**PLATFORM ENGINEERING ASSIGNMENT**

**NAME:** Muthuvarshini S

**REG:** 2021506054

**1) IPv4 – INTERNET PROTOCOL VERSION 4:**

Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides the logical connection between network devices by providing identification for each device.

**IPv4 Address :**

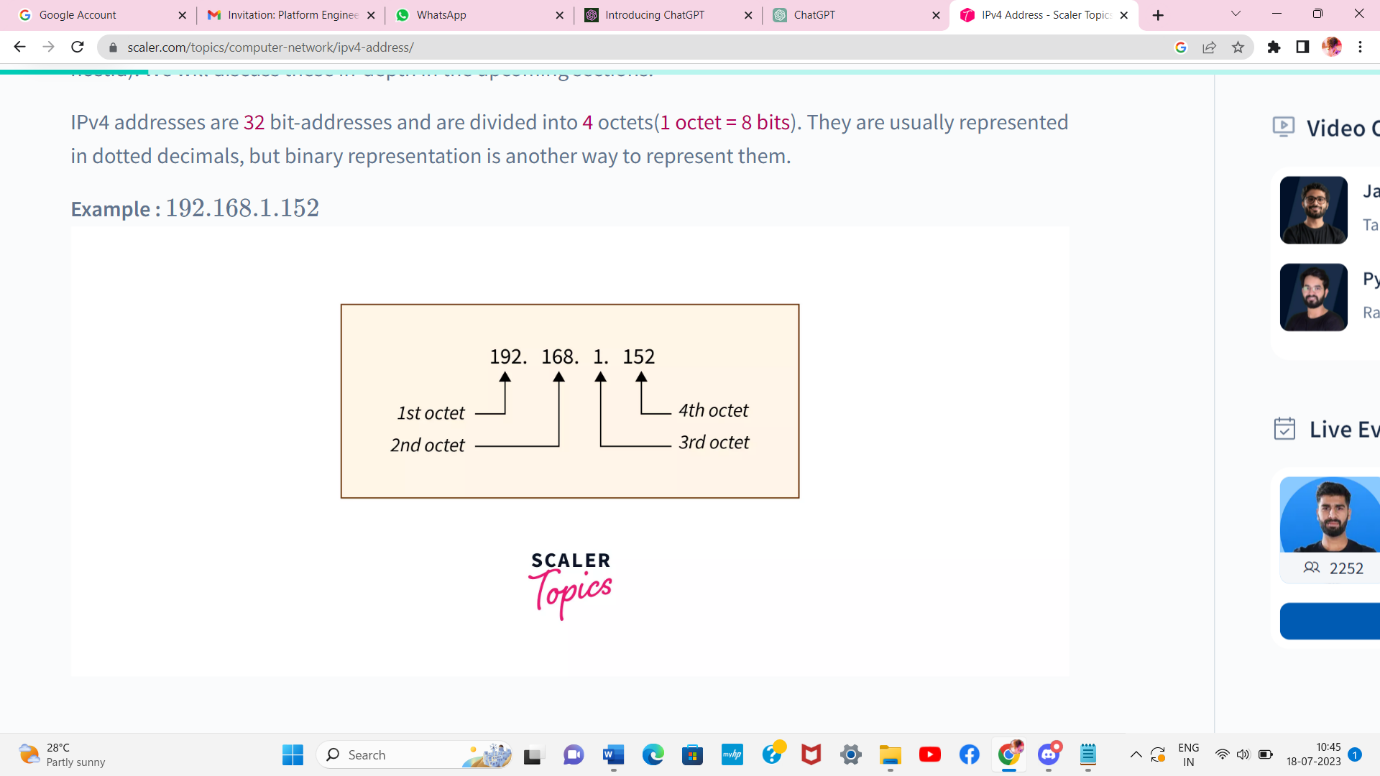
Consider the example of the telephone. If we want to make a call to someone using a telephone, it is only possible when we know the phone number of the other person. Without knowing the phone number, it is not possible to make a call. In the same way, if we want to send data to any host on the internet, we need the address of the recipient. This allows us to uniquely identify the host on the internet so that the data is transferred and communication is established between that particular host.

IP addresses are of two types - IPv4 and IPv6 addresses. IPv4 is a 32-bit address and IPv6 are 128-bit address. The 'v' in IPv4 and IPv6 stands for version. The IPv4 address or the Internet Protocol Address is the fourth version of the Internet Protocol. It is a unique address.

The IPv4 address is divided into two parts - the network part and the host part(also referred to as netid and hostid). We will discuss these in-depth in the upcoming sections.

IPv4 addresses are 32 bit-addresses and are divided into 4 octets(1 octet = 8 bits). They are usually represented in dotted decimals, but binary representation is another way to represent them.

**Example :** 192.168.1.152



**Key features:**

32-bit Address Format: IPv4 addresses are 32 bits long and are represented in the decimal format with four octets separated by dots (e.g., 192.168.0.1). Each octet can have a value ranging from 0 to 255, allowing for approximately 4.3 billion unique addresses.

**Public and Private IP Addresses:** IPv4 addresses are divided into public and private address spaces. Public addresses are globally unique and routable over the internet, while private addresses are used within private networks (like your home or office) and are not routable over the internet. This allows for conservation of public IP addresses.

**Subnetting:** To efficiently allocate IP addresses and manage networks, IPv4 allows for subnetting. Subnetting involves dividing a larger IP address block into smaller, more manageable sub-networks, each with its own range of IP addresses.

**Classful Addressing:** In the early days of IPv4, IP addresses were divided into classes, known as classful addressing (Class A, Class B, Class C, Class D, and Class E). This division was based on the number of network and host bits, but it has become obsolete with the introduction of Classless Inter-Domain Routing (CIDR).

**CIDR (Classless Inter-Domain Routing**): CIDR is a method used to allocate IP addresses more efficiently. Instead of using fixed-length subnet masks as in classful addressing, CIDR uses variable-length subnet masks (e.g., 192.168.0.0/24), allowing for more flexibility in address allocation.

**Advantages of IPv4 Addressing**

* IPv4 is a connectionless protocol.
* The IPv4 routing can be handled easily by all the systems.
* Across a large network, IPv4 can connect various devices and along with connection, the verification can also be done. This is done without the use of **NAT** (Network Address Translation)
* The process of routing is carried out smoothly because the addresses are combined more effectively.
* Privacy and security are maintained in IPv4 as the data is encrypted in the packets.
* The encoding in IPv4 is flawless.

**Disadvantages of IPv4 Addressing**

* IPv4 can be assigned manually or by a protocol known as DHCP and if it is done through DHCP, it needs a lot of management for its infrastructure.
* Since IPv4 was established way back, its implementation did not provide security against threats introduced today. **Internet Protocol Security** (IPSec) enables network security to IPv4 by specifying the use of the internet. But the problem arises when IPSec is not built-in and its implementation is optional.
* Most of the IP addresses are reserved in the United States.
* To overcome the drawbacks of IPv4, IPv6 was introduced.

**2) IPv6 – INTERNET PROTOCOL VERSION 6:**

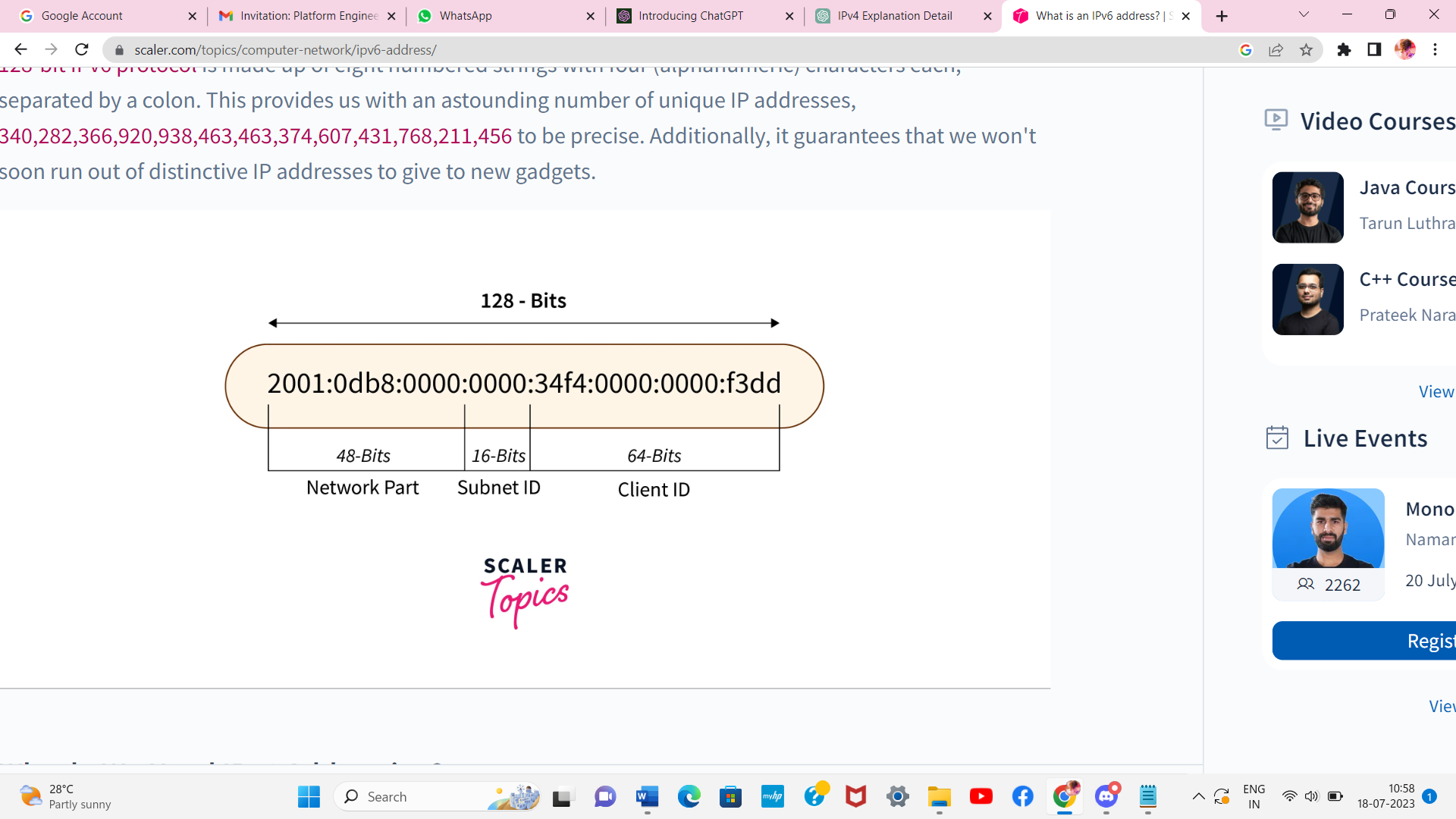
IPv6, which stands for Internet Protocol version 6, is the successor to IPv4 and is designed to address the limitations of its predecessor. It was standardized in 1998 by the Internet Engineering Task Force (IETF) to replace IPv4, primarily to provide a larger address space and overcome the exhaustion of available public IP addresses. IPv6 uses 128-bit addresses, which allows for an exponentially larger number of unique addresses compared to the 32-bit addresses used in IPv4.

**IPv6 Address :**

Information can be exchanged between devices on a network thanks to IP addresses, which serve as identification. There must be a way for computers, routers, and webpages to be distinguished on the internet. A method for achieving this is provided by IP addresses, which are crucial to the operation of the internet.

The new generation IP address, or IPv6, was created primarily to get over IPv4's limits and exhaustion. The 128-bit IPv6 protocol is made up of eight numbered strings with four (alphanumeric) characters each, separated by a colon.

This provides us with an astounding number of unique IP addresses, 340,282,366,920,938,463,463,374,607,431,768,211,456 to be precise. Additionally, it guarantees that we won't soon run out of distinctive IP addresses to give to new gadgets.



**Types of IPv6 Addresses:**

There are three addressing methods available in IPv6 representation:

**Unicast Address** – A single network interface is detected by a unicast address. A unicast address directs a packet to the interface that the address designates.

**Multicast Address** – A group of hosts referred to as a multicast address purchases a multicast destination address. These hosts don't have to be close by geographically. All interfaces belonging to that multicast address will receive any packet transmitted to this multicast address.

**Anycast Address** – A collection of interfaces has been assigned an Anycast Address. Whenever a packet is sent to an anycast address, only one member interface will receive it.

**Key features:**

**128-bit Address Format**: IPv6 addresses are 128 bits long and are represented in hexadecimal format with eight groups of four hexadecimal digits separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). This results in approximately 340 undecillion unique addresses (3.4 x 10^38), providing a virtually unlimited address space.

**Simplified Header:** The IPv6 header is more streamlined compared to IPv4, with a fixed size of 40 bytes. It eliminates some of the rarely used fields present in the IPv4 header, making packet processing more efficient.

**No More NAT (Network Address Translation) Requirement:** The vast number of available IPv6 addresses eliminates the need for Network Address Translation (NAT) to share a single public IP address among multiple private devices. Each device can have its unique global IPv6 address, promoting end-to-end connectivity.

**Autoconfiguration (SLAAC and DHCPv6):** IPv6 supports stateless address autoconfiguration (SLAAC), which allows devices to generate their unique IP addresses based on the network prefix provided by the router. Additionally, Dynamic Host Configuration Protocol version 6 (DHCPv6) can be used for stateful address assignment and additional configuration options.

**Improved Security:** IPv6 includes built-in support for IPsec (Internet Protocol Security), which provides encryption and authentication of IP packets, enhancing network security at the IP layer.

**Mobility Support:** IPv6 includes native support for mobile devices, enabling seamless handovers between different networks without changing the device's IP address.

**Flow Labeling:** IPv6 includes a flow label field in the header, which can be used to identify and provide special handling for specific packets within a flow, such as real-time multimedia data.

**Advantages of IPv6 Address:**

* Efficient Routing – With IPv6, routing becomes more streamlined and hierarchical while also shrinking the size of routing tables. In IPv6 networks, the source device manages fragmentation using a protocol for the detection of the path's maximum transmission unit rather than a router.
* Efficient Packet Processing – The checksum does not need to be regenerated at each router hop because IPv6 does not include an IP-level checksum as IPv4 does.
* Directed Data Flows – Multicast is supported by IPv6 as opposed to broadcast. Network bandwidth can be conserved by using multicast to simultaneously send packet flows that use a lot of bandwidth to several destinations.
* Security – IPv6 is built using IPSec security, which offers data integrity, confidentiality, and authentication.

**Disadvantages of IPv6 Address:**

* The network infrastructure becomes overworked when routing table entries are needed for such a large number of networks.
* Older devices that do not support IPv6 must be manually set up using the Daul stack approach, adding extra effort for the network administrator.
* The globe is slow to switch to IPV6 and IPV4 is still widely used.

**3) IP ADDRESSING SCHEMES WITH EXAMPLES:**

IP addressing schemes are methods used to allocate and manage IP addresses in a network. There are two primary IP addressing schemes: IPv4 addressing and IPv6 addressing. Let's explore each scheme with examples:

**IPv4 Addressing Scheme:**

IPv4 addresses consist of 32 bits and are commonly represented in a dotted-decimal notation, where each octet is expressed in decimal format. The address is divided into two parts: the network portion and the host portion.

**Example of an IPv4 address:** 192.168.0.1

In this example, the IP address 192.168.0.1 is divided into the following components:

Network Portion: 192.168.0

Host Portion: 1

IPv4 addresses are further categorized into classes and subnetted using CIDR notation.

**Example of an IPv4 address with CIDR notation:** 203.0.113.0/24

In this example, the IP address 203.0.113.0 is accompanied by a subnet mask of /24, indicating that the first 24 bits represent the network portion, and the remaining 8 bits represent the host portion.

**IPv6 Addressing Scheme:**

IPv6 addresses consist of 128 bits and are represented in hexadecimal format with colons separating each group of 16 bits.

**Example of an IPv6 address:** 2001:0db8:85a3:0000:0000:8a2e:0370:7334

In this example, the IPv6 address is divided into the following components:

Network Portion: 2001:0db8:85a3:0000

Subnet ID: 0000

Interface ID: 8a2e:0370:7334

IPv6 addresses are typically assigned with a /64 prefix length for efficient subnetting and autoconfiguration.

**Example of an IPv6 address with a subnet prefix**: 2001:0db8:85a3::/64

In this example, the IPv6 address 2001:0db8:85a3:: is accompanied by a /64 prefix length, indicating that the first 64 bits represent the network and subnet portion, and the remaining 64 bits are available for addressing individual hosts within that subnet.

**4) RESERVED PORTS:**

Reserved ports, also known as well-known ports, refer to a set of specific network port numbers that are reserved for well-known services and applications in the TCP and UDP protocols. These port numbers range from 0 to 1023 and are standardized by the Internet Assigned Numbers Authority (IANA). The reservation of these ports helps ensure consistency, interoperability, and security in network communications across different systems and networks.

**Characteristics of reserved ports:**

**Port Number Range**: Reserved ports cover the range of port numbers from 0 to 1023. These are the lowest and most privileged port numbers available in the TCP and UDP protocols.

**Well-Known Services:** Many popular services and applications have been assigned specific port numbers in the reserved range. This allows for easy identification and standardized communication across the internet. Examples of well-known ports include port 80 for HTTP (web browsing), port 443 for HTTPS (secure web browsing), port 21 for FTP (file transfer), port 22 for SSH (secure shell), port 25 for SMTP (email), port 53 for DNS (domain name system), and more.

**Privileged Ports:** Ports in the reserved range are often referred to as "privileged ports" because only processes running with administrative or root privileges on a system can bind to these ports. This restriction helps prevent unauthorized applications from using these well-known port numbers, enhancing security and stability.

**Standardization and Interoperability**: The assignment of specific port numbers to well-known services ensures that applications and services across different platforms and operating systems can communicate with each other in a standardized manner. This uniformity enables seamless interoperability, making it possible for a web browser on one system to connect to a web server on another, regardless of the underlying technology.

**Avoiding Port Conflicts**: The use of reserved ports helps avoid conflicts between different services that might attempt to use the same port number. By following the established port assignments, developers and administrators can prevent communication issues and potential vulnerabilities in the network.

**Examples of reserved ports in TCP/IP include:**

Port 20 (TCP/UDP): FTP Data Transfer

Port 21 (TCP): FTP Control

Port 22 (TCP/UDP): SSH (Secure Shell)

Port 23 (TCP): Telnet

Port 25 (TCP): SMTP (Simple Mail Transfer Protocol)

Port 53 (UDP/TCP): DNS (Domain Name System)

Port 80 (TCP): HTTP (Hypertext Transfer Protocol)

Port 110 (TCP): POP3 (Post Office Protocol version 3)

Port 443 (TCP): HTTPS (Hypertext Transfer Protocol Secure)

These reserved port numbers are used for well-known services, and applications often use them to listen for incoming connections or communicate with other system.

**How reserved ports are used in each protocol ?**

**TCP (Transmission Control Protocol):**

* In TCP, reserved ports are used to identify and assign specific port numbers to well-known services and applications.
* When a server application wants to offer a service, it listens on a specific port number associated with that service. For example, a web server would listen on port 80 for regular HTTP requests or port 443 for HTTPS requests.
* Client applications use the corresponding reserved port number to connect to the desired service. For example, web browsers use port 80 or 443 when requesting web pages.
* The use of reserved port numbers ensures that the communication between clients and servers occurs through standardized and well-known port assignments, promoting interoperability and consistency.

**UDP (User Datagram Protocol):**

* Similarly to TCP, reserved ports in UDP are used to associate specific port numbers with well-known services and applications.
* Unlike TCP, UDP is a connectionless protocol, meaning it does not establish a persistent connection between the sender and receiver.
* UDP is commonly used for real-time communication and low-latency applications such as audio and video streaming or online gaming.
* Reserved ports help clients and servers find each other for specific services, and they use the assigned port numbers for communication.

**IP (Internet Protocol):**

* IP itself does not directly use reserved ports in the same way as TCP and UDP.
* IP is responsible for routing and forwarding data packets across networks based on IP addresses, while TCP and UDP operate at a higher layer, providing reliable or connectionless communication services.
* However, the IP header includes information about the protocol being used (e.g., TCP or UDP), which helps routers and other network devices direct packets to the appropriate transport layer protocol based on the destination port number.