## Week 1

### Define following terms and concepts shortly:

* **Network Bandwidth:** This is simply defined as the maximum amount of data that can be transmitted over a network connection in a given period of time. The higher the bandwidth, the more data can be transmitted transferred at once which allows faster download and upload rate.

Think of it like a highway: bandwidth is the number of lanes available. More lanes (higher bandwidth) allow more cars (data) to travel at the same time, reducing congestion.

* Network throughput: Network Throughput is the actual amount of data which are transmitted over a network connection in a given period of time.
* **Packet Loss and jitter:** Packet loss is failing to reach the destination while packet transmitting from one to another. It usually happens in UDP connections. In TCP. Packets are retransmitted in case of packet loss. On the other hand, Jitter refers to the inconsistency in the time it takes for data packets to travel from one to another. Ideally, data packets should arrive at regular intervals, but due to various network issues, they sometimes arrive at uneven times.
* **Bps vs Bps:** bps (bits per second) measures data transfer speed in bits, while Bps (bytes per second) measures it in bytes, with 1 byte equaling 8 bits. Since 1 byte = 8 bits, a 1 MBps speed is 8 times faster than 1 Mbps.
* **Protocol Payload:** A protocol payload refers to the actual data being transmitted over a network within a packet, excluding the headers or metadata added by the protocol for routing, addressing, or error checking.
* **Protocol overhead (especially for resource-constrained IoT purposes):** Protocol overhead is the extra information added to data, like headers and control details, to help manage communication. For small IoT devices with limited resources like battery, memory, and network speed, keeping this extra data small is important. Too much overhead can slow things down, use more power, and make communication less efficient.
* **Spanning Tree Protocol:** Spanning Tree Protocol (STP) is a network protocol used to prevent loops in a network with multiple switches. When switches are connected in a loop, data can circulate endlessly, causing issues like network slowdowns or failures.
* **Colision Domain:** A collision domain is a part of a network where data packets can collide with each other when two or more devices try to send data at the same time. In such cases, the devices have to wait and resend the data, which can slow down the network.
* **Broadcast Domain:** A broadcast domain is a section of a network where any broadcast message sent by a device is received by all other devices in that domain. In simpler terms, when one device sends a message meant for all, every device within the same broadcast domain can hear it. Routers typically separate broadcast domains, while switches and hubs do not, meaning all devices connected to the same switch are in the same broadcast domain. Keeping broadcast domains small can help reduce unnecessary traffic and improve network performance.
* **SOHO network:** A SOHO network (Small Office/Home Office network) refers to a network setup designed for small businesses or home offices. It typically includes basic networking devices like routers, switches, and wireless access points to connect computers, printers, and other devices.
* **MAC (physical) address:** A MAC (Media Access Control) address is a unique identifier assigned to a network interface card (NIC) or device for use in network communication. It's a physical address embedded into the hardware by the manufacturer, and it helps devices on the same local network identify and communicate with each other. A MAC address is usually written as a series of hexadecimal numbers separated by colons or hyphens, like 00:1A:2B:3C:4D:5E.
* **Physical layer protocol data unit (PDU):** A Physical Layer Protocol Data Unit (PDU) is the basic unit of data that is transmitted over a network at the physical layer of the OSI model. It represents the raw bits or signals sent across the physical medium, such as electrical voltages, light pulses, or radio waves.
* A **MAC (Media Access Control) layer Protocol Data Unit (PDU)**, often called a **frame**, is the unit of data handled by the MAC layer of the OSI model. It includes both the payload (the actual data being transmitted) and the MAC header, which contains addressing and control information necessary for managing access to the network medium and ensuring proper data delivery.
* Half-duplex vs Full-Duplex: **Half-duplex**: Data transmission can occur in both directions, but not simultaneously. Devices must take turns sending and receiving data. An example is a walkie-talkie, where you need to switch between talking and listening.

**Full-duplex**: Data transmission can occur in both directions simultaneously. Devices can send and receive data at the same time. An example is a telephone call, where both parties can talk and listen simultaneously.

* **Ethernet auto-negotiation:** Ethernet auto-negotiation is a feature that allows Ethernet devices to automatically determine the best possible connection settings when they connect. This includes selecting the optimal speed (like 10/100/1000 Mbps) and duplex mode (half or full-duplex).
* **Hidden node problem (wireless):** The hidden node problem in wireless networks occurs when two devices are within range of a common access point but out of range of each other. This means they can't detect each other’s transmissions, which can lead to collisions at the access point. For example, if Device A and Device B both try to send data to the same access point at the same time, their signals might collide because neither device can "see" the other’s transmission.
* **Physical Topology:** This refers to the actual physical layout of the network hardware, including the devices (like computers and routers) and the physical connections (cables, switches, etc.) between them. It shows how the hardware components are physically arranged and connected.

**Logical Topology:** This refers to how data flows through the network and how devices communicate with each other, regardless of the physical layout. It represents the logical or conceptual arrangement of the network, focusing on how data is transferred and how network services are provided.

For example, a network might have a physical star topology (where all devices are connected to a central switch) but use a logical bus topology (where data appears to travel along a single shared channel).

* **TIA/EIA-568**: This is a standard developed by the Telecommunications Industry Association (TIA) and the Electronic Industries Alliance (EIA) that defines the wiring schemes for twisted-pair cabling used in Ethernet networks.

**ISO/IEC 11801:** This is an international standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It provides guidelines for the generic cabling systems used in commercial buildings, including the design and installation of cabling to support various types of networks, such as Ethernet, telephone, and data communication

* **Ethernet cabling categories. For example, CAT 6**: Ethernet cables come in various categories, such as CAT 5e, CAT 6, CAT 6a, CAT 7, and CAT 8. Each category supports different speeds and frequencies, with higher numbers offering better performance and reduced interference. For example, CAT 6 supports speeds up to 1 Gbps, while CAT 8 supports speeds up to 40 Gbps.
* **8P8C** (8 Position 8 Contact) is a type of modular connector commonly used in Ethernet cables, often referred to as **RJ45**. It features eight pins for connecting eight wires, allowing for network data transmission and reception.
* Wifi AD HOC: Wi-Fi ad hoc mode is a wireless network setup where devices connect directly to each other without using a central access point or router. In this mode, devices communicate peer-to-peer, allowing for temporary and spontaneous network connections. It's often used for small, local networks or in situations where a traditional infrastructure network isn't available.
* IEEE 802.11ac (Wi-Fi 5): Faster Wi-Fi on the 5 GHz band, improving speed and efficiency.

IEEE 802.11ax (Wi-Fi 6): Better performance in crowded areas, with higher speeds and improved battery life, working on both 2.4 GHz and 5 GHz bands.

IEEE 802.11be (Wi-Fi 7): The newest standard, offering even faster speeds and better performance in busy environments.