# WEEKLY TASK

**1. Among A and B, select which one is software layer and which one is hardware layer in Open Systems Interconnection Model.**

**A**

**Application layer**<br>
**Presentation layer**<br>
**Session layer**

**B**

**Network layer**<br>
**Datalink layer**<br>
**Physical layer**

**ANSWER**

- A (Software Layer):

    Application layer
    Presentation layer
    Session layer

- B (Hardware Layer):

    Network layer
    Datalink layer
    Physical layer

**2) HTTPS uses which protocol for security?**

HTTPS (HyperText Transfer Protocol Secure) uses **TLS (Transport Layer Security)** for security. TLS is the successor to SSL (Secure Sockets Layer), and it provides encryption, data integrity, and authentication between the client and server.

**3) Apart from LAN, VAN and MAN, what do you understand by VPN?**

A **VPN (Virtual Private Network)** is a technology that creates a secure and encrypted connection over a less secure network, such as the internet. VPNs are used to ensure privacy and security for data transmitted over the internet by creating a virtual encrypted "tunnel" between the user's device and the VPN server. Here are some key aspects of a VPN:

1. **Privacy and Anonymity:** VPNs mask the user's IP address, making their online activities more private and anonymous.
2. **Security:** VPNs encrypt data, protecting it from hackers and eavesdroppers, especially on public Wi-Fi networks.
3. **Remote Access:** VPNs enable remote users to securely access a private network, such as a company's internal network, as if they were directly connected to it.

4. **Bypassing Geo-restrictions:** VPNs can help users access content that is restricted based on geographic location by making it appear as if they are browsing from a different location.

VPNs are widely used for both personal and business purposes to enhance security, privacy, and accessibility of online resources.

**4) Digital Signatures, As the name sounds are the new alternative to signing a document digitally. What other authenticity you have used over network in regular life.**

In addition to digital signatures, several other methods of ensuring authenticity and security over a network are commonly used in everyday life. Here are some examples:

### 1. Password Authentication:

- Users provide a unique password to verify their identity when accessing accounts or services.

### 2. Two-Factor Authentication (2FA):

- A combination of two different authentication methods, such as a password and a temporary code sent to a mobile device, to enhance security.

### 3. Biometric Authentication:

- Utilizes unique physical characteristics, such as fingerprints, facial recognition, or iris scans, to authenticate users.

### 4. Secure Sockets Layer (SSL)/Transport Layer Security (TLS):

- Protocols used to secure communication between web browsers and servers, ensuring that data is encrypted and authenticated.

### 5. Public Key Infrastructure (PKI):

- Uses a pair of keys (public and private) to encrypt and decrypt messages, ensuring that only the intended recipient can access the information.

### 6. Electronic Certificates:

- Digital certificates issued by a trusted Certificate Authority (CA) that authenticate the identity of the certificate holder.

### 7. Time Stamping:

- Adding a time stamp to a document or message to verify when it was created or sent, providing an additional layer of authenticity.

## 8. Digital Watermarking:

- Embedding information into digital content (images, videos) that helps verify the authenticity of the content and its source.

## 9. Secure Messaging Apps:

- Apps like Signal or WhatsApp use end-to-end encryption to ensure that messages are only accessible to the sender and receiver.

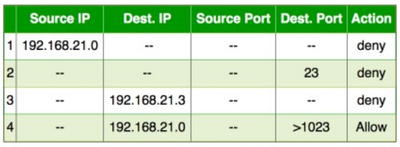
## 10. Hash Functions:

- Used to ensure data integrity by generating a unique hash value for a document; any change in the document will result in a different hash.

These methods work together to provide a secure environment for online transactions and communications, ensuring that users can trust the authenticity of the information they receive and share.

**5) After the authentication is successful, ___**authorization**___(Authorization/Communication) can be used to determine what resources is the user allowed to access and the operations that can be performed.**

**6) A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic, and based on a defined set of security rules it accepts, rejects, or drops that specific traffic.**



| | Source IP | Dest. IP | Source Port | Dest. Port | Action |
|---|---|---|---|---|---|
| 1 | 192.168.21.0 | -- | -- | -- | deny |
| 2 | -- | -- | -- | 23 | deny |
| 3 | -- | 192.168.21.3 | -- | -- | deny |
| 4 | -- | 192.168.21.0 | -- | >1023 | Allow |

Sample Packet Filter Firewall Rule

**Consider above Packet firewall rule. Now Network IP: 192.168.21.0, Trying to connect to your machine and want to send data. IIs the Action allowed, as per above table firewall rule? (Allow/Deny)**

**ANSWER**

• Incoming packets from network 192.168.21.0 are blocked.
•Incoming packets destined for the internal TELNET server (port 23) are blocked.
•Incoming packets destined for host 192.168.21.3 are blocked.
•All well-known services to the network 192.168.21.0 are allowed.

**7) Application Layer Firewall, software Firewall and Hardware Firewall allows only destined and avoids malicious data. If these firewalls are not installed, your application may receive ____**malicious **____ data (malicious / all Secured ) data.**

**8) When a bigger network is divided into smaller networks, in order to maintain security and to maintain smaller networks easier using routing table, we go for ___**subnetting**____(Subnetting/Firewall)**

**9) Move A and B to corresponding IP assignment.**

Static IP Address:

• A) This IP address does not change at any time, which means if an IP address is provided, then it can't be changed or modified and is easily traceable. It is provided by ISP (Internet Service Provider).

Dynamic IP Address:

• B) These addresses change at any time and are not easily traced. While it is provided by DHCP (Dynamic Host Configuration Protocol).

**10)List any two difference between MAC address , IP address and Network Address.**

**1. Purpose and Layer of Operation:**

- **MAC Address**: A MAC (Media Access Control) address is a unique identifier assigned to network interfaces for communications on the physical network segment. It operates at the Data Link Layer (Layer 2) of the OSI model.
- **IP Address**: An IP (Internet Protocol) address is used to identify devices on a network and facilitates routing of data packets between them. It operates at the Network Layer (Layer 3) of the OSI model.
- **Network Address**: This term often refers to an IP address that identifies a particular network rather than an individual device within the network. It is used in the context of routing and subnetting to identify and manage network segments.

2. **Format and Length**:

- **MAC Address**: MAC addresses are typically 48 bits (6 bytes) long and are usually represented in hexadecimal format, such as `00:1A:2B:3C:4D:5E`.
- **IP Address**:
  - **IPv4** addresses are 32 bits (4 bytes) long and are usually represented in decimal format, such as `192.168.1.1`.
  - **IPv6** addresses are 128 bits long and are represented in hexadecimal format, such as `2001:0db8:85a3:0000:0000:8a2e:0370:7334`.
- **Network Address**: A network address can refer to either an IPv4 or IPv6 address with a subnet mask to define the network portion. For example, in IPv4, `192.168.1.0/24` represents a network address where `/24` indicates the subnet mask.

These differences highlight the distinct roles each type of address plays in networking and their different characteristics in terms of operation and representation.

**11. Match numbers with letters according to 7 layers roles:**

**1.Application Layer:**

**2.Presentation Layer:**

**3.Session Layer:**

**4.Transport Layer**

**5.Network Layer**

**6.Data Link Layer**

**7.Physical Layer**

**A. Bit Stream, physical medium, Cable, Connectors**

**B. MAc Address, Flow control, Frames, switches, ARP**

**C. Coding into 1s and 0s, encryption, compression, JPG, HTTPS, SSL,TSL, ASCII, Data**

**D. Authentication, Permission, connection between two hosts, NetBIOS, PPTP, RPC, API, Data**

**E. End-to-End Error Control, TCP, UDP, Segment F. Routing , switching, IPV4,IPV6, IPSec, Packet**

**G. Message format, Human-Machine interfaces, HTTP, FTP, Data**

1.Application Layer:

- G. Message format, Human-Machine interfaces, HTTP, FTP, Data

2.Presentation Layer:

- C. Coding into 1s and 0s, encryption, compression, JPG, HTTPS, SSL, TSL, ASCII, Data

- 3.Session Layer:
  - D. Authentication, Permission, connection between two hosts, NetBIOS, PPTP, RPC, API, Data

4.Transport Layer:

- E. End-to-End Error Control, TCP, UDP, Segment

5. Network Layer:

- F. Routing, switching, IPV4, IPV6, IPSec, Packet

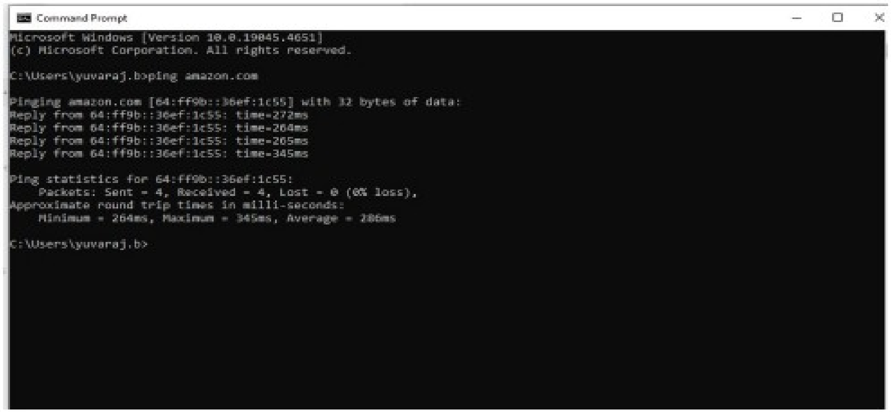
6.Data Link Layer:

- B. MAC Address, Flow control, Frames, switches, ARP

7.Physical Layer:

- A. Bit Stream, physical medium, Cable, Connectors

**12.DNS is a host name to IP address translation service. Use ping amazon.com and share IP address.**



```
Microsoft Windows [Version 10.0.19045.4651]
(c) Microsoft Corporation. All rights reserved.

C:\Users\yuvaraj.b>ping amazon.com

Pinging amazon.com [64:ff9b::36ef:1c55] with 32 bytes of data:
Reply from 64:ff9b::36ef:1c55: time=272ms
Reply from 64:ff9b::36ef:1c55: time=264ms
Reply from 64:ff9b::36ef:1c55: time=265ms
Reply from 64:ff9b::36ef:1c55: time=345ms

Ping statistics for 64:ff9b::36ef:1c55:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 264ms, Maximum = 345ms, Average = 286ms

C:\Users\yuvaraj.b>
```

**13.Consider below network address and subnetID.**

**1. Network Address: 172.16.0.0**

**2. Subnet ID: 172.16.0.0/16**

**From the routing table, which Interface should be choosen for Network ID 172.16.0.0: (A/B)**

**Routing Table:**

**Network ID Subnet Mask Interface**

**200.1.2.0 255.255.255.192 A**

**172.16.0.0 255.255.255.193 B**

To determine which interface should be chosen for Network ID 172.16.0.0, you need to match the subnet mask with the given Subnet ID (172.16.0.0/16).

Here's the comparison:

- **Subnet ID:** 172.16.0.0/16
  - This means the subnet mask is 255.255.0.0.
- **Routing Table:**
  - **Network ID:** 200.1.2.0, Subnet Mask: 255.255.255.192, Interface: A
  - **Network ID:** 172.16.0.0, Subnet Mask: 255.255.255.193, Interface: B

The subnet mask 255.255.255.193 is not a standard subnet mask for a /16 network; it does not cover the range 172.16.0.0/16.

Since none of the subnet masks in the routing table exactly match the /16 mask for 172.16.0.0, but 172.16.0.0 is listed in the routing table, we need to use the longest prefix match. However, if there was a mistake and 255.255.255.192 was intended to be 255.255.0.0 for 172.16.0.0, the correct interface should be:

- **Interface B**, as it corresponds to the network 172.16.0.0 directly.

If the subnet mask 255.255.255.193 is a typo and was meant to be 255.255.0.0, then Interface B should be used. If the mask is correct and you are required to select an interface based on exact match and standard masks, it is likely a routing issue in the table.