

# Computer Networks (UCS06B15)

## Lecture - 11

Prepared By

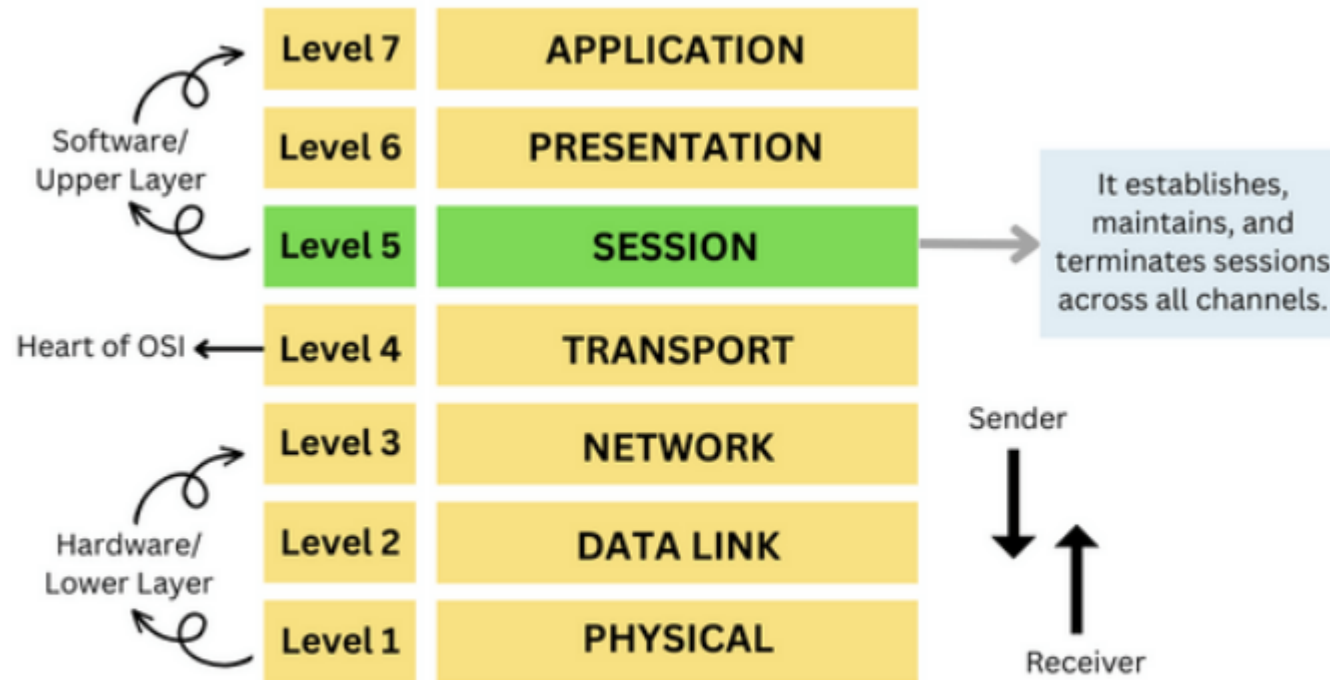
**Dr. Smita Das**

*smitadas.nita@gmail.com*

National Institute of Technology, Agartala  
Computer Science & Engineering Department

# Session Layer

The session layer is the 5<sup>th</sup> layer from the bottom in the OSI model. The job of the session layer is to control and maintain connections between systems to share data. It establishes, maintains, and ends sessions across all channels. In case of a network error, it checks the authenticity and provides recovery options for active sessions. It manages sessions and synchronizes data flow.



**The OSI Model: Session Layer**

# Session Layer- Functions

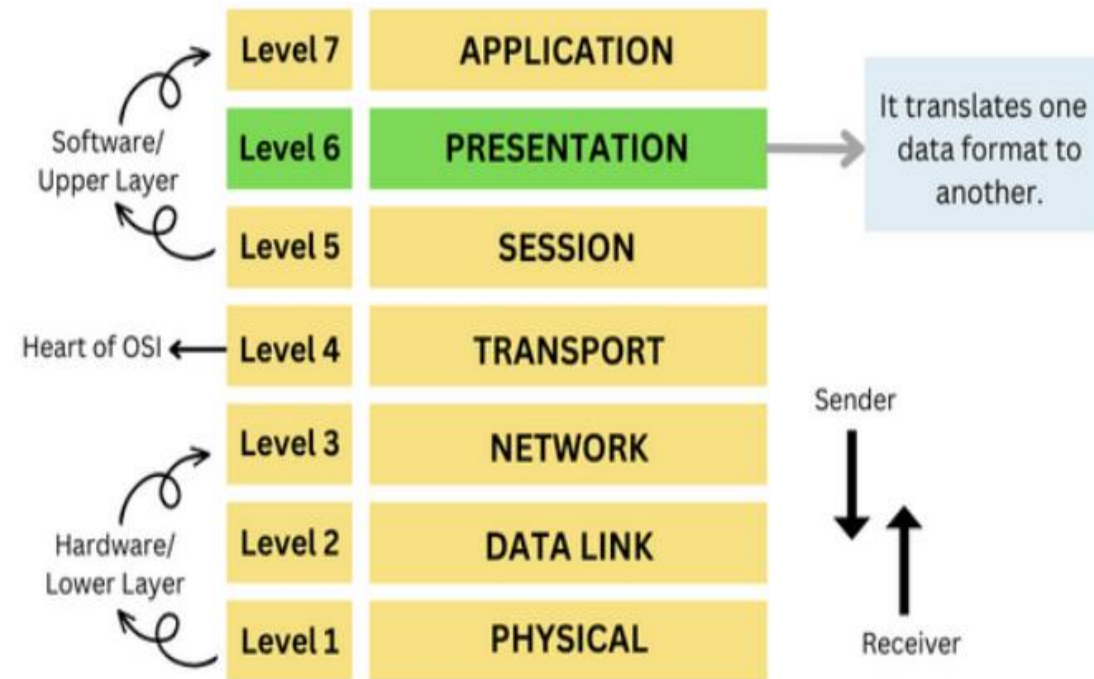
1. Authentication
2. Authorization
3. Session Establishment
4. Session Restoration or Checkpoint
5. Data Transfer
6. Dialog Management
7. Synchronization

# Session Layer- Used Protocols

- Real-time Transport Control Protocol (RTCP)
- Point-to-Point Tunnelling Protocol (PPTP)
- AppleTalk Data Stream Protocol (ADSP)
- Remote Procedure Call Protocol (RPC)
- Password Authentication Protocol (PAP)
- Sockets Direct Protocol (SDP)
- Internet Storage Name Service (ISNS).

# Presentation Layer

The presentation layer is the 6<sup>th</sup> layer from the bottom in the OSI model. This layer presents the incoming data from the application layer of the sender machine to the receiver machine. It converts one format of data to another format of data if both sender and receiver understand different formats; hence this layer is also called the **translation layer**. It deals with the semantics and syntax of the data, so this layer is also called the **syntax layer**. It uses operations such as data compression, data encryption & decryption, data conversion, etc.



The OSI Model: Presentation Layer

# Presentation Layer- Functions

- Translation
- Encryption and Decryption
- Compression and Decompression

# Presentation Layer- Used Protocols

- Network Data Representation (NDR)
- Independent Computing Architecture (ICA)
- NetWare Core Protocol (NCP)
- Apple Filing Protocol (AFP)
- Packet Assembler/Disassembler Protocol (PAD)
- eXternal Data Representation (XDR)
- Lightweight Presentation Protocol (LPP)

# Application Layer

The application layer in the OSI model is the closest layer to the end user which means that the application layer and end user can interact directly with the software application. The application layer programs are based on client and servers.

The Application layer includes the following functions:

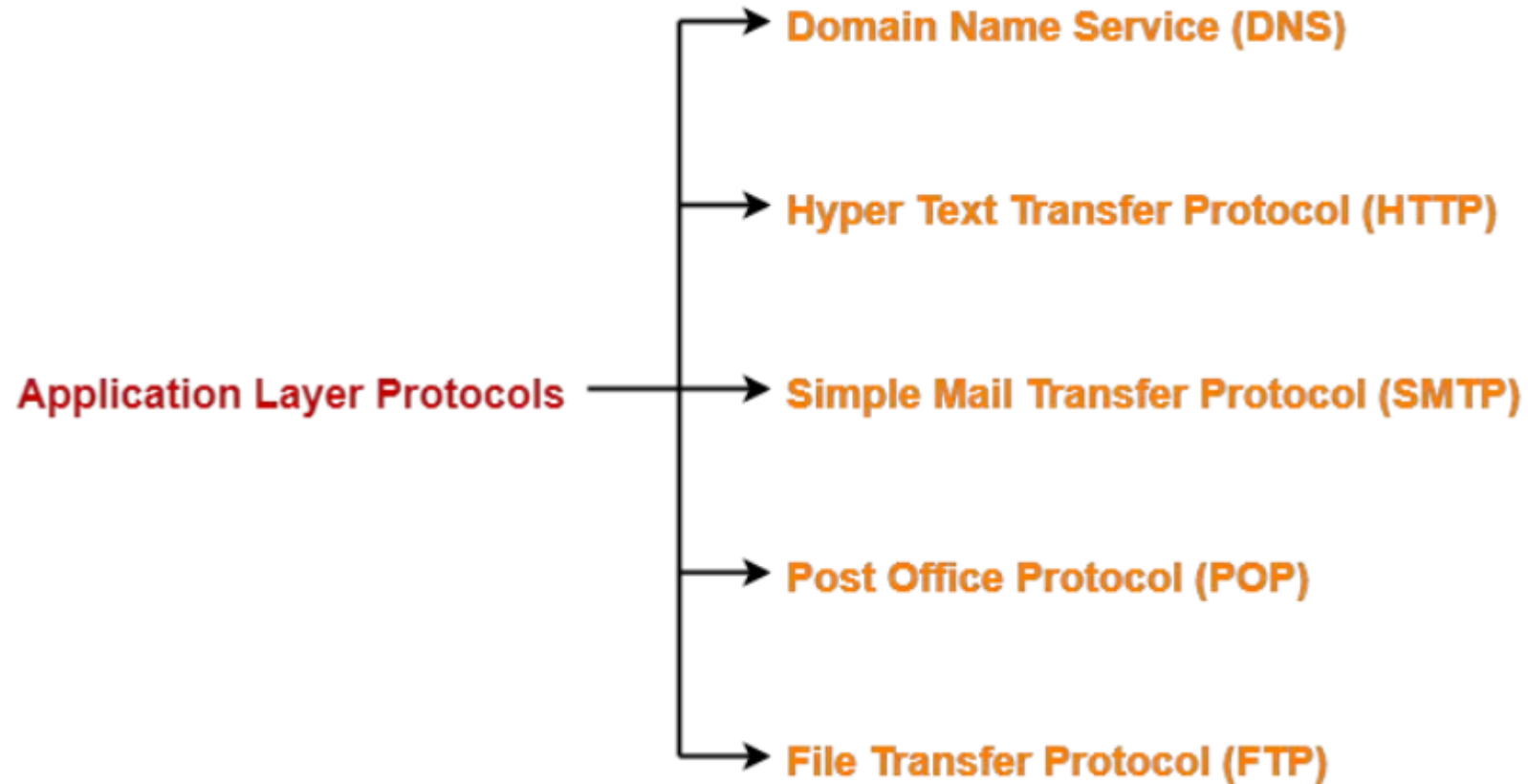
- Identifying communication partners
- Determining resource availability
- Synchronizing communication



# Architecture of Network Application Layer

- **Client-server architecture**
- **P2P (peer-to-peer) architecture**

# Application Layer – used protocols



# DNS

## Purpose-

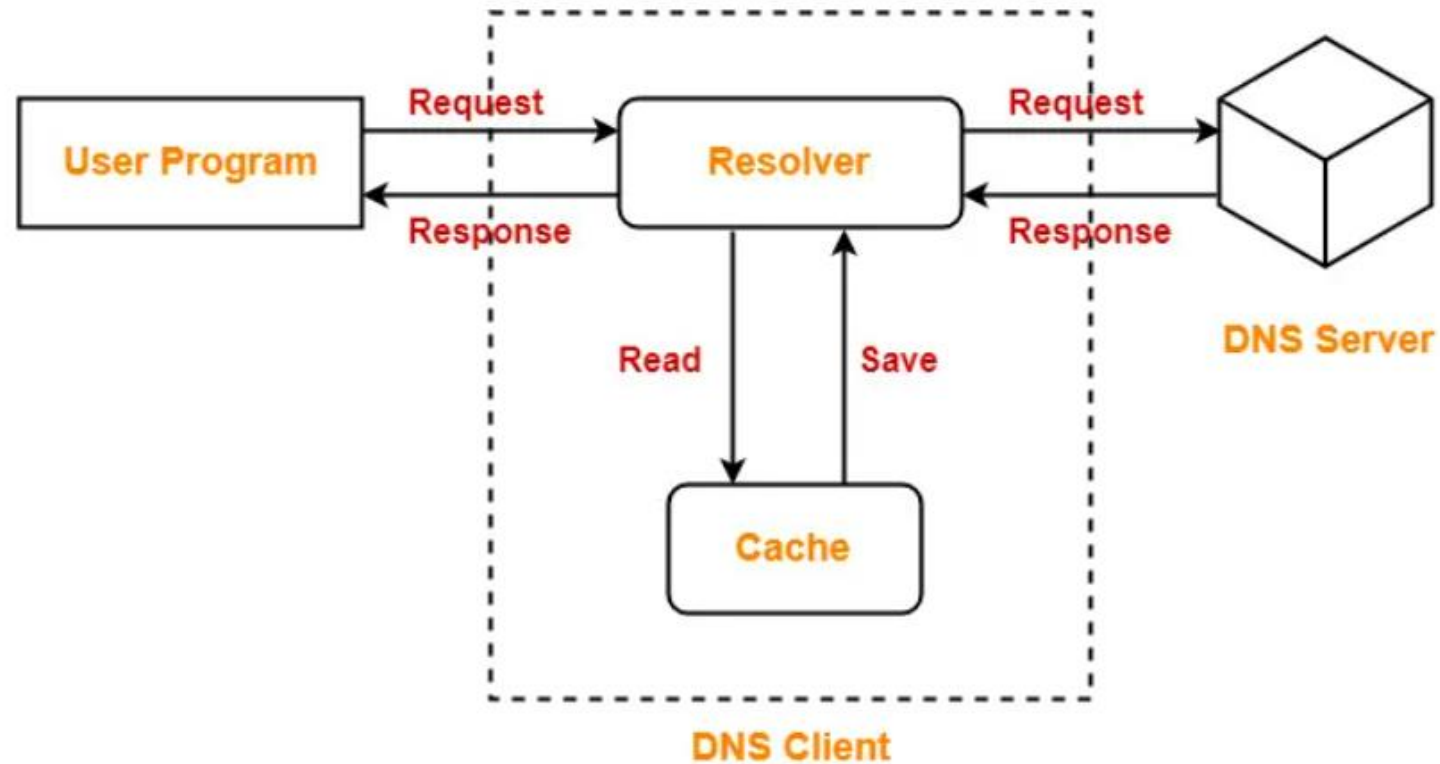
- DNS is a host name to IP Address translation service.
- It converts the names we type in our web browser address bar to the IP Address of web servers hosting those sites.



# DNS Resolution

DNS Resolution is a process of resolving a domain name onto an IP Address.

The following diagram illustrates the process of DNS resolution-



# HTTP

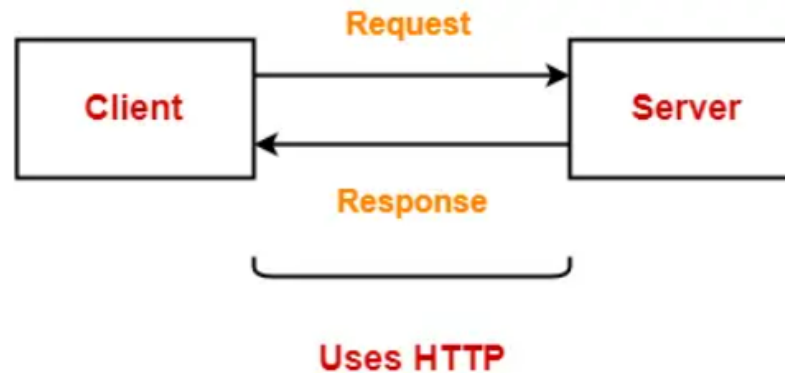
## Purpose-

- It is mainly used for the retrieval of data from websites throughout the internet.
- It works on the top of TCP/IP suite of protocols.

## Working-

HTTP uses a client-server model where-

- Web browser is the client.
- Client communicates with the web server hosting the website.



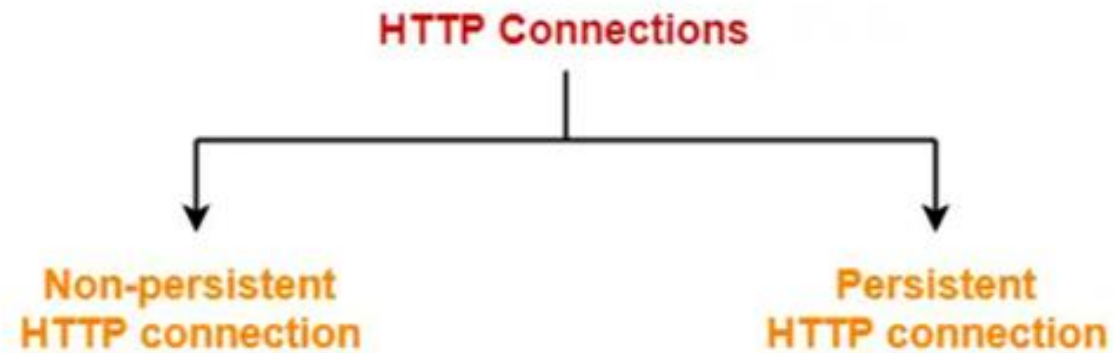
# HTTP Characteristics

- Uses Port no. 80.
- It uses TCP in the transport layer.
- Its an in-band protocol because data and command pass through same port.
- It is stateless because it does not store any metadata or additional information.
- HTTP 1.0 is non-persistent but HTTP 1.1 is persistent.

# HTTP

HTTP connections can be of two types-

1. Non-persistent HTTP connection
2. Persistent HTTP connection



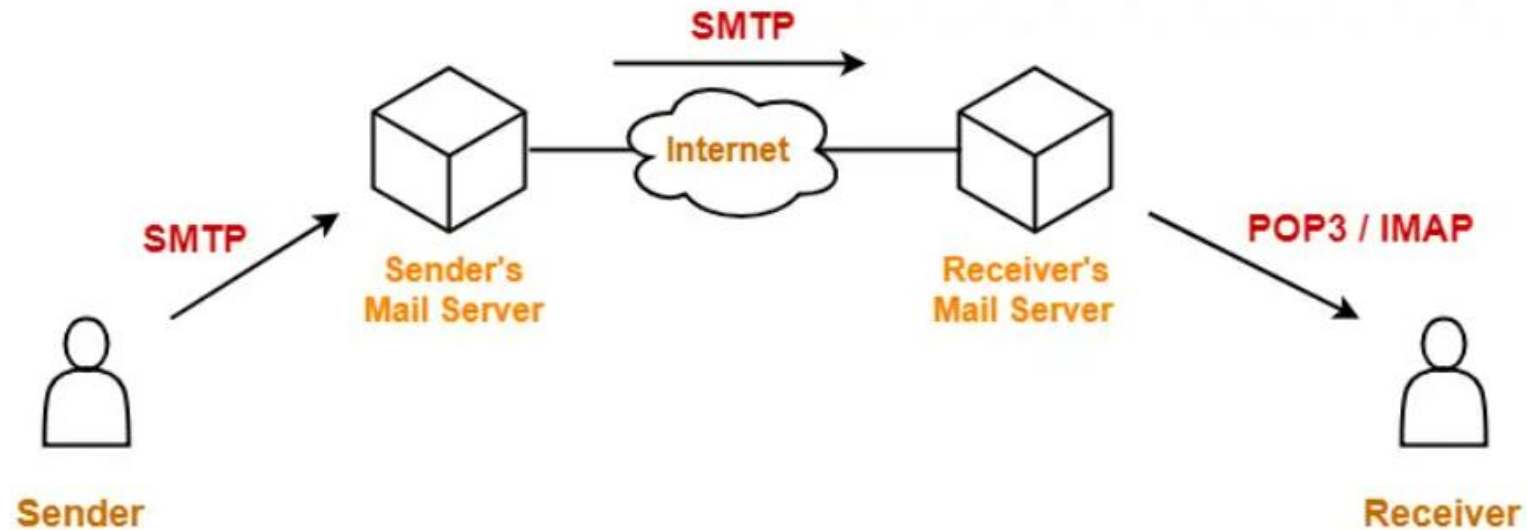
# HTTP

Non-persistent HTTP connection	Persistent HTTP connection
Non-persistent HTTP connection is one that is used for serving exactly one request and sending one response.	Persistent HTTP connection is one that can be used for serving multiple requests.
HTTP server closes the TCP connection automatically after sending a HTTP response.	HTTP server closes the TCP connection only when it is not used for a certain configurable amount of time.
A new separate TCP connection is used for each object.	A single TCP connection is used for sending multiple objects one after the other.
HTTP 1.0 supports non-persistent connections by default.	HTTP 1.1 supports persistent connections by default.



# SMTP

- SMTP server is always on a listening mode.
- Client initiates a TCP connection with the SMTP server.
- SMTP server listens for a connection and initiates a connection on that port.
- The connection is established.
- Client informs the SMTP server that it would like to send a mail.
- Assuming the server is OK, client sends the mail to its mail server.
- Client's mail server use DNS to get the IP Address of receiver's mail server.
- Then, SMTP transfers the mail from sender's mail server to the receiver's mail server.



# SMTP

## **Characteristics of SMTP-**

- SMTP is a push protocol.
- SMTP uses TCP at the transport layer.
- SMTP uses port number 25.
- SMTP uses persistent TCP connections, so it can send multiple emails at once.
- SMTP is a connection oriented protocol.
- SMTP is an in-band protocol.
- SMTP is a stateless protocol.

# POP

## **Purpose-**

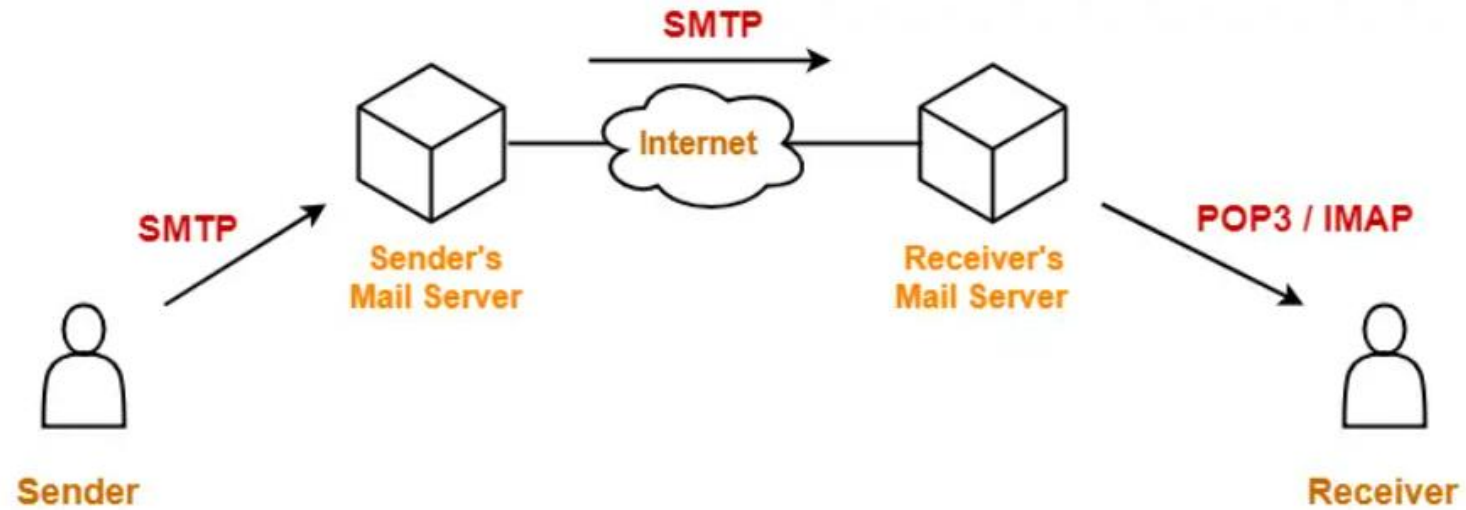
- It is a message access protocol.
- It enables the clients to receive or download the emails from their remote mail server.
- POP version 3 (POP3) is the most popularly used version.

## **Working-**

To retrieve a message from the mail server-

- Client establishes a TCP connection using port 110.
- Client identifies itself to the server.
- Client issues a series of POP3 commands.

# POP



## Characteristics of POP-

- POP is a pull protocol.
- POP uses TCP at the transport layer.
- POP uses port number 110.
- POP uses persistent TCP connections.
- POP is a connection oriented protocol.
- POP is an in-band protocol.
- POP is a stateful protocol until the mail is downloaded as well as stateless across sessions.

# FTP

## Purpose-

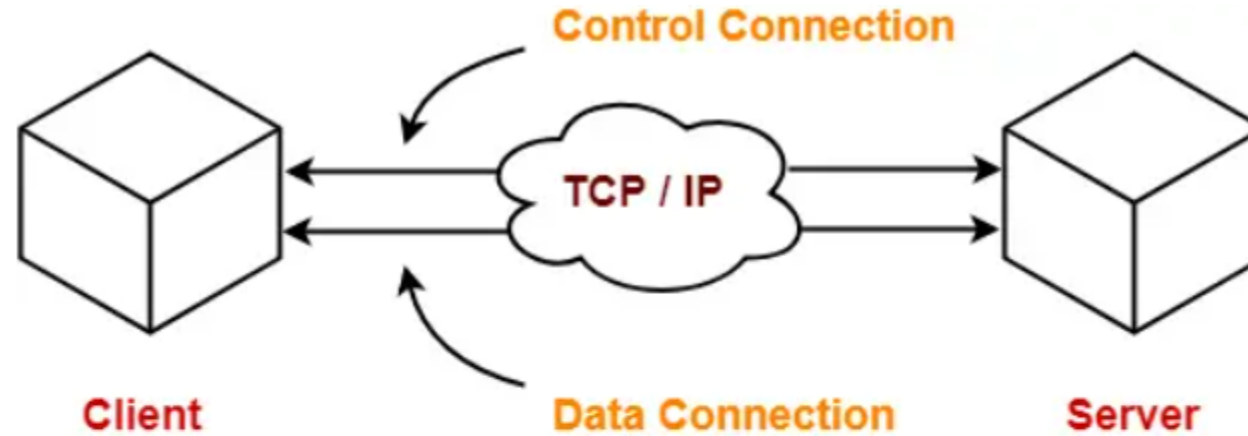
- It is used for exchanging files over the internet.
- It enables the users to upload and download the files from the internet.

## Working-

FTP establishes two TCP connections between the client and the server.

- One connection is used for transferring data.
- Other connection is used for transferring control information.

# FTP



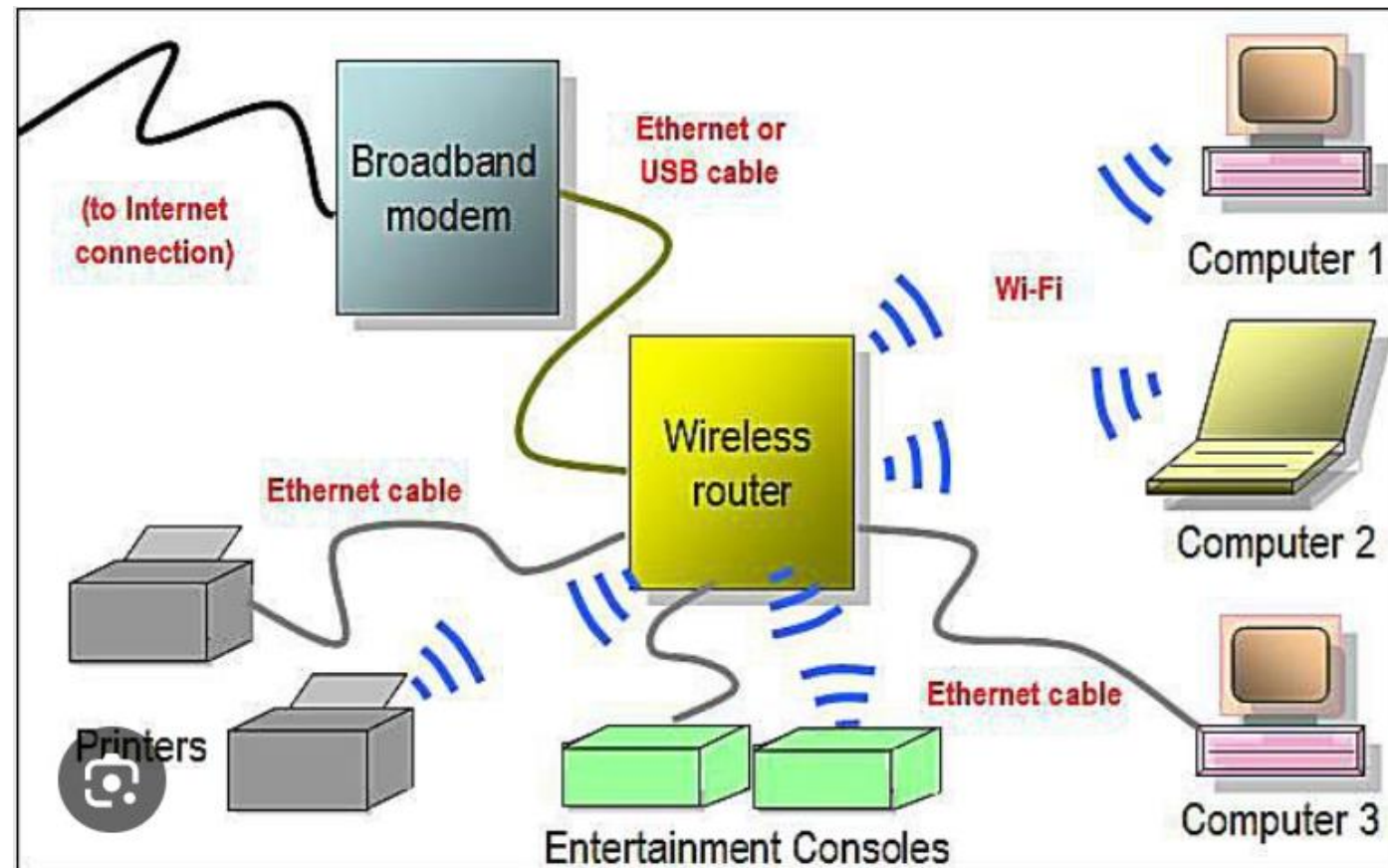
## Characteristics of FTP-

- FTP uses TCP at the transport layer.
- FTP uses port number 21 for control connection.
- FTP uses port number 20 for data connection.
- FTP uses persistent TCP connections for control connection.
- FTP uses non-persistent connections for data connection.
- FTP is a connection oriented protocol.
- FTP is an out-of-band protocol as data and control information flow over different connections.
- SMTP is a stateful protocol.

	<b>DNS</b>	<b>HTTP</b>	<b>SMTP</b>	<b>POP</b>	<b>FTP</b>
<b>Stateful / Stateless</b>	Stateless	Stateless	Stateless	Stateful	Stateful
<b>Transport Protocol Used</b>	UDP	TCP	TCP	TCP	TCP
<b>Connectionless / Connection Oriented</b>	Connectionless	Connectionless	Connection Oriented	Connection Oriented	Connection Oriented
<b>Persistent / Non-persistent</b>	Non-persistent	HTTP 1.0 is non-persistent. HTTP 1.1 is persistent.	Persistent	Persistent	Control connection is persistent. Data connection is non-persistent.
<b>Port Number Used</b>	53	80	25	110	20 for data connection. 21 for control connection.
<b>In band / Out-of-band</b>	In band	In band	In band	In band	Out-of-band

# IEEE 802.11

IEEE 802.11 standard is popularly known as Wi-fi, that lays down the architecture and specifications of wireless LANs (WLANs). It uses high-frequency radio waves instead of cables for connecting the devices in LAN.





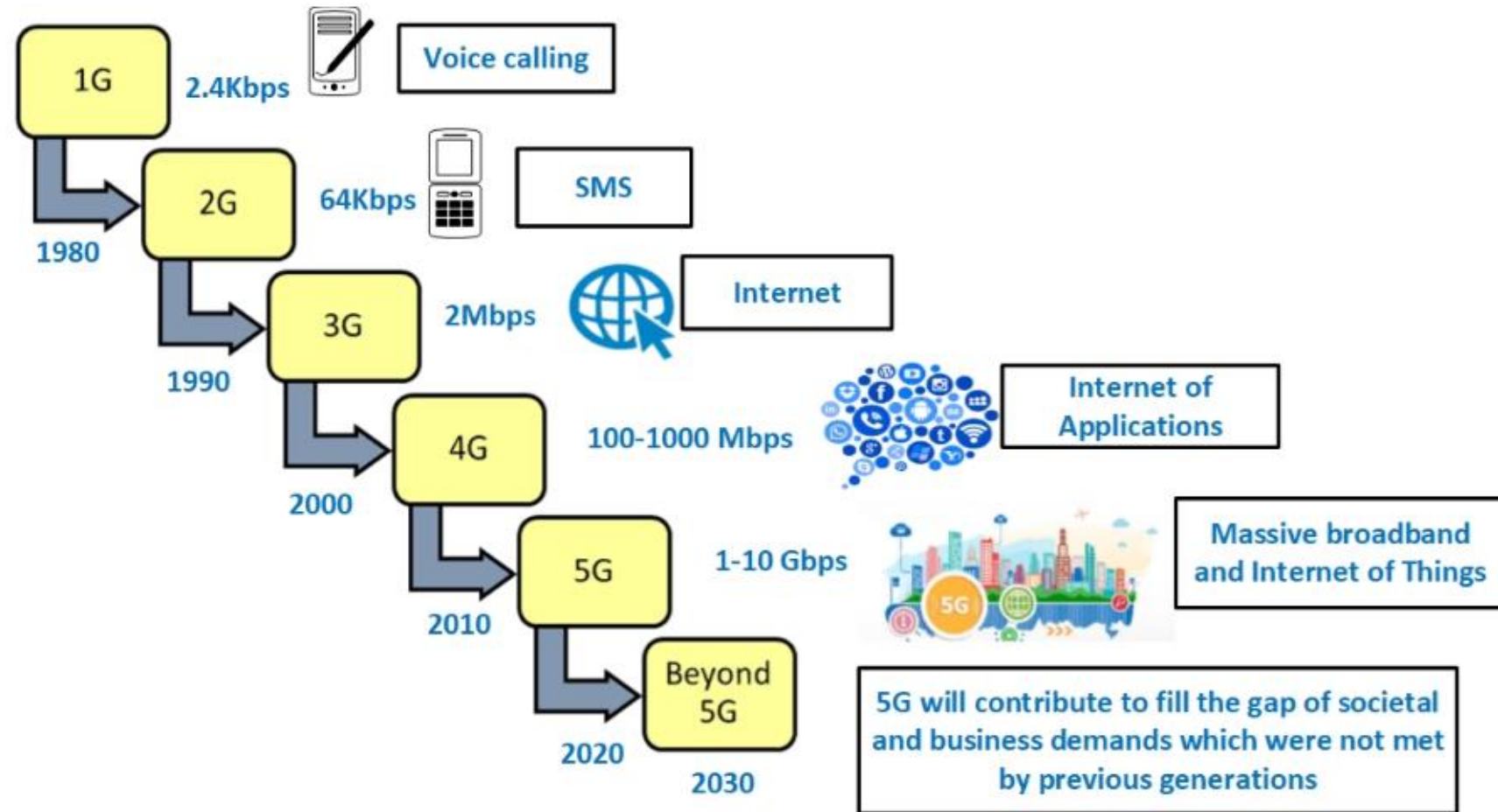
# How Wi-fi works?

- A Wi-Fi based wireless network sends signals using radio.
- In a typical Wi-Fi network, the AP (Access Point) will advertise the specific network that it offers connectivity to. This is called a Service Set Identifier (SSID).
- A client device receives the beacon transmitted by the AP and converts the RF signal into digital data, then that data is passed along to the device for interpretation.
- Data from the client (or from the AP to the client) is converted from digital data into an RF modulated signal and transmitted over the air. When received, this is de-modulated, converted back to digital data, and then forwarded along to its destination.

# Evolution of Wi-fi Standards

Wi Fi Generation	Maximum Theoretical Transfer Rate	Frequency
802.11	2Mbps	2.4GHz
802.11b	11Mbps	2.4GHz
802.11a	54Mbps	5GHz
802.11g	54Mbps	2.4GHz
Wi Fi 4(802.11n)	600Mbps	2.4GHz/5GHz
Wi Fi 5(802.11ac)	~6900Mbps(6.9Gbps)	5GHz
Wi Fi 6(802.11ax)	~9600Mbps(9.6Gbps)	2.4GHz/5GHz
Wi Fi 6E(802.11ax)	~9600Mbps(9.6Gbps)	6GHz

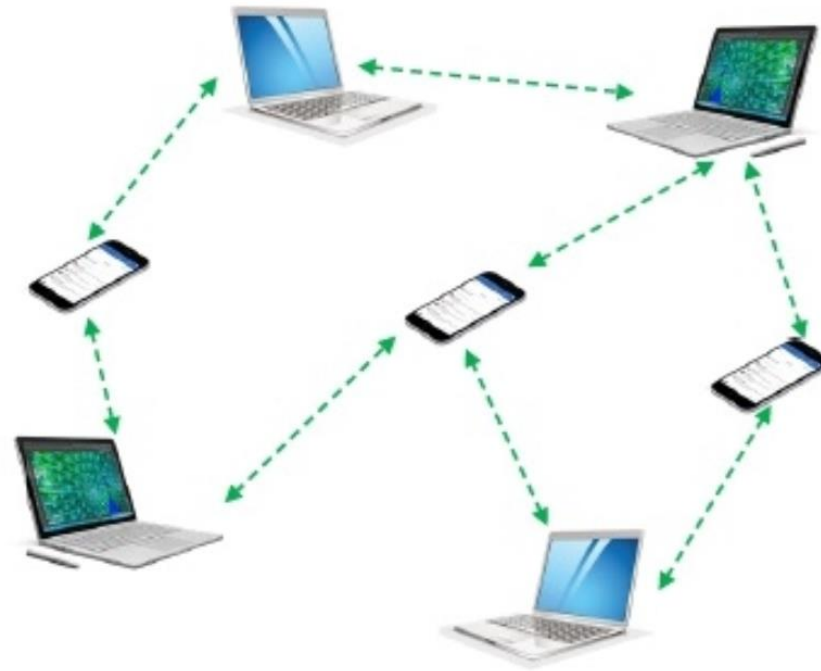
# Evolution of Mobile Communications Standards



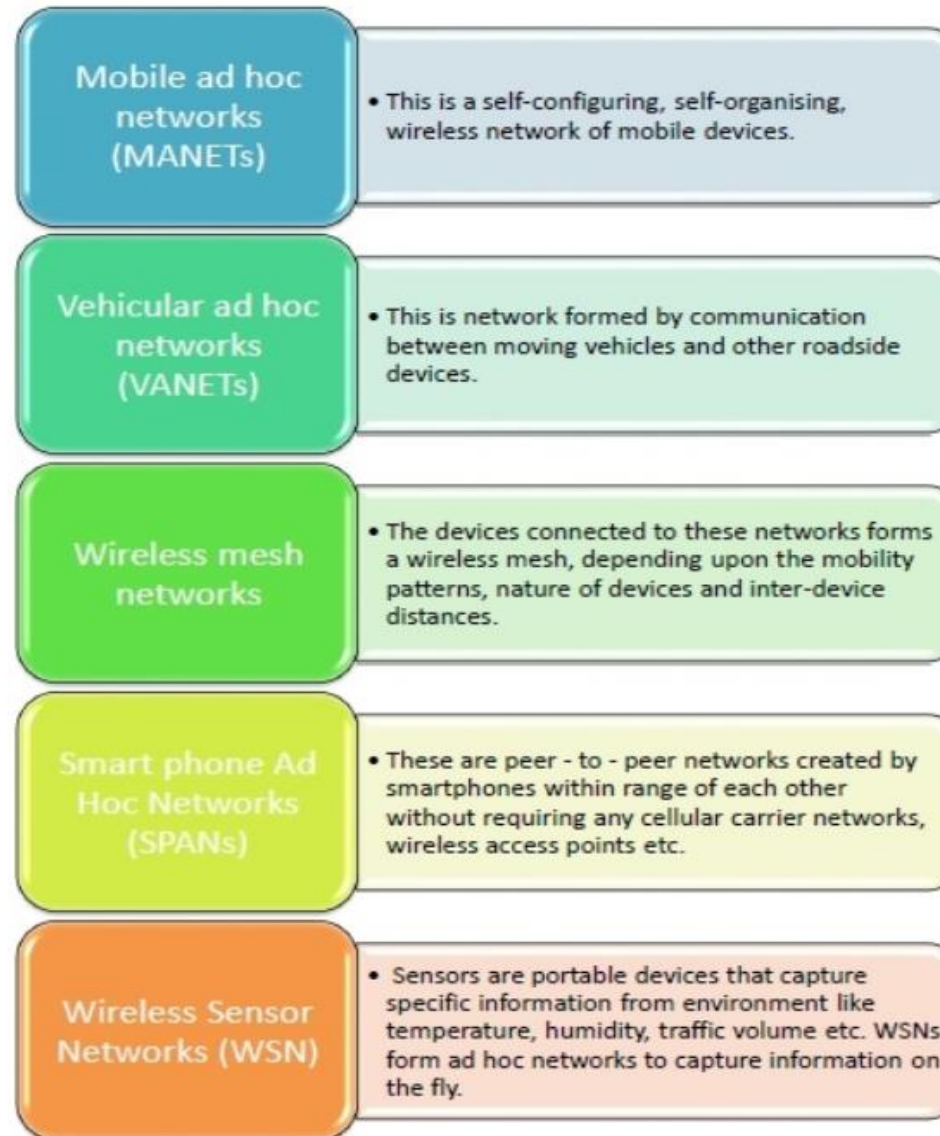
Timeline of Mobile communication generations [27]

# Overview of Ad-hoc Networks

An ad-hoc network is one that is spontaneously formed when devices connect and communicate with each other. Ad-hoc networks are mostly wireless in nature where devices communicate with each other directly instead of relying on a base station or access points.



# Types of Ad-hoc Networks



# Pros and cons of Ad-hoc Networks

## **Pros:**

1. Separation from central network administration.
2. Each node can play both the roles ie. of router and host showing autonomous nature.
3. Self-configuring and self-healing nodes do not require human intervention.
4. Highly scalable and suits the expansion of more network hub.

## **Cons:**

1. Resources are limited due to various constraints like noise, interference conditions, etc.
2. Lack of authorization facilities.
3. More prone to attacks due to limited physical security.
4. There is a huge delay in the transfer of data between two sleeping nodes.

