Session#4 Part 1

Introduction on How The Internet Works

- Because the Internet is a global network of computers each computer connected to the Internet must have a unique address. Internet addresses are in the form nnn.nnn.nnn.nnn where nnn must be a number from 0 - 255. This address is known as an **IP address** . (IP stands for Internet Protocol).
- If you connect to the Internet through an **Internet Service Provider (ISP)** , you are usually assigned a temporary IP address for the duration of your dial-in session. If you connect to the Internet from a **local area network (LAN)** your computer might have a permanent IP address or it might obtain a temporary one from a **DHCP (Dynamic Host Configuration Protocol)** server. In any case, if you are connected to the Internet, your computer has a unique IP address.
- Some types of hardware that support the Internet include routers, servers, cell phone towers, satellites, radios, smartphones and other devices. All these devices together create the network of networks. The Internet is a malleable system -- it changes in little ways as elements join and leave networks around the world. Some of those elements may stay fairly static and make up the backbone of the Internet.

The Difference between Local and Puplic IP addresses

Local IP address:

- It's the address which is assigned automatically by the router with default settings. It's hidden from the outside world and used only inside your private network.
- The local IP address can change depending on what other devices are connected to the same network and in what order they were connected. Most network routers assign IP addresses starting at `192.168.1.2`, and increment the last digit with each new device that connects.
- You can assign devices specific IP addresses in the router control panel, so that a device will always receive the same local IP address when it connects. This is called a static local IP address.

Puplic IP address:

- The Internet Service Provider (ISP) assigns you an external IP address when you connect to the Internet. When your web browser requests a webpage, it sends this IP address along with it. Your ISP uses this to know which of its customers are requesting which webpage. Also, any website that you visit will have access to this IP address.
- An example for external IP address `162.158.150.122`.

IP address allocation(Static, DHCP)

Static IP address:

A static IP address is an address that is permanently assigned to your network devices by your ISP, and does not change even if your device reboots. It has typically have two versions: IPv4 and IPv6. And here are some static IP advantages:

- Address does not change over time unless it is changed manually - good for web servers, and email servers.
- Using DNS to map domain name to IP address, and using domain name to address the static IP address.

DHCP (Dynamic Host Configuration Protocol):

Dynamic IP address is an address that keeps on changing. DHCP is a way of dynamically and automatic assigning IP addresses to network devices on a physical network. It provides an automated way to distribute and update IP addresses and other configuration information over a network. And here are some dynamic IP advantages:

- Computers with Dynamic IP address have relatively lower security risk .
- The user does not have to do the network configuration. It's done by DHCP.

Data Packets

What are data packets?

A data packet is a unit of data which is transmitted through the Internet. This is what the Internet Protocol uses. Data heavy networks will also use the concept of a data packet to transmit information. A packet has the following components:

- A **source address** specifying the sending computer.
- A **destination address** specifying where the packet is being sent.

- **Instructions** telling the computer how to pass the data on.
- **Reassembly information** (if the packet is part of a longer message).
- The data to be transmitted to the remote computer (often called the **packet payload**).
- **Error-checking information** to ensure that the data arrives intact.

These components are assembled into slightly larger chunks. Each packet consists of three distinct parts, each part contains some of the components listed above:

- **Header** : typically includes an alert signal to indicate that the data is being transmitted, source and destination addresses, and clock information to synchronise the transmission.
- **Data** : The actual data being sent. It can vary (depending on the network) from 48 bytes to 4 kilobytes.
- **Trailer** : The contents of the trailer (or even its existence) can vary among network types, but it normally includes a Cyclic Redundancy Checksum (CRC) which lets the network determine whether or not a packet has been damaged in transmission.

Gateways.

A gateway is a network point that works as an access to another network. Generally in intranet a node can be either a gateway node or the nodes that join the network are gateways.
Gateway security: A gateway generally works as a safeguard to a local network and also connects the local network to public network. A gateway offers security just like a firewall with the technique of NAT.
Gateway get packets from the local network and alternate its exterior IP address and a new port address into the resource fields of the IP and UDP headers.
Gateways can take several forms and perform a variety of tasks. These include:

- **Web application firewall** - filters traffic to and from a web server and look at application-layer data.
- **Cloud storage gateway** - translates storage requests with various cloud storage service API calls.
- **Email security gateway** - prevents the transmission of emails that break company policy or will transfer information with malicious intent.
- **Media gateway** - converts data from the format required for one type of network to the format required for another.

An example for a default Gateway : `192.168.1.1`

Network Address Classes

With an IPv4 IP address, there are five classes of available IP ranges: Class A, Class B, Class C, Class D and Class E, while only **A, B, and C** are commonly used. Each class allows for a range of valid IP addresses, shown in the following table.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.

Class	Address Range	Supports
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or research and development purposes.

Note: Ranges 127.x.x.x are reserved for the loopback or localhost, for example, 127.0.0.1 is the loopback address. Range 255.255.255.255 broadcasts to all hosts on the local network.

Subnet Masking

- A subnet mask is a 32-bit number used to differentiate the network component of an IP address by dividing the IP address into a network address and host address. It does so with bit arithmetic whereby a network address is bit multiplied by the subnet mask reveal the underlying subnetwork.
- It hides the network part of a system's IP address and leaves only the host part as the machine identifier. It uses the same format as an IPv4 address – four sections of one to three numbers, separated by dots. Each section of the subnet mask can contain a number from 0 to 255. For example, a typical subnet mask for a Class C IP address is: `255.255.255.0`

Why Use Subnetting?

- **Conservation of IP addresses:** Imagine having a network of 20 hosts. Using a Class C network will waste a lot of IP addresses (254-20=234). Breaking up large networks into smaller parts would be more efficient and would conserve a great amount of addresses.
- **Reduced network traffic:** The smaller networks created the smaller broadcast domains are formed hence less broadcast traffic on network boundaries.
- **Simplification:** Breaking large networks into smaller ones could simplify fault troubleshooting by isolating network problems down to their specific existence.

Domain Name Systems(DNS)

What a DNS is ?

- The Domain Name Systems (DNS) is the phonebook of the Internet. Humans access information online through domain names, like google.com or yahoo.com. Web browsers interact through Internet Protocol (IP) addresses. DN S translates domain names to IP addresses so browsers can load Internet resources.
- Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as `192.168.1.1` (in IPv4), or more complex newer alphanumeric IP addresses such as `2400:cb00:2048:1::c629:d7a2` (in IPv6).

DNS Server Hierarchy

The DNS hierarchy is comprised of the following elements:

- **Root Level:** The DNS root level is the highest level in the DNS hierarchy tree. The root name server is the name server for the root zone. It answers the requests for records in the root zone and answers other requests by providing a list of authoritative name servers for the appropriate TLD (top-level domain).

> Organizational hierarchy such as .com, .net, .org.
> Geographic hierarchy such as .uk, .fr, .pe.

- **Top Level Domains:** The next level in the DNS hierarchy is Top level domains. There are many TLDs available at the moment. As we have seen the TLDs are classified as two sub categories. They are organizational hierarchy and geographic hierarchy. Let us see each in detail.
- **Second Level Domains:** The next level in the DNS hierarchy is the Second Level Domains. This is the domain that is directly below the TLD. This is the main part of the domain name. It can vary according to the buyer. There are no limits here as the tlds. Once the domain is available anyone can purchase it. If the domain is unavailable at the moment, same 2nd level name with other tlds is the best option.
- **Sub-domain:** The sub-domain is the next level in the DNS hierarchy. The sub-domain can be defined as the domain that is a part of the main domain. The only domain that is not also a sub-domain is the root domain. Suppose two domains. one.example.com and two.example.com. Here, both the domains are the sub-domains of the main domain example.com and the example.com is also a subdomain of the com top level domain.
- **Host**

Open Systems Interconnection(OSI) Model

What is OSI Model ?

- The Open Systems Interconnection (OSI) Model is a conceptual and logical layout that defines network communication used by systems open to interconnection and communication with other systems.
- The model is broken into seven subcomponents, or layers, each of which represents a conceptual collection of services provided to the layers above and below it. The OSI Model also defines a logical network and effectively describes computer packet transfer by using different layer protocols.

The OSI layers are :

- **Application Layer:** This is the topmost layer in the seven OSI Layers. This is the layer that the end-user (can be a computer programmer, or a regular PC user) is actually interacting with. This layer allows access to network resources.
- **Presentation Layer:** This is the layer in which the operating system operates with the data. Main functions of this layers includes translation, encryption and compression of data. Basically User interacts with Application layer, which sends the data down to Presentation layer.

- **Session Layer:** This layer has the job of maintaining proper communication by establishing, managing and terminating sessions between two computers. For example, whenever we visit any website, our computer has to create a session with the web server of that website.
- **Transport Layer:** This layer decides how much information should be sent at a time. So, when you are communicating with a website, this layer will decide how much data you can transfer and receive at a given point of time. Also, this layer provides reliable process to process message delivery and error recovery.
- **Network Layer:** The main job of this layer is to move packets from source to destination and provide inter-networking. This is the layer that the routers operate on. Since routers operate at the network level, hence we can say that the IP address is at the network level.
- **Data Link Layer:** This layer is responsible for organising bits into frames and ensuring hop to hop delivery. This is the layer on which the Switches operate on. Since routers operate at the network level, hence we can say that the MAC address resides at the data link layer.
- **Physical Layer:** This is the layer on which the real transmission of data bits takes place through a medium. This layer is, as the name suggests, all the physical stuff that connects the computers together.

Network Protocols

What are network protocols ?

A **network protocol** is a set of established rules that dictates how to format, transmit and receive data so computer network devices -- from servers and routers to endpoints -- can communicate regardless of the differences in their underlying infrastructures, designs or standards.

Some types of protocols:

- **FTP ->** File transfer protocol is basically used for transferring files to different networks.
- **SMTP ->** Simple mail transfer protocol manages the transmission and outgoing mail over the internet.
- **HTTP ->** HTTP is based on client and server model, It is used for making a connection between the web client and web server.
- **Ethernet ->** Ethernet is a most important for LAN communication. Ethernet transmits the data in digital packets.

Difference between TCP and UDP protocols :

	TCP	UDP
Connection	Connection-oriented	Connectionless

| Sequencing | TCP numbers each packet so they can be arranged in a sequence by the recipient | UDP sends the packets without numbering
| Speed | Slower | Faster |
| Reliability| High | Low |
| Header size | Packets are heavy because of overheads | Lightweight packets with minimal headers

| Transfer method | Stream | Individual packets |
| Applications | File transfer, email, web browsing | Video conferencing, gaming, broadcasts|

Ports

What is a port?

- **ports** are part of the addressing information used to identify the senders and receivers of messages. They are associated with TCP/IP network connections and might be described as a sort of add-on to the IP address.
- **Networking ports** are software-based and unrelated to physical ports that network devices have for plugging in cables.

Some examples on a common ports:

Port	Service
20/21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
80	Hypertext Transfer Protocol (HTTP)
443	Hypertext Transfer Protocol (HTTPS)