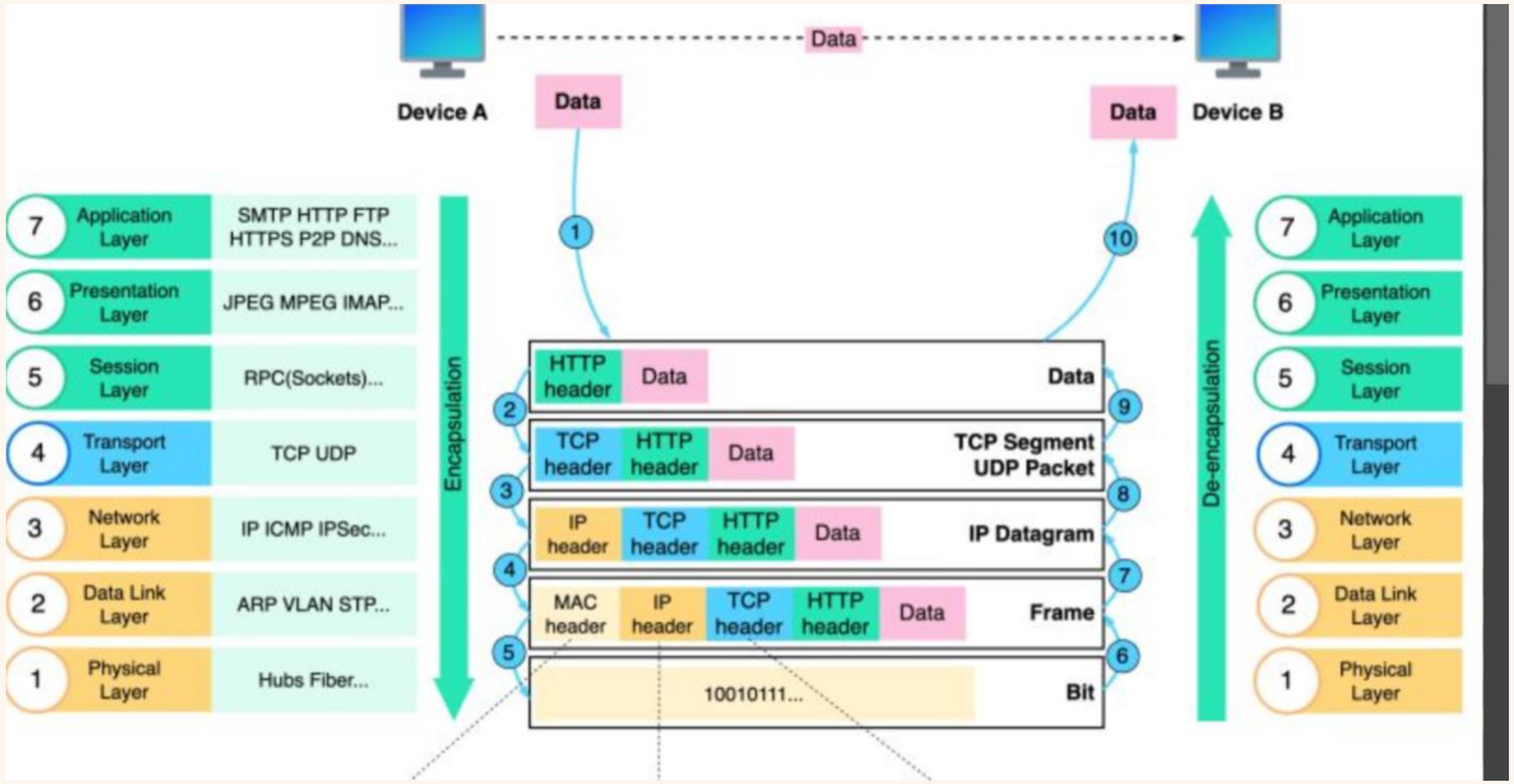


The Presentation Layer, also known as the syntax layer, is responsible for translating data between the application layer and the network format. It ensures that data sent from the application layer of one system is readable by the application layer of another system. This layer handles data formatting, encryption, and compression, facilitating interoperability between different systems.

7. Application Layer



The Application Layer serves as the interface between the end-user applications and the underlying network services. This layer provides protocols and services that are directly utilized by end-user applications to communicate across the network. Key functionalities of the Application Layer include resource sharing, remote file access, and network management.


Data
Device A
Data
Data
Device B
7 Application Layer
SMTP HTTP FTP HTTPS P2P DNS...
6 Presentation Layer
JPEG MPEG IMAP...
5 Session Layer
RPC(Sockets)...
4 Transport Layer
TCP UDP
3 Network Layer
IP ICMP IPSec...
2 Data Link Layer
ARP VLAN STP...
1 Physical Layer
Hubs Fiber...
Encapsulation
1
2
3
4
5
6
7
8
9
10
HTTP header
Data
Data
TCP header
HTTP header
Data
TCP Segment
UDP Packet
IP header
TCP header
HTTP header
Data
IP Datagram
MAC header
IP header
TCP header
HTTP header
Data
Frame
10010111...
Bit
De-encapsulation
7 Application Layer
6 Presentation Layer
5 Session Layer
4 Transport Layer
3 Network Layer
2 Data Link Layer
1 Physical Layer

IEEE STANDARDS :

IEEE 802 is a collection of networking standards that cover the physical and data link layer specifications for technologies such as Ethernet and wireless. These specifications apply to local area networks (LANs) and metropolitan area networks (MANs). IEEE 802 also aids in ensuring multivendor interoperability by promoting standards for vendors to follow.

iEEE 802 is divided into different parts that cover the physical and data link aspects of networking. The family of standards is developed and maintained by the Institute of Electrical and Electronics Engineers (IEEE) 802 LAN/MAN Standards Committee, also called the LMSC.

Without these standards, equipment suppliers could manufacture network hardware that would only connect to certain computers. It would be much more difficult to connect to systems not using the same set of networking equipment. Standardizing protocols helps ensure multiple types of devices can connect to multiple network types.

Logical Link Control (LLC)

This sublayer manages the data link by:

•Checking for errors

•Identifying protocols

•Synchronizing frames

•Providing flow control, acknowledgment, and error notification

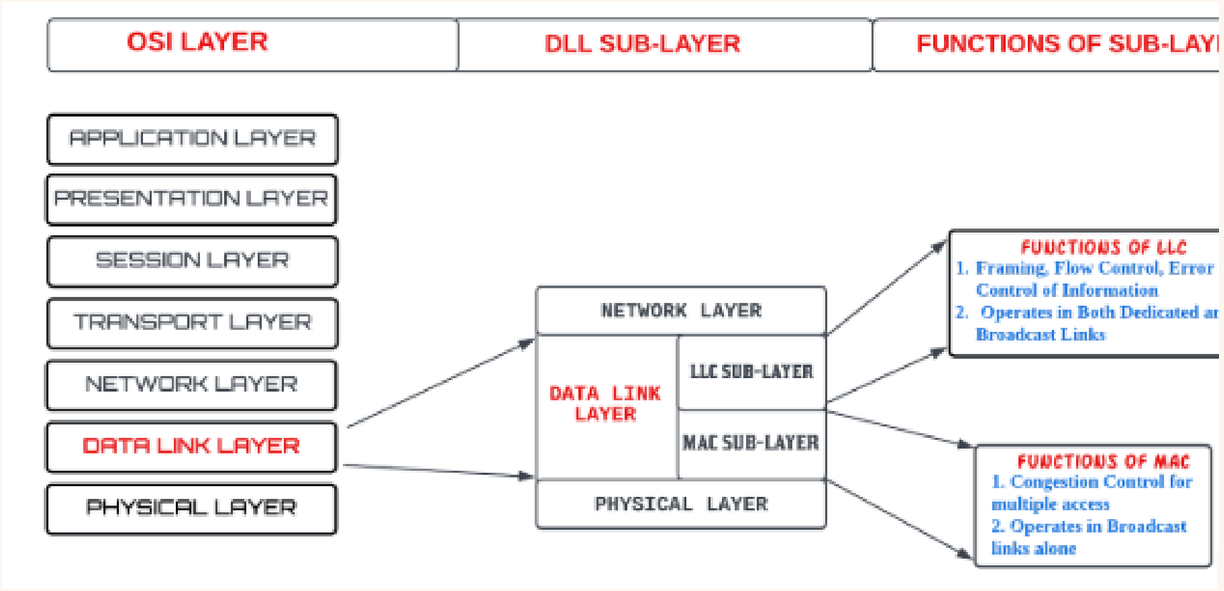
Media Access Control (MAC)

This sublayer manages data flow between devices by :

•Connecting MAC addresses

•Ensuring a clear flow of information between source and destination addresses

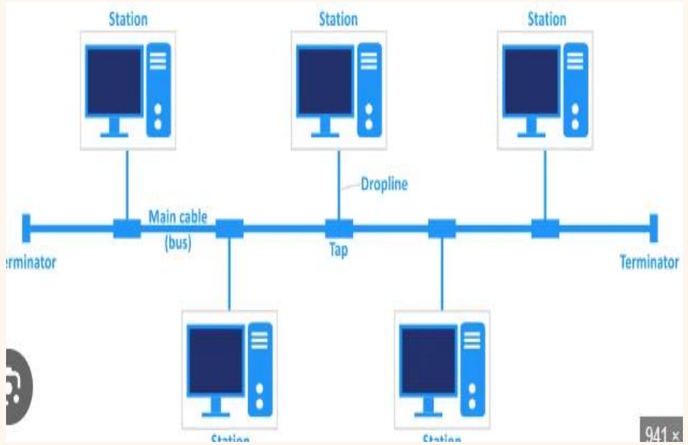
•Determining who is allowed to access the media at any one time

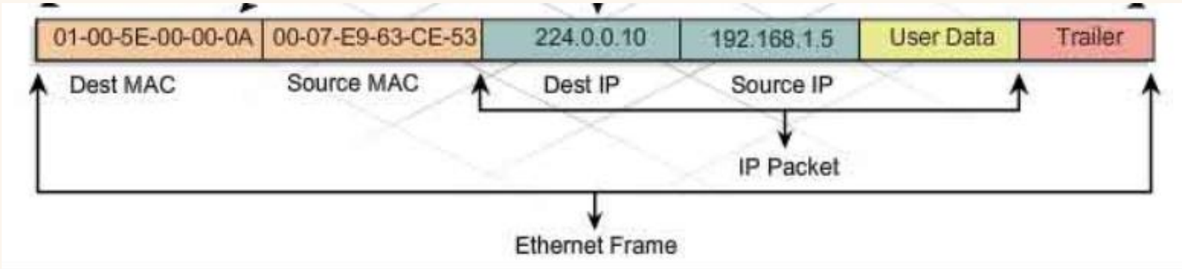


802	Overview	Basics of physical and logical networking concepts
802.1	Bridging	■ LAN/MAN bridging and management. ■ Covers management and the lower sublayers of OSI Layer 2, including MAC-based bridging, virtual LANs and port-based access control. ■ Also contains the Time-Sensitive Networking Task Group.
802.2	Logical link control	Disbanded
802.3	Ethernet	■ The grandfather of the 802 specifications. ■ Provides asynchronous networking using carrier sense, multiple access with collision detect (CSMA/CD) over coax, twisted-pair copper and optical fiber
802.11	Wi-Fi	Wireless LAN MAC and physical layer specification. 802.11a, b, g, ax, etc., are amendments to the original 802.11 standard. Products that implement 802.11 standards must pass tests and are referred to as Wi-Fi certified.
802.11a		■ Specifies a physical layer that operates in the 5 GHz U-NII band in the U.S. -- initially 5.15 GHz to 5.35 GHz and 5.725 GHz to 5.85 GHz -- and since expanded to additional frequencies. ■ Uses orthogonal frequency-division multiplexing (OFDM). ■ Enhanced data speed to 54 Mbps. ■ Ratified after 802.11b.
802.14	Cable modems	Disbanded
802.15	Wireless PANs	Communications specification for wireless PANs that IEEE approved in early 2002
802.15.1	Bluetooth	Short-range (10 meters) wireless technology used for cordless mouse, keyboard and wireless headphones at 2.4 GHz
802.15.3a	Ultra wideband	Short-range, high-bandwidth ultra wideband link
802.15.4	Zigbee	Short-range wireless sensor networks
802.15.5	Mesh network	■ Extension of network coverage without increasing the transmit power or the receiver sensitivity. ■ Enhanced reliability via route redundancy

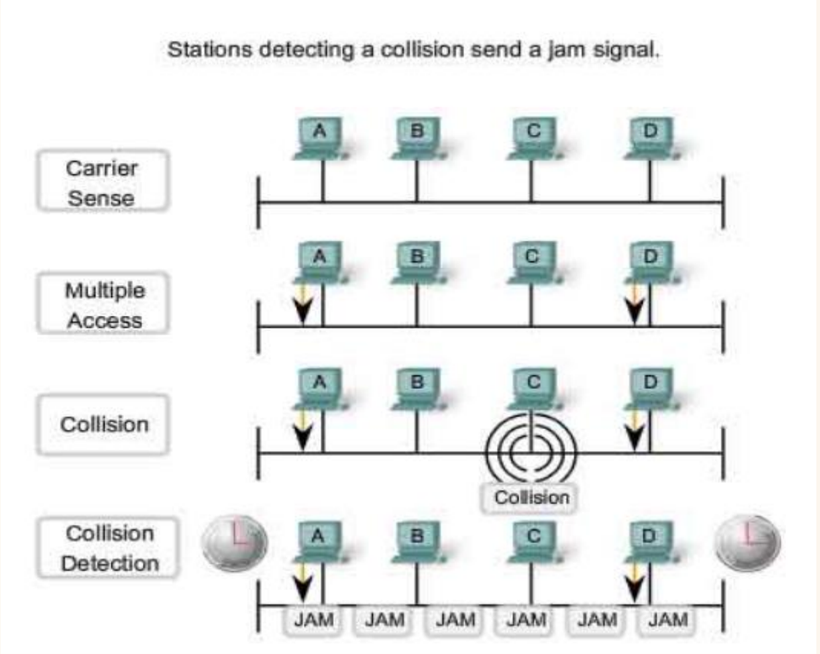
ETHERNET

Ethernet is the most widely used LAN technology and is defined under IEEE standards 802.3. The reason behind its wide usability is that Ethernet is easy to understand, implement, and maintain, and allows low-cost network implementation. Also, Ethernet offers flexibility in terms of the topologies that are allowed. Ethernet generally uses a bus topology. Ethernet operates in two layers of the OSI model, the physical layer and the data link layer. For Ethernet, the protocol data unit is a frame since we mainly deal with DLLs. In order to handle collisions, the Access control mechanism used in Ethernet is CSMA/CD.





•**Carrier Sense (CS):** Before transmitting data, a device checks whether the communication channel is free (i.e., no other device is transmitting).
•**Multiple Access (MA):** All devices on the network share the same communication medium.
•**Collision Detection (CD):** If two devices transmit simultaneously, their signals collide, causing data corruption. The devices detect this collision by monitoring the medium

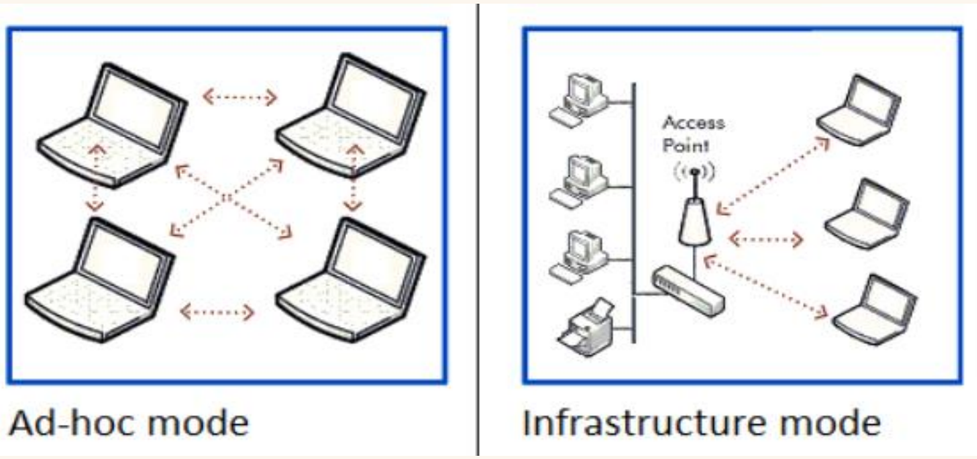


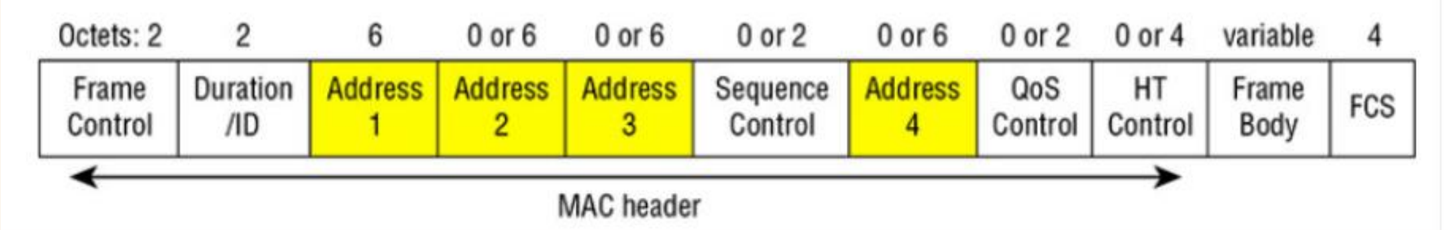
WIFI(WIRELESS FEDILITY)

- Wi-Fi is a wireless networking technology based on the IEEE 802.11 standards, enabling devices to connect to the internet or a local area network (LAN) without physical cables.
- Operates in **2.4 GHz**, **5 GHz**, and **6 GHz** bands, with higher frequencies offering faster speeds and lower interference but shorter ranges.
- Typical range is **30–50 meters indoors** and **100–200 meters outdoors**, depending on obstacles and environmental conditions.
- speed depends on the ieee standard the highest yet achieved is 46gbs.

Network types :

- Adhoc network
- Infrastructure network





Limitations:

- Limited range
- Physical obstructions, like walls, can block Wi-Fi signals
- External radio signals can interfere with Wi-Fi
- Wi-Fi 5 signals can use more battery power on mobile devices.
- Too many devices connected to a router can slow down internet speeds.
- **Where it is used :**
  homes,office,public places

ZIGBEE

IEEE 802.15.4 is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs) and is the basis for the ZigBee.

802.15.4 is a MAC and PHY layer protocol (OSI layers 1 and 2)

IEEE 802.15.4 can operates on several bands –

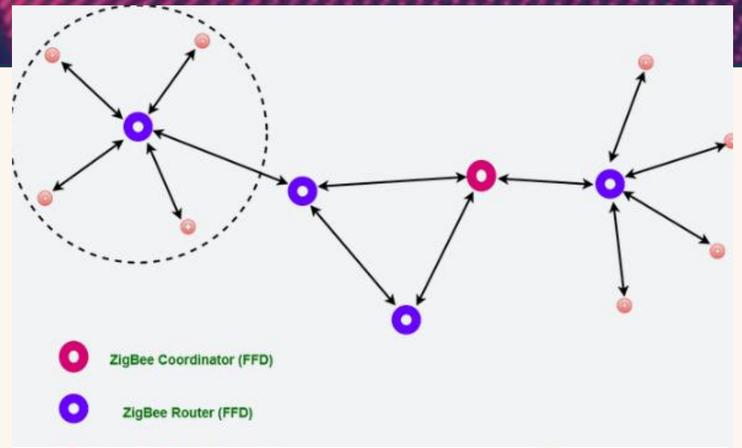
– 2.4 GHz ISM band (Q-QPSK at 250 Kbits/s) 20 dBm, 100 mW

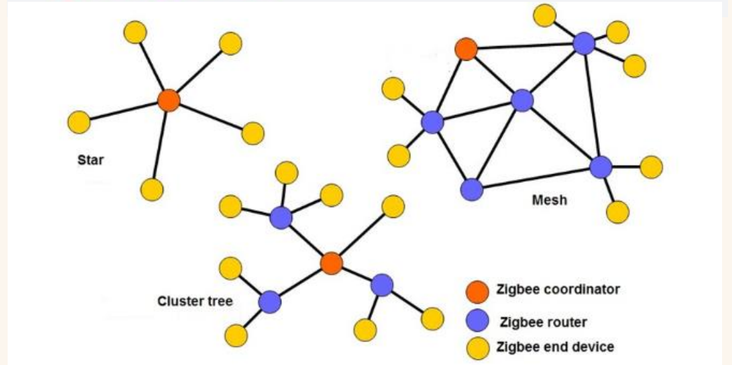
– 915 MHz (BPSK at 40 kb/s, Q-QPSK at 250 kb/s) >10 dBm

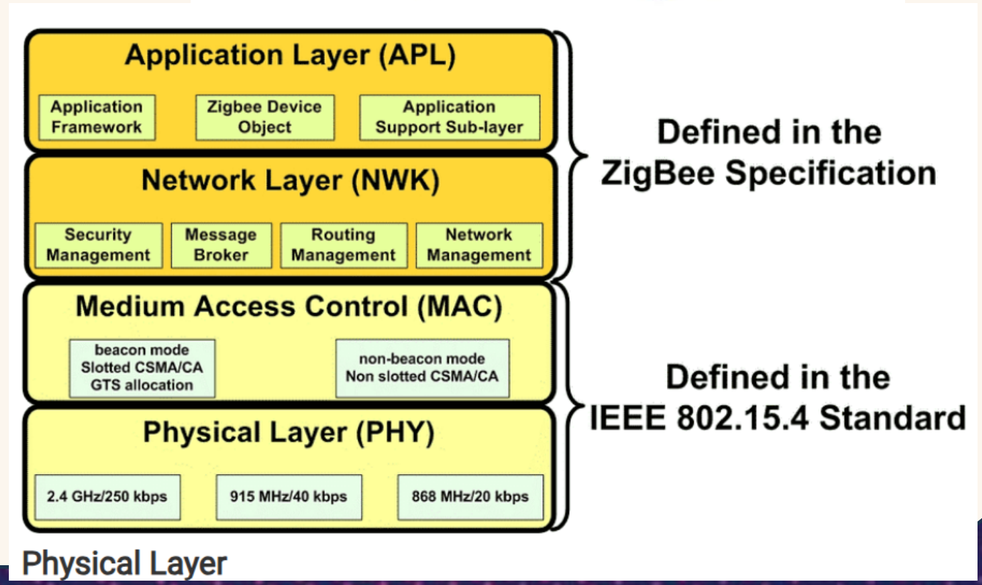
– 868 MHz (BPSK at 20 kb/s, Q-QPSK at 100 kb/s) 1 W (USA)

It uses three types of topologies star ,mesh , tree.

- Low Power Consumption
- Low Data Rate (20- 250 kbps)
- Short-Range (75-100 meters)
- Network Join Time (~ 30 msec)
- Support Small and Large Networks (up to 65000 devices (Theory); 240 devices (Practically))







LORAWAN(LONG RANGE WIDE AREA NETWORK):

- **LoRa (Long Range)** is a proprietary modulation technology used for low-power, long-range wireless communication. It is the foundation of the **LoRaWAN protocol**, enabling communication over vast distances with minimal energy consumption.
- LoRa focuses on the **physical layer** of communication, while **LoRaWAN** operates at higher layers (MAC layer and above), making LoRa responsible for the actual transmission of data over the air.
- It uses chip spread spectrum modulation technique
- it can achieve a communication range of 2-5km in urban and 10 -15km I rural.
- The data rate is 0.3kbs-50kbs.

LoRa (Physical Layer):

•Responsible for the actual transmission of data using **Chirp Spread Spectrum (CSS)**.

•Provides long-range, low-power communication between devices and gateways.

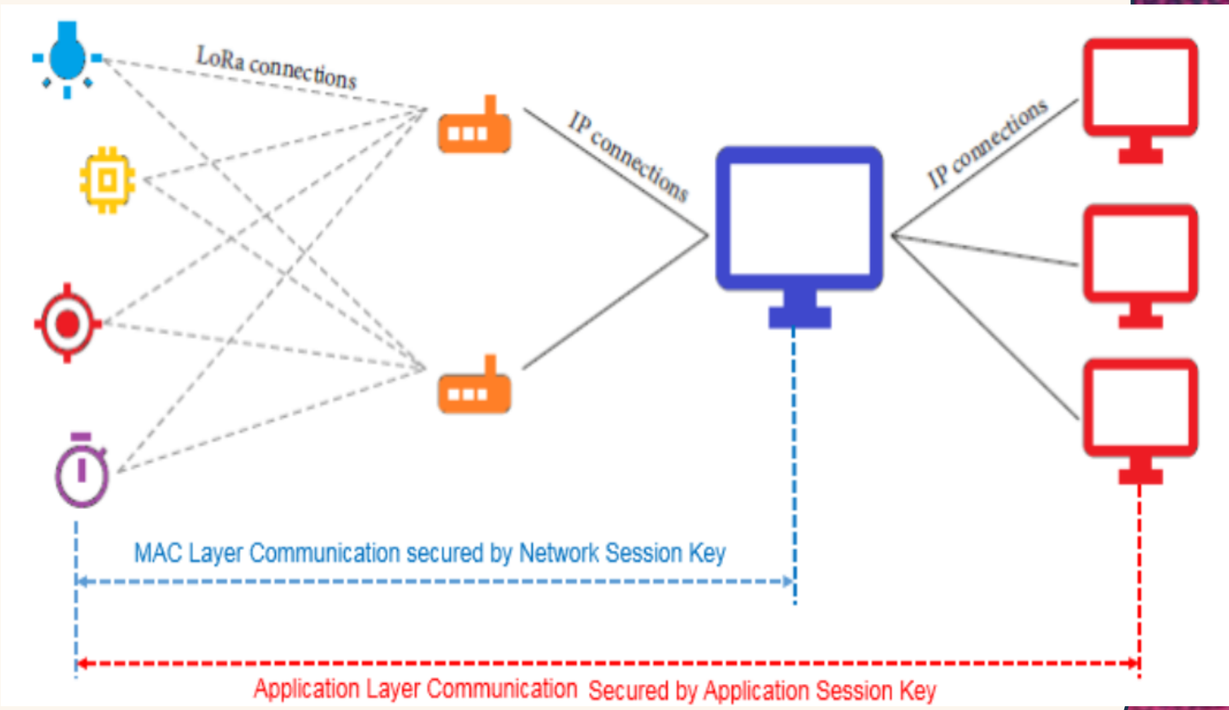
•Operates in unlicensed frequency bands (e.g., 868 MHz, 915 MHz).

LoRaWAN (Protocol Layer):

•Defines how devices connect to gateways and communicate with servers.

•Manages **data encryption**, **device authentication**, and **message integrity**.

•Specifies the **network topology** (star-of-stars) and device communication classes (A, B, and C).



NFC(NEAR FIELD COMMUNICATION):

It is a short-range wireless communication protocol that enables two devices to communicate over a distance of **4 cm or less**. It is built on RFID technology and operates at **13.56 MHz**, within the High-Frequency (HF) band. NFC is widely used for secure and simple communication in applications like contactless payments, ticketing, and access control.

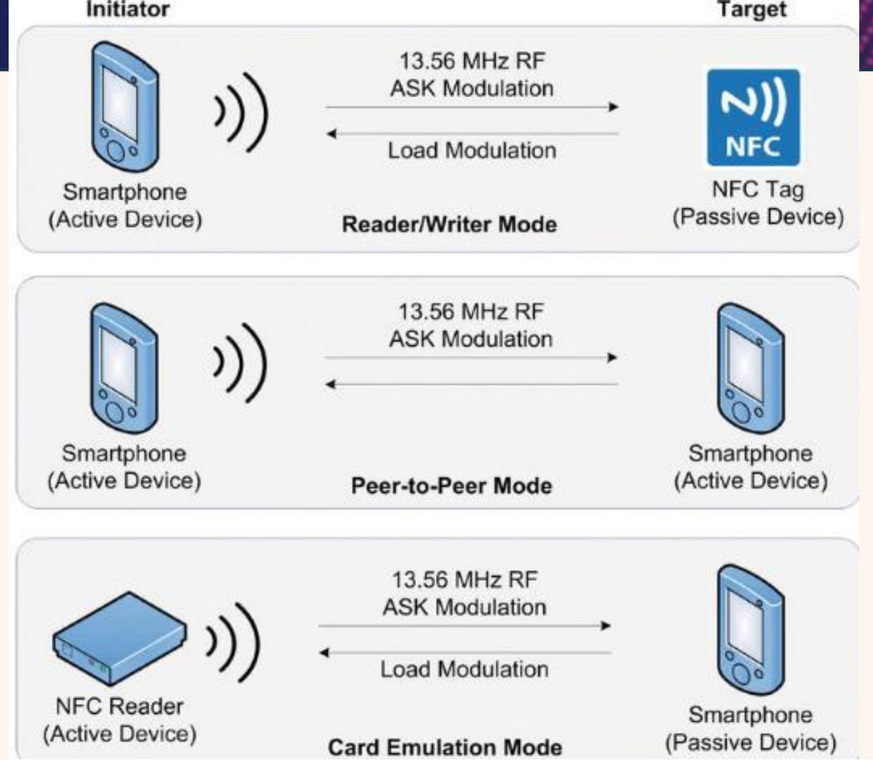
- Frequency 13.56Mhz
- Range 0-4cm
- Data rate 106 kbps, 212 kbps, 424 kbps

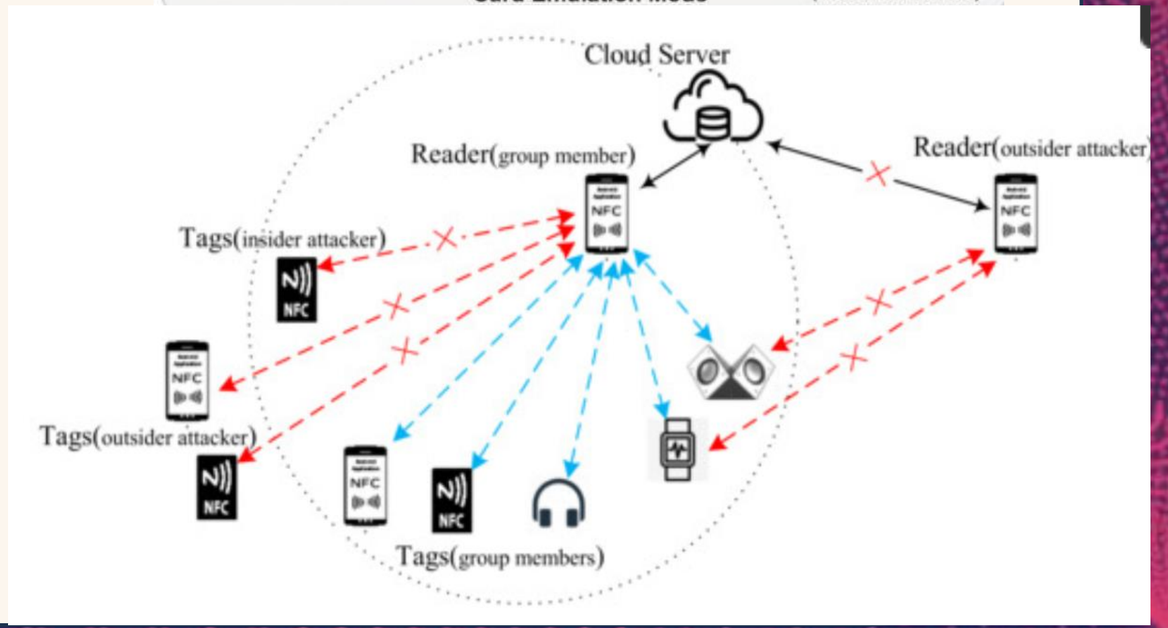
NFC devices can operate in three distinct modes:

•**Reader/Writer Mode**:
One device reads or writes data to an NFC tag (e.g., reading an RFID tag in a smart poster).

•**Peer-to-Peer Mode**:
Two NFC-enabled devices exchange information directly (e.g., file sharing between phones).

•**Card Emulation Mode**:
An NFC device acts as a contactless smart card (e.g., for mobile payments like Google Pay or Apple Pay).

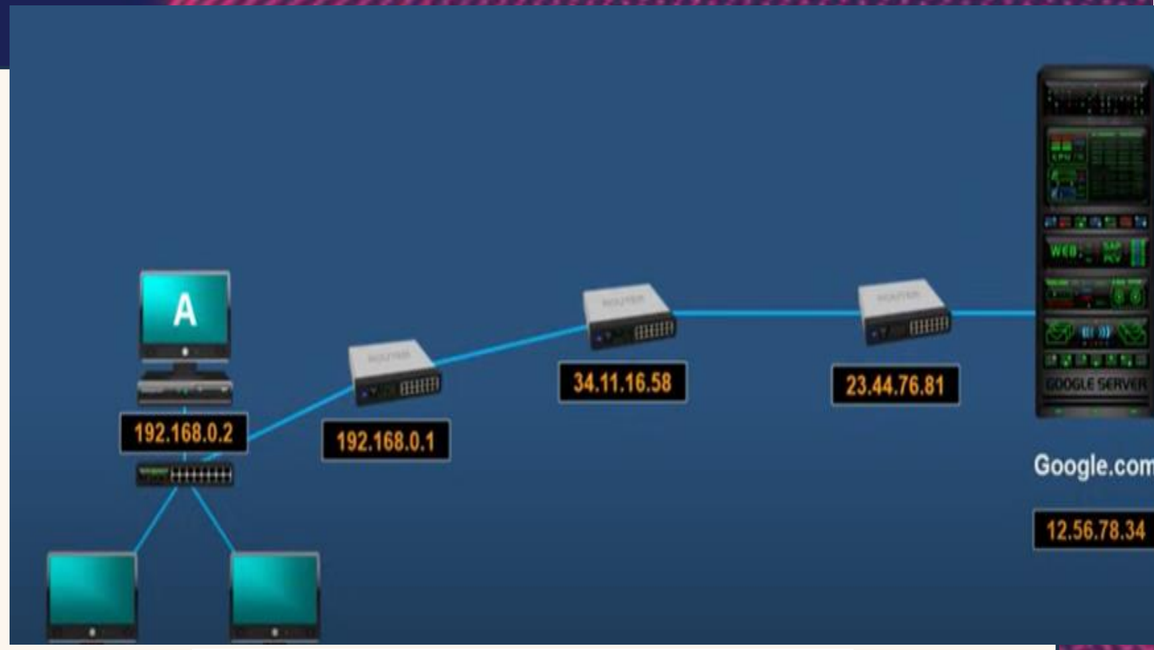


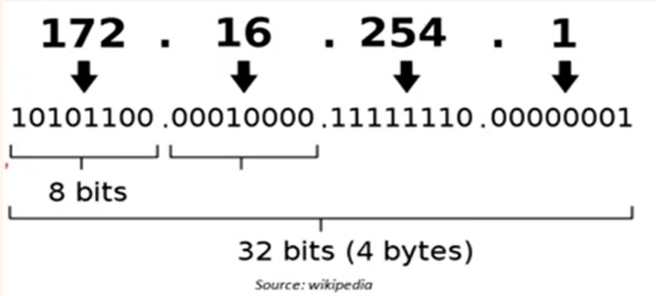


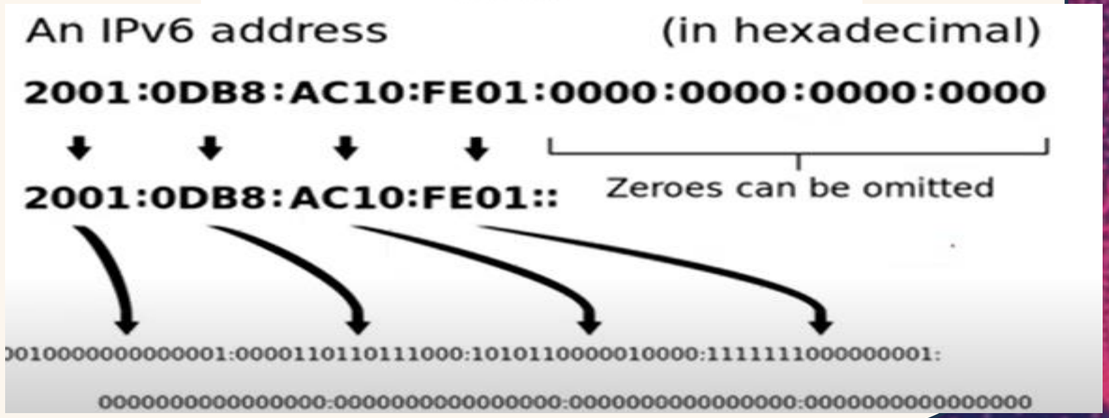
INTERNET PROTOCOL :

The **Internet Protocol (IP)** is a fundamental protocol of the Internet Layer in the **TCP/IP model** (or the Network Layer in the OSI model). It is responsible for **addressing, routing, and delivering data packets** across networks. IP ensures that data sent from one device can reach another device over a network, even if they are on different subnets or networks.

- This comes into picture whenever there is communication between host to host or network to network
- It assigns each device some numerical address(ip address) and by which it can find the sender and receiver and establish a communication between them
- There are two types of ip address according to IP4,IP6

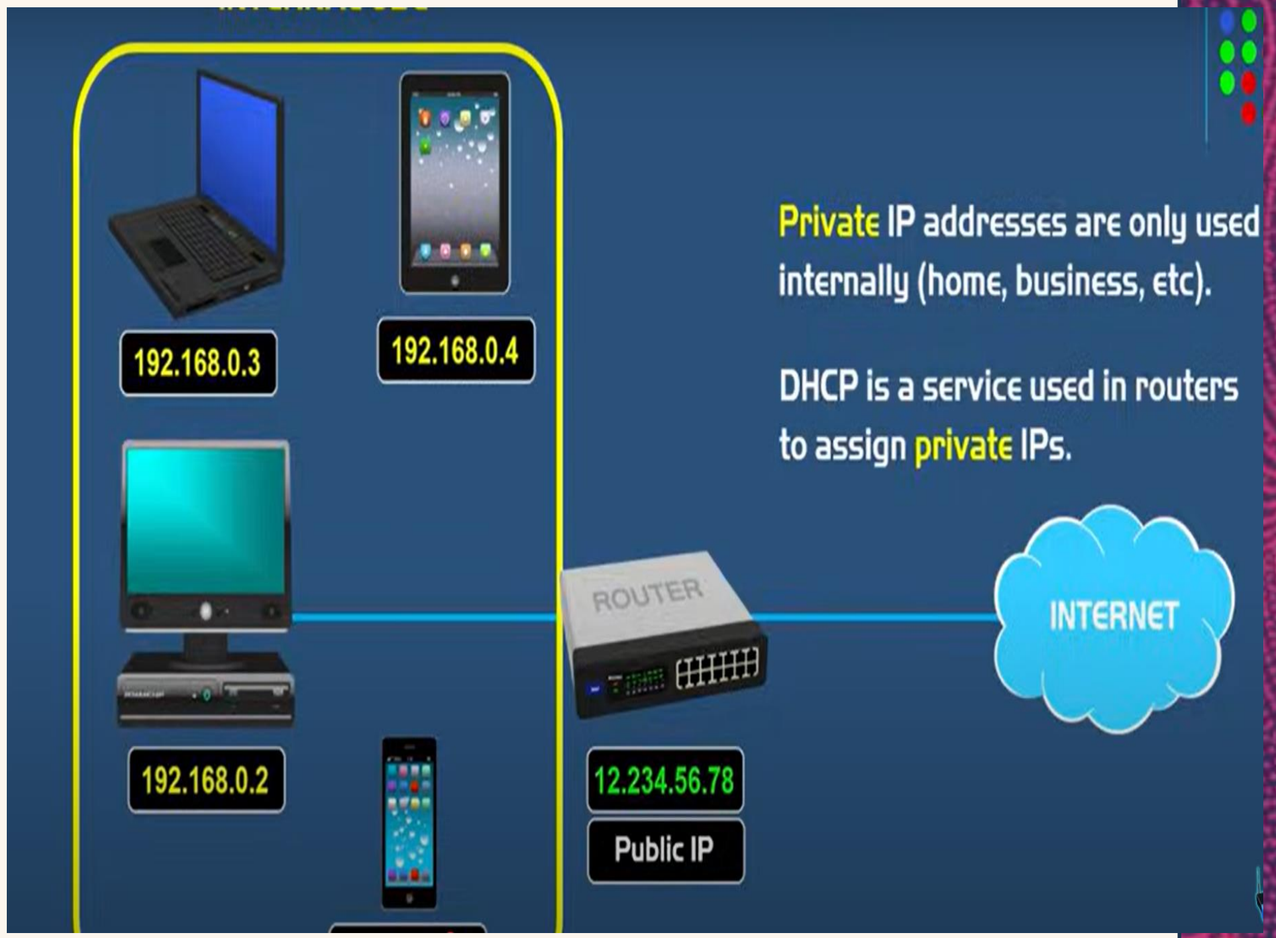






Ip address are either private or public

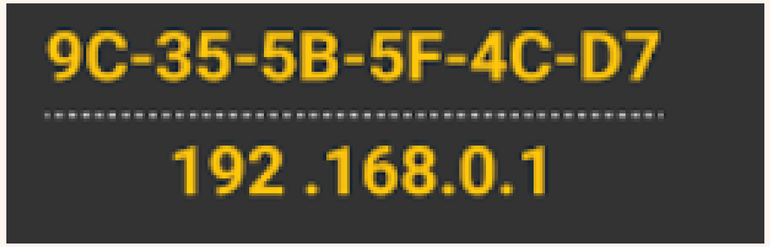
- Public addresses are licenced and they are more secure these addresses are identified by the public severs to share the information
- Private addresses are used for low area communication like our smart homes where we use this addressing for communication between devices
- If we want to access the internet outside then we need to first convert our private ip address to public ip address which is done by **NAT (network address translation)**

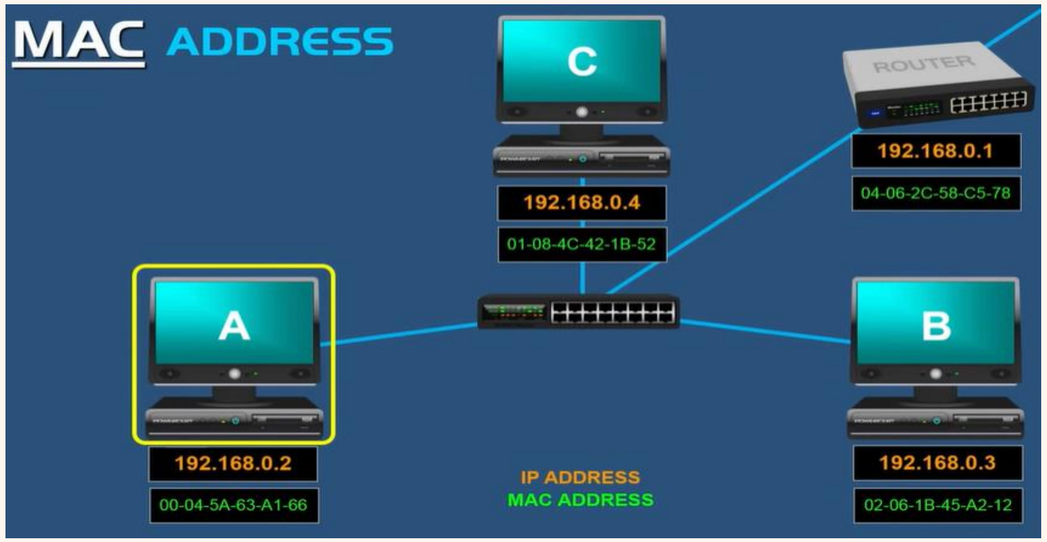


DIFFERENCE BETWEEN IP AND MAC ADDRESS

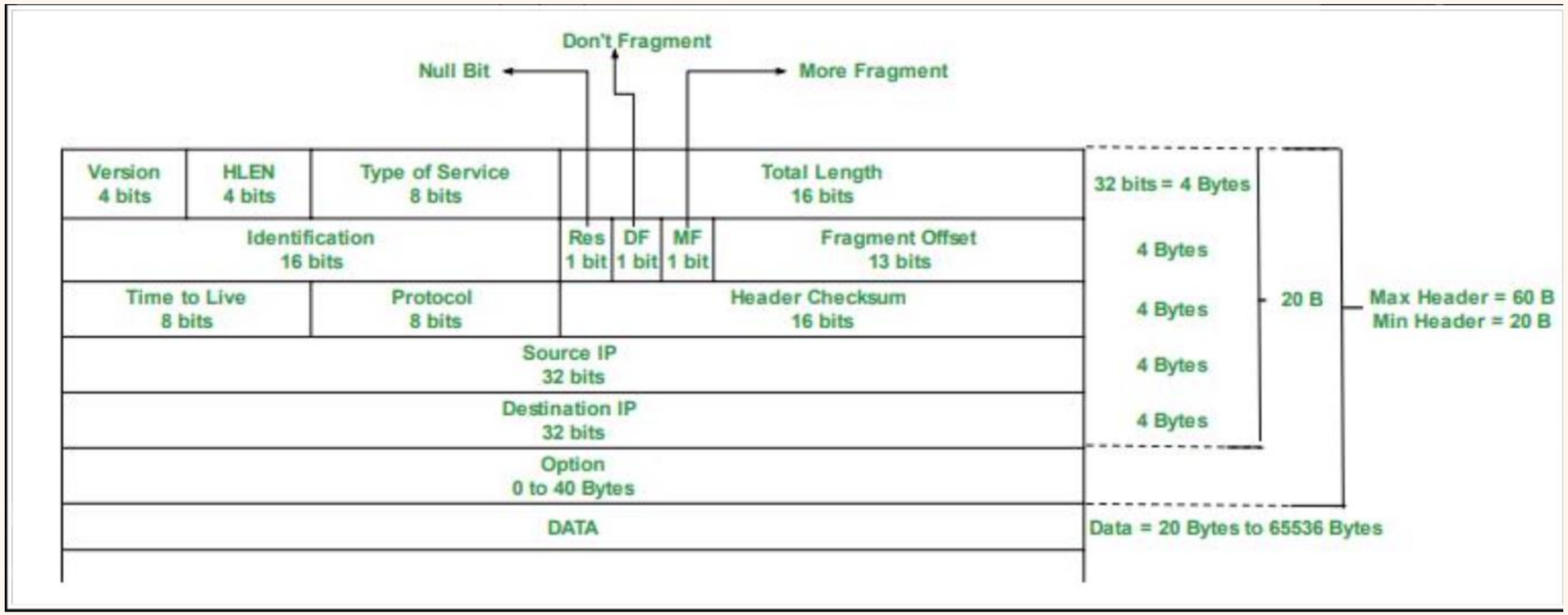
ip address is used for locating devices like in which network they are present

Mac address tell us who the device is

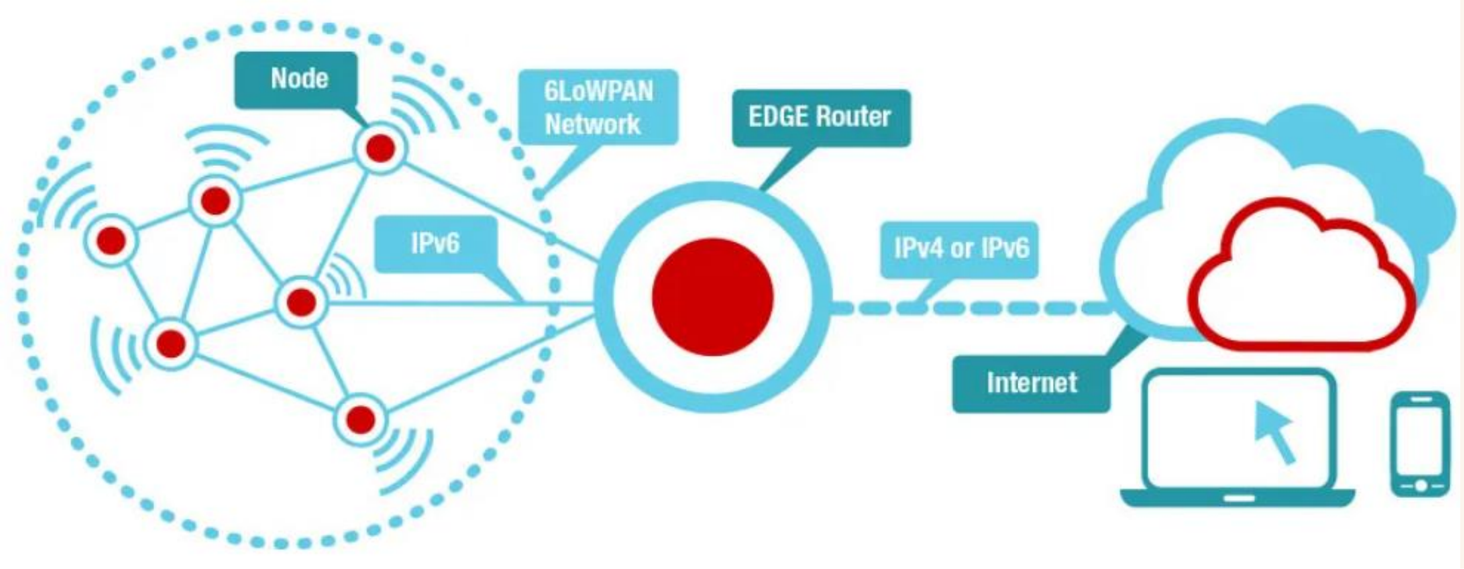




IP4 PACKET FORMAT



6LOWPAN



- 6lowpan – ipv6 over low power wireless personal area network
- 6lowpan is low cost, short range , low memory usage ,low bit rate
- Using 6lowpan even smallest iot devices can be part of the network and talk to outside world
- It offers end-to-end IP addressable nodes. There's no need for a gateway, only a router which can connect the 6LoWPAN network to IP.

ISO/OSI layer
Application
Presentation
Session
Transport
Network
Data link
Physical

6LoWPAN protocol stack	
Application protocols	
Not explicitly used	
Not explicitly used	
UDP	ICMP
IPv6	
Adaptation layer 6LoW(PAN)	
IEEE 802.15.4 MAC	
IEEE 802.15.4 PHY	

- Requirements for using 6lowpan :
- 6LoWPAN devices must have a sleep mode to save battery life and devices have minimal memory requirements
- 6LoWPAN devices must be compatible with the IEEE 802.15.4 standard

➢ It uses mesh networks which makes it more robust by self healing and its sclability

TCP(TRANSMISSION CONTROL PROTOCOL)

it is used when we are doing reliable communication

Uses a three-way handshake process:

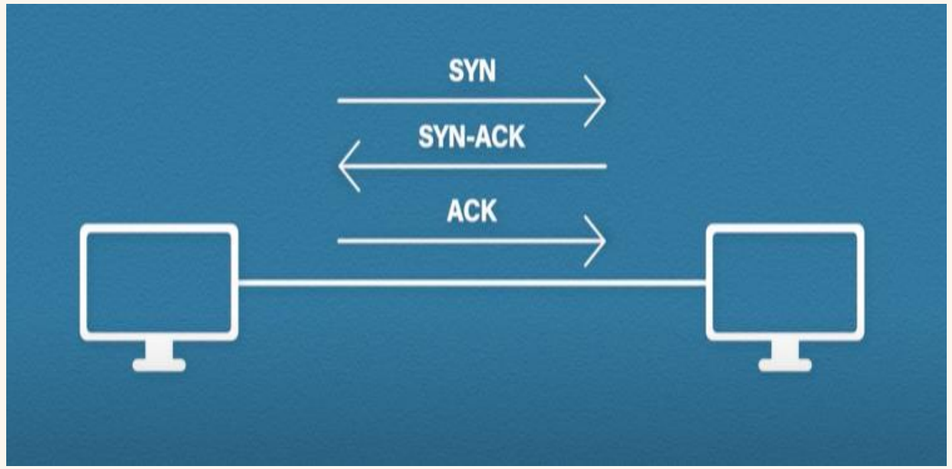
•The client sends a SYN (synchronize) packet to the server.

•The server responds with a SYN-ACK (synchronize-acknowledge) packet.

•The client sends an ACK (acknowledge) packet back to the server.

•The data is divided fragments and sent so to ensure reliable communication it use

•Sequencing , checksum.



Key Features:

- Reliable delivery.
- Data integrity checks.
- Flow control and congestion control.

Use Cases:

- Web browsing (HTTP/HTTPS).
- File transfers (FTP).
- Email (SMTP, IMAP, POP3).
- Remote connections (SSH, Telnet).

UDP (USER DATAGRAM PROTOCOL)

It is used when we really don’t care about reliability in communication

- There is no mechanism for data retransmission, flow control.

Key Features:

•Low latency.

•Lightweight protocol (less overhead).

•No guarantee of delivery.

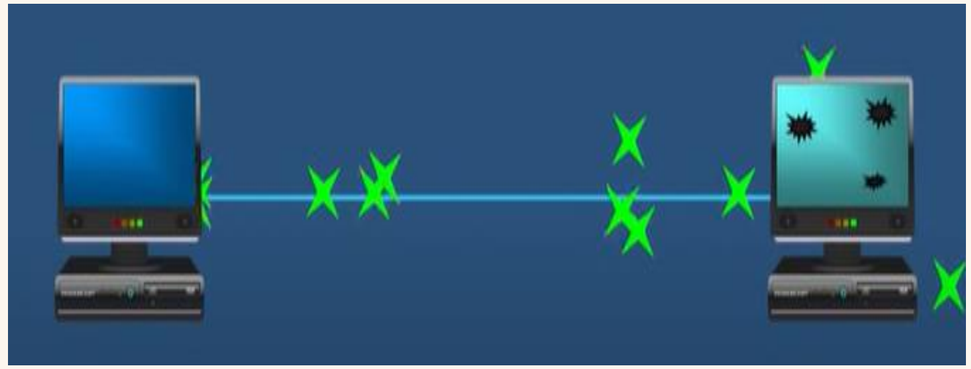
Use Cases:

•Real-time applications (VoIP, online gaming, video conferencing).

•Streaming services (audio/video).

•DNS (Domain Name System) lookups.

•Broadcast or multicast transmissions.



Source Port	Destination Port
Length	Checksum

MQTT(MESSAGE QUEUING TELEMETRY TRANSPORT)

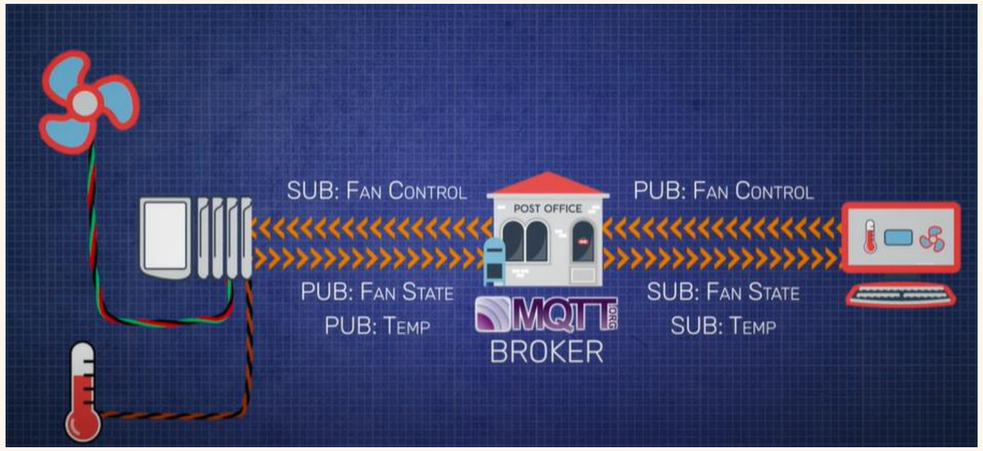
There will be no direct communication between sender and receiver .

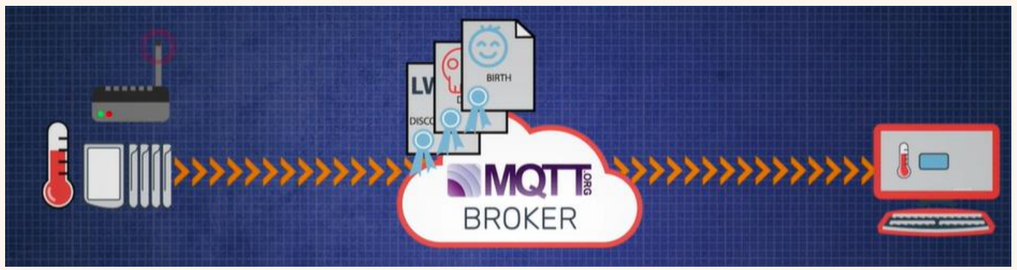
It uses publish-subscribe model with a broker handling in between.

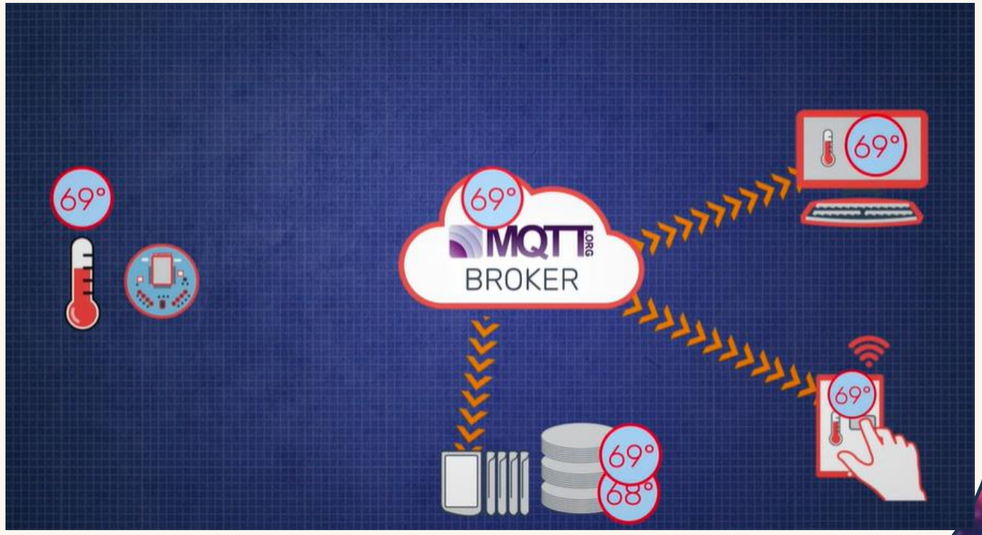
MQTT BROKER :

it is just some software on computer

It may be on your premises or in the cloud





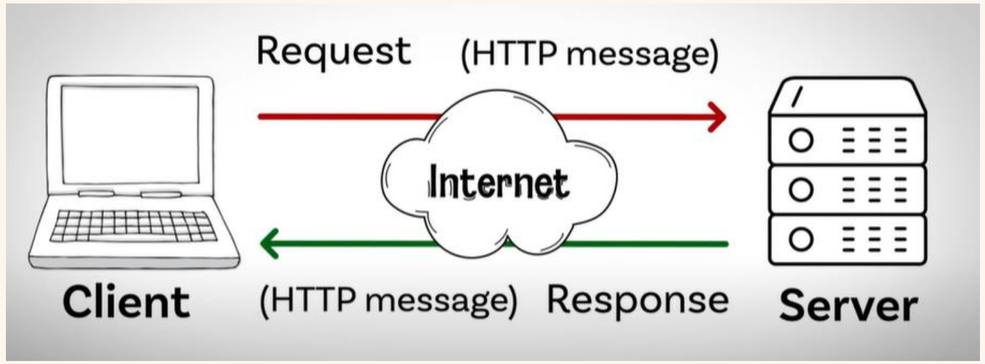


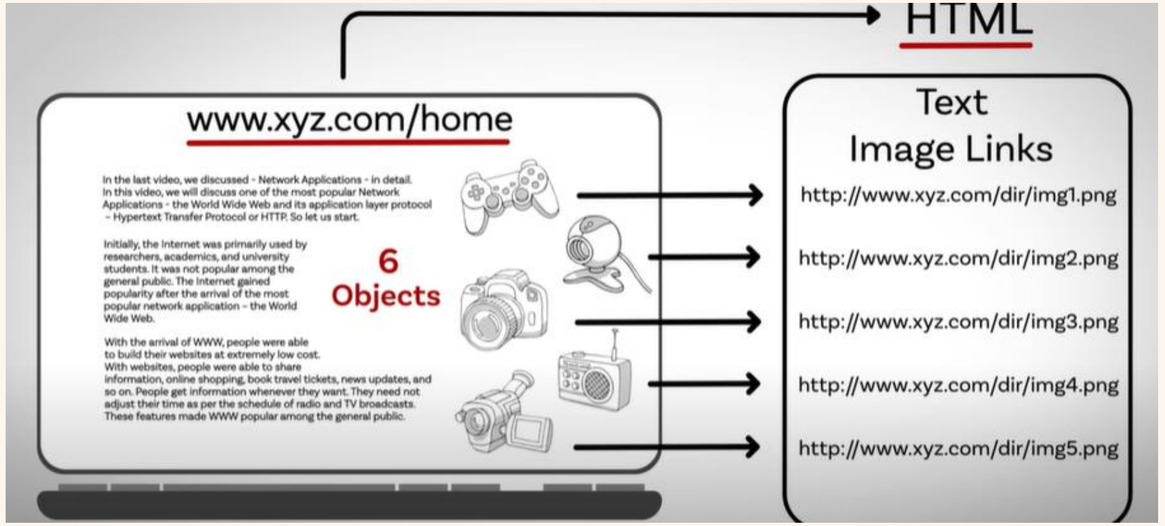
- Smart lighting systems: Lights subscribe to MQTT topics, and the control app publishes commands (e.g., "turn on/off").

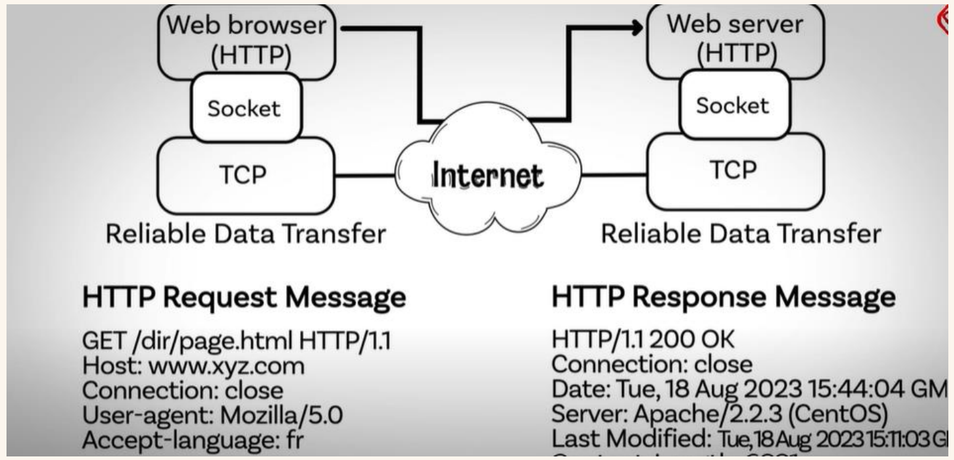
- Monitoring machine performance: Devices publish telemetry data like temperature, vibration, and runtime to a central broker.

- GPS devices in vehicles publish location data to an MQTT broker.

HTTP


Request (HTTP message)
Internet
Client
(HTTP message) Response
Server


HTML
www.xyz.com/home
In the last video, we discussed - Network Applications - in detail. In this video, we will discuss one of the most popular Network Applications - the World Wide Web and its application layer protocol - Hypertext Transfer Protocol or HTTP. So let us start.
Initially, the Internet was primarily used by researchers, academics, and university students. It was not popular among the general public. The Internet gained popularity after the arrival of the most popular network application - the World Wide Web.
With the arrival of WWW, people were able to build their websites at extremely low cost. With websites, people were able to share information, online shopping, book travel tickets, news updates, and so on. People get information whenever they want. They need not adjust their time as per the schedule of radio and TV broadcasts. These features made WWW popular among the general public.
6 Objects
Text
Image Links
http://www.xyz.com/dir/img1.png
http://www.xyz.com/dir/img2.png
http://www.xyz.com/dir/img3.png
http://www.xyz.com/dir/img4.png
http://www.xyz.com/dir/img5.png


Web browser (HTTP)
Socket
TCP
Internet
Web server (HTTP)
Socket
TCP
Reliable Data Transfer
Reliable Data Transfer
HTTP Request Message
GET /dir/page.html HTTP/1.1
Host: www.xyz.com
Connection: close
User-agent: Mozilla/5.0
Accept-language: fr
HTTP Response Message
HTTP/1.1 200 OK
Connection: close
Date: Tue, 18 Aug 2023 15:44:04 GM
Server: Apache/2.2.3 (CentOS)
Last Modified: Tue,18 Aug 2023 15:11:03 G

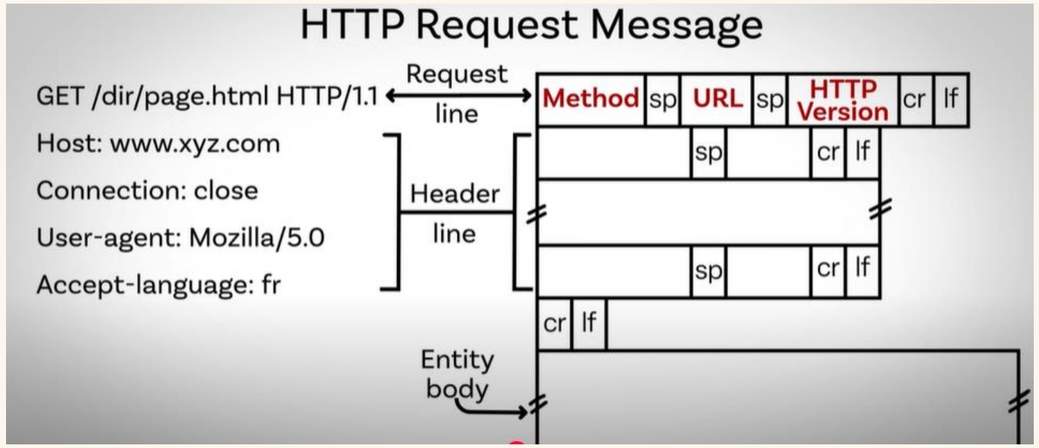
GET ⟶ used when a web browser requests an object from a web server

POST ⟶ used to submit data to the server for processing

HEAD ⟶ used by the application developers for debugging

PUT ⟶ used to upload an object to a specific directory on a server

DELETE ⟶ used to delete objects from the server



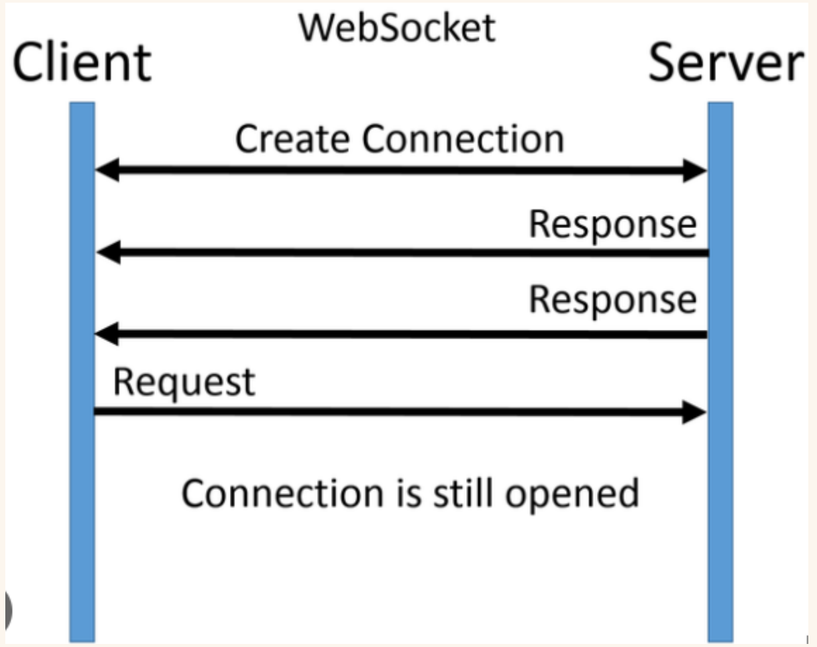
WEBSOCKETS

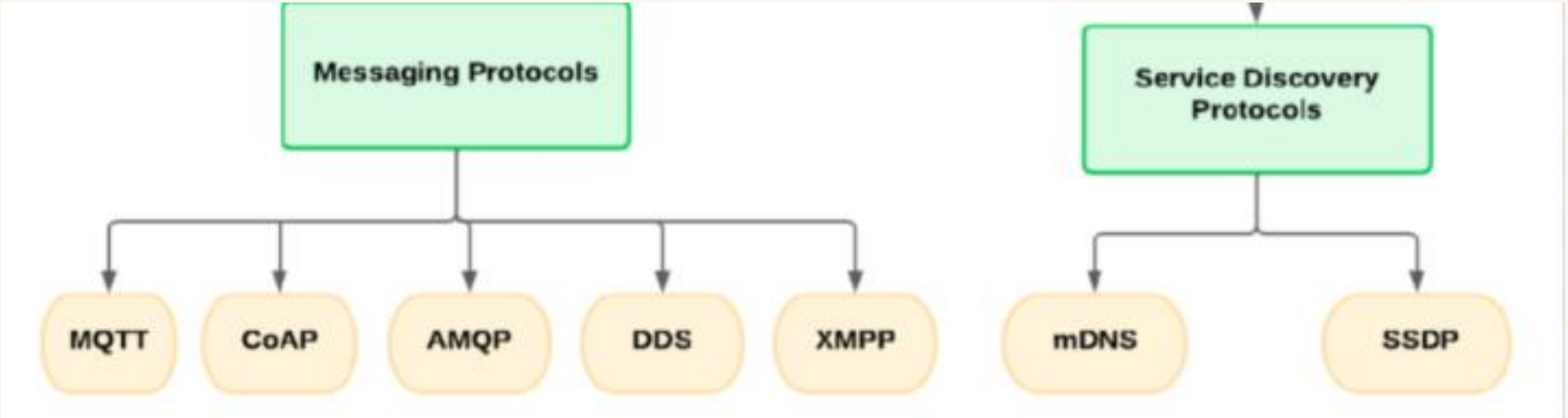
It is bidirectional communication between client and server

They are used for

- Real time app application
- Live notification
- Online gaming

It will reduce latency and server resources by persistent connection in between .




Messaging Protocols
MQTT
CoAP
AMQP
DDS
XMPP
Service Discovery Protocols
mDNS
SSDP