

Weekly Assignment

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
- Presentation layer
- Session layer

B

- Network layer
- Datalink layer
- Physical layer

Answer:

In the Open Systems Interconnection (OSI) Model:

- **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 Transport Layer Security (TLS) to provide encryption, authentication, and data integrity for secure communication over a computer network.

Here's a more detailed breakdown of how TLS works in HTTPS:

1. **Encryption:** TLS uses a combination of asymmetric and symmetric encryption to secure data. When a client (like a web browser) connects to a server over HTTPS, an initial handshake occurs where they agree on encryption methods and exchange keys. Asymmetric encryption (public and private keys) is used during this handshake to securely exchange a symmetric key, which is then used to encrypt the data transferred during the session.
2. **Authentication:** During the TLS handshake, the server presents a digital certificate issued by a trusted Certificate Authority (CA). This certificate contains the server's

public key and information about the server's identity. The client verifies the certificate against a list of trusted CAs to ensure it is communicating with the legitimate server, preventing man-in-the-middle attacks.

3. **Data Integrity:** TLS uses message authentication codes (MACs) to ensure that data sent over the connection has not been tampered with. Each message includes a MAC, and the recipient verifies this to ensure the message is authentic and unchanged.

4. Handshake Process:

- **Client Hello:** The client sends a request to the server, including information like the supported TLS versions, encryption algorithms, and a randomly generated number.
- **Server Hello:** The server responds with its own supported TLS version, chosen encryption algorithm, its digital certificate, and another randomly generated number.
- **Key Exchange:** The client and server exchange keys. In the case of asymmetric encryption, the client uses the server's public key to encrypt a randomly generated session key, which only the server can decrypt with its private key.
- **Session Key Generation:** Both the client and server use the agreed-upon session key to create a secure, encrypted communication channel.
- **Secure Communication:** All subsequent data sent between the client and server is encrypted with the session key, ensuring privacy and security.

By using TLS, HTTPS provides a secure communication channel that protects against eavesdropping, tampering, and forgery.

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 public network, like the internet. This secure connection offers several key benefits:

1. **Security:** VPNs protect data by encrypting it, preventing unauthorized access and ensuring that sensitive information remains confidential.
2. **Privacy:** By masking the user's IP address, VPNs enhance privacy and anonymity, making it harder for websites, advertisers, and hackers to track online activities.
3. **Remote Access:** VPNs allow remote users to securely connect to a private network, such as a corporate network, enabling access to resources as if they were on-site.

4. **Bypassing Geo-Restrictions:** VPNs enable users to access content that may be restricted or censored in their geographic location by routing their internet traffic through servers in different regions.
5. **Data Integrity:** VPNs ensure that data sent and received over the network remains unaltered and secure from tampering.

How VPN Works:

- **Client Software:** The user installs VPN client software on their device.
- **Connection Establishment:** The client connects to a VPN server, creating an encrypted tunnel for data transmission.
- **Data Encryption:** Data is encrypted before being sent over the internet and decrypted by the VPN server.
- **Secure Communication:** The process is reversed for data received by the user, ensuring secure communication throughout.

Types of VPNs:

- **Remote Access VPN:** For individual users to securely connect to a private network from a remote location.
- **Site-to-Site VPN:** For connecting entire networks (e.g., branch offices) securely over the internet.
- **Personal VPN:** Used by individuals for privacy, security, and accessing restricted content.

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.

1. Two-Factor Authentication (2FA):

- Requires two forms of verification before granting access. This typically includes something the user knows (password) and something the user has (a mobile device for a verification code).

2. Biometric Authentication:

- Uses unique biological traits such as fingerprints, facial recognition, or iris scans to verify identity.

3. Public Key Infrastructure (PKI):

- Utilizes a pair of keys (public and private) to encrypt and decrypt data. PKI is often used in conjunction with digital certificates to authenticate identities.

4. SSL/TLS Certificates:

- Secure Sockets Layer (SSL) and Transport Layer Security (TLS) certificates authenticate the identity of a website and establish an encrypted connection, ensuring that data sent between the user and the site remains private.

5. OAuth:

- An open standard for access delegation, commonly used as a way to grant websites or applications limited access to user information without exposing passwords.

6. CAPTCHA:

- Completely Automated Public Turing test to tell Computers and Humans Apart. Used to verify that the user is human and not an automated bot.

7. Email Verification:

- Sending a verification link or code to a user's email address to confirm their identity.

8. SMS Verification:

- Sending a one-time password (OTP) or verification code to the user's mobile phone to verify their identity.

9. Blockchain Verification:

- Using blockchain technology to create a secure and tamper-proof record of transactions, ensuring authenticity and integrity.

10. Access Tokens:

- Used in APIs to grant secure access to resources. Tokens are often short-lived and provide a secure way to authenticate users without repeatedly sharing credentials.

11. MAC Address Filtering:

- Restricting network access based on the unique hardware addresses of devices, ensuring only authorized devices can connect.

12. Security Questions:

- Answering pre-set questions to verify identity, commonly used in account recovery processes.

5. After the authentication is successful, **Authorization** can be used to determine what resources the user is 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. Is 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.

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**.

9. Move A and B to corresponding IP assignment.

Answer:

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 Scope:

- **MAC Address:**
 - **Purpose:** A MAC (Media Access Control) address uniquely identifies a network interface card (NIC) or hardware device on a local network.
 - **Scope:** Operates at the Data Link Layer (Layer 2) of the OSI model and is used for communication within the same local network segment or subnet.
- **IP Address:**
 - **Purpose:** An IP (Internet Protocol) address identifies a device on a network and helps in routing data between devices across different networks.
 - **Scope:** Operates at the Network Layer (Layer 3) of the OSI model and is used for communication across different networks, including the internet.
- **Network Address:**
 - **Purpose:** Represents the address of an entire network or subnet, used for routing and managing traffic between different networks.
 - **Scope:** Often used in conjunction with IP addresses, network addresses refer to the whole subnet or network segment and help in identifying and routing data within and between networks.

2. Permanence and Assignment:

- **MAC Address:**
 - **Permanence:** Typically fixed and assigned by the hardware manufacturer; it is hard-coded into the NIC and usually does not change.

- **Assignment:** Static and unique to the hardware device.
- **IP Address:**
 - **Permanence:** Can be either static (permanently assigned) or dynamic (assigned temporarily by a DHCP server).
 - **Assignment:** Can change based on network configuration or the DHCP lease time.
- **Network Address:**
 - **Permanence:** Refers to the network or subnet as a whole and is typically stable unless the network design changes.
 - **Assignment:** Defined by network administrators and depends on the IP addressing scheme used in the network.

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

Answer:

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:**

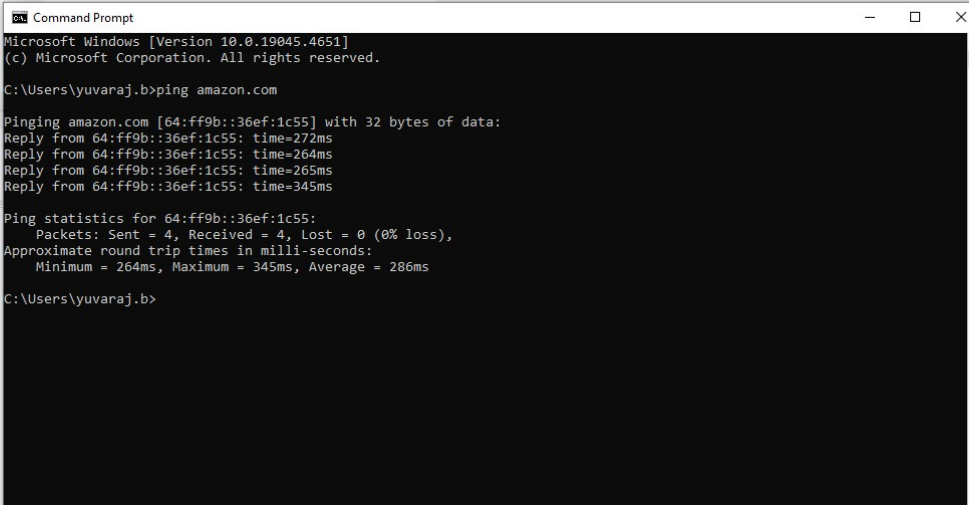
- **B.** MAC Address, Flow control, Frames, switches, ARP

- **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.

Answer:



```
Command Prompt
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 chosen 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

Answer:

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.