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

**Hardware Layer**: This generally refers to the layers involved in the actual transmission of data and physical connections between devices. In the OSI Model, these are:

* **Network Layer** (Layer 3)
* **Data Link Layer** (Layer 2)
* **Physical Layer** (Layer 1)

2. 2) HTTPS uses which protocol for security?

HTTPS (HyperText Transfer Protocol Secure) uses **Transport Layer Security (TLS)** for security. TLS is the successor to the older **Secure Sockets Layer (SSL)** protocol, though the term SSL is still commonly used.

TLS provides encryption for data transmitted over the internet, ensuring confidentiality and integrity between a client (such as a web browser) and a server. It also includes mechanisms for authenticating the server and, optionally, the client, to protect against eavesdropping and tampering.

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

A **Virtual Private Network (VPN)** is a technology that creates a secure and encrypted connection over a less secure network, such as the internet. Here’s a breakdown of its main features and uses:

1. **Encryption**: VPNs encrypt the data transmitted between your device and the VPN server, which helps protect sensitive information from eavesdropping and interception.
2. **Privacy**: By masking your IP address and routing your traffic through a VPN server, VPNs help maintain your privacy online and can prevent websites and online services from tracking your browsing activities.
3. **Access Control**: VPNs can provide access to restricted or geo-blocked content by making it appear as if you are accessing the internet from a different location. This is particularly useful for bypassing geographic restrictions on streaming services or accessing company resources from remote locations.
4. **Secure Remote Access**: VPNs allow employees to securely access a company’s internal network from remote locations, which is especially valuable for remote work and accessing sensitive corporate resources.
5. **Data Integrity**: VPNs help ensure that the data sent and received remains intact and unaltered during transmission, which can protect against certain types of cyber attacks.

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)**:
   * **Description**: This involves an additional layer of security where, after entering a password, users must provide a second form of verification. This could be a code sent to a mobile device, a fingerprint scan, or a hardware token.
   * **Usage**: Commonly used for online banking, email accounts, and other sensitive applications to enhance security.
2. **Password-Based Authentication**:
   * **Description**: Users are required to provide a password or passphrase to access a system or account. While basic, passwords are often combined with other security measures for better protection.
   * **Usage**: Used across most online services, including social media, email, and various accounts.
3. **Biometric Authentication**:
   * **Description**: This method uses unique biological traits such as fingerprints, facial recognition, or iris scans to verify identity.
   * **Usage**: Frequently used in smartphones, some laptops, and secure facilities.
4. **Public Key Infrastructure (PKI)**:
   * **Description**: PKI involves a pair of keys—public and private—used for encrypting and decrypting information. Digital certificates issued by Certificate Authorities (CAs) help authenticate identities and secure communications.
   * **Usage**: Used for secure email communication, website SSL/TLS certificates, and software code signing.
5. **Secure Sockets Layer (SSL) / Transport Layer Security (TLS)**:
   * **Description**: SSL/TLS protocols encrypt data transmitted between a web server and a client, ensuring secure communications over the internet.
   * **Usage**: Used to secure web browsing (HTTPS), online transactions, and data exchange between servers and clients.
6. **One-Time Passwords (OTPs)**:
   * **Description**: OTPs are temporary passwords that are valid for a single session or transaction. They provide a time-sensitive layer of security.
   * **Usage**: Often used in online banking, transaction verification, and some authentication systems.
7. **Secure Token-Based Authentication**:
   * **Description**: This involves using a physical or digital token to authenticate users. Tokens generate unique codes or use cryptographic methods to verify identity.
   * **Usage**: Used in various secure access systems, including some VPNs and multi-factor authentication solutions.
8. **Digital Certificates**:
   * **Description**: Digital certificates use encryption to verify the identity of entities, such as websites or individuals, and ensure secure communications.
   * **Usage**: Used in SSL/TLS certificates for websites, email encryption, and software distribution.
9. After the authentication is successful, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Authorization/Communication) can be used to determine what resources is the user allowed to access and the operations that can be performed

**Authorization** involves specifying and enforcing permissions and access rights for authenticated users. It ensures that once a user is verified, their access to resources and operations is controlled based on predefined policies and permissions.

1. ) 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. Consider above Packet firewall rule. Now Network IP: 192.168.21.0, Trying to connect to your machine and want to send data..
2. **Network IP**: 192.168.21.0
3. **Action**: Allow/Reject/Drop

The action taken by the firewall depends on the defined rules. For example, if the firewall rule table includes a rule like:

* **Allow**: 192.168.21.0/24, **Port**: Any, **Protocol**: Any

Then, traffic from the IP address 192.168.21.0 would be allowed based on this rule. If the rule was:

* **Deny**: 192.168.21.0/24, **Port**: Any, **Protocol**: Any

Then, traffic from the IP address 192.168.21.0 would be rejected or dropped based on this rule.

7Application Layer Firewall, software Firewall and Hardware Firewall allows only destined and avoids malicious data. If these firewalls are

If these firewalls are not installed, your application may receive \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ data (malicious / all Secured ) data.

 **Application Layer Firewall**: Monitors and filters traffic based on application-level data. Without it, malicious data intended to exploit vulnerabilities in applications can pass through unchecked.

 **Software Firewall**: Provides a layer of protection on individual machines, controlling traffic based on rules and policies. Without it, malicious data from external sources can directly reach your applications.

 **Hardware Firewall**: Protects the network perimeter and manages incoming and outgoing traffic. Without it, malicious data from external networks can enter your internal network and reach your applications

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 **Improving Security**: By isolating different parts of the network, subnetting can contain potential security breaches within a specific subnet rather than allowing them to affect the entire network.

 **Optimizing Performance**: Reducing the size of broadcast domains can decrease network congestion and improve performance.

 **Simplifying Management**: Managing smaller subnets can be more straightforward, and routing between them can be handled more efficiently with appropriate routing tables.

9 S.NO Static IP Address Dynamic IP address It is provided by ISP(Internet Service Provider). While it is provided by DHCP (Dynamic Host Configuration Protocol). A) This IP address does not change at IP any time, which means if a ip address is provided then it can’t be changed or modified and is easily traceable. B) These addresses changes at any time and not easily traced.

**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.**
  + **Reason**: Static IP addresses are manually assigned and remain constant over time. They are useful for situations where a consistent IP address is needed, such as for servers or network devices that require a fixed address for access.

**Dynamic IP Address**

* **B) These addresses change at any time and are not easily traced.**
  + **Reason**: Dynamic IP addresses are assigned by a DHCP server and can change periodically as devices connect and disconnect from the network. This makes them less consistent and harder to trace compared to static IP addresses.

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

**1. Purpose and Layer of Operation**

* **MAC Address**:
  + **Purpose**: MAC (Media Access Control) addresses are used for identifying devices at the Data Link Layer (Layer 2) of the OSI model. They are unique to each network interface card (NIC) and are used for communication within the same local network segment.
  + **Layer**: Data Link Layer (Layer 2).
* **IP Address**:
  + **Purpose**: IP addresses are used for identifying devices at the Network Layer (Layer 3) of the OSI model. They provide logical addressing, which allows devices to be identified and communicate over different networks and the internet.
  + **Layer**: Network Layer (Layer 3).
* **Network Address**:
  + **Purpose**: Network addresses are used to define and identify a network segment or an individual device on a network. In the context of IP addressing, a network address specifies the network portion of an IP address.
  + **Layer**: Can refer to both Layer 2 (in the context of MAC addresses) and Layer 3 (in the context of IP addresses).

**2. Address Format and Assignment**

* **MAC Address**:
  + **Format**: Typically a 48-bit address, expressed in hexadecimal format (e.g., 00:1A:2B:3C:4D:5E).
  + **Assignment**: Assigned by the manufacturer of the network interface card (NIC) and is hardcoded into the hardware.
* **IP Address**:
  + **Format**: Can be either IPv4 (32-bit address, e.g., 192.168.1.1) or IPv6 (128-bit address, e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
  + **Assignment**: Assigned dynamically by DHCP or statically configured by network administrators.
* **Network Address**:
  + **Format**: The format depends on the IP addressing scheme used. For example, in IPv4, it could be a part of an IP address and subnet mask (e.g., 192.168.1.0/24 specifies the network portion of an address).
  + **Assignment**: Defined by network design and subnetting practices, not assigned to devices but rather used to define the scope of IP address ranges.

11. Match numbers with letters according to 7 layers roles: 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 S.NO Static IP Address Dynamic IP address It is provided by ISP(Internet Service Provider). While it is provided by DHCP (Dynamic Host Configuration Protocol). 1. Application Layer: 2. Presentation Layer: 3. Session Layer: 4. Transport Layer 5. Network Layer 6. Data Link Layer 7. Physical Layer 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

So the complete matching is:

1. Application Layer: **G**
2. Presentation Layer: **C**
3. Session Layer: **D**
4. Transport Layer: **E**
5. Network Layer: **F**
6. Data Link Layer: **B**
7. Physical Layer: **A**

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

To find the IP address associated with a domain like amazon.com, you can use the ping command from a command line interface (such as Command Prompt on Windows, Terminal on macOS or Linux). Here’s how you can do it:

1. Open your command line interface.
2. Type the following command and press Enter:

Copy code

ping amazon.com

1. You will see output similar to:

python

Copy code

Pinging amazon.com [<IP address>] with 32 bytes of data:

Reply from <IP address>: bytes=32 time=xx ms TTL=xx

The <IP address> will be the IP address associated with amazon.com at the time of the query.

**Note:** The IP address can vary due to the use of load balancing and distributed servers. For instance, when I last checked, the IP address for amazon.com might be 205.251.242.103, but this could change over time or vary based on your geographic location and DNS server.

If you are unable to use the ping command or need a specific IP address at a particular moment, you can also use online tools or websites like whatismyip.com or dnschecker.org to perform a DNS lookup.

13 Consider below network address and subnetID. From the routing table, which Interface should be choosen for Network ID 172.16.0.0: (A/B) Routing Table: 1.  Network Address: 172.16.0.0 2.  Subnet ID: 172.16.0.0/16 Network ID Subnet Mask Interface 200.1.2.0 255.255.255.192 A 172.16.0.0 255.255.255.193 B

1. **Identify the relevant entry in the routing table**:
   * The routing table provides two entries:
     1. **Network Address: 200.1.2.0** with a subnet mask of 255.255.255.192 (Interface A)
     2. **Network Address: 172.16.0.0** with a subnet mask of 255.255.255.193 (Interface B)
2. **Match the Network ID with the Subnet ID**:
   * **Network ID**: 172.16.0.0
   * **Subnet ID**: 172.16.0.0/16

The subnet ID /16 indicates that the subnet mask is 255.255.0.0 for this network. However, in the routing table, the subnet mask for the entry 172.16.0.0 is 255.255.255.193.

1. **Compare with Routing Table Entries**:
   * The subnet mask 255.255.255.193 is unusual, as it does not align with standard subnet masks. Typically, subnet masks are in the form of 255.0.0.0, 255.255.0.0, 255.255.255.0, etc. This might be a typo or an unconventional subnet mask.
   * **Interface A** (Network 200.1.2.0 with mask 255.255.255.192): This does not match 172.16.0.0 and thus is not relevant for this network ID.
   * **Interface B** (Network 172.16.0.0 with mask 255.255.255.193): This entry matches the network ID 172.16.0.0, and it is specifically listed in the routing table.

Based on the information provided:

* **Interface B** should be chosen for the network ID 172.16.0.0, as it directly matches the network ID in the routing table.

**So, the correct interface is B**