Question 1:

*1. Define 172.18.10. /22 in terms of its type of IP and Subnet Mask.**

- **IP Type:**
  172.18.10.* is a **Class B private IP address** as it falls within the range of 172.16.0.0 – 172.31.255.255. Private IP addresses are used within internal networks and are not routable on the internet.
- **Subnet Mask:**
  A /22 subnet mask corresponds to **255.255.252.0**. This means that the first 22 bits are used for network identification and the remaining 10 bits are used for host identification.

---

2. Calculate the subnet mask of /22 metric.
The subnet mask for /22 is **255.255.252.0**. In binary, this looks like:

```
11111111.11111111.11111100.00000000
```

Which means the first 22 bits are set to 1, and the remaining 10 bits are set to 0.

---

3. From the information provided, fill in the table:

We need to calculate the **Network Address**, **Valid Host Address Range**, **Broadcast Address**, and the **Number of Idle IP addresses** for each department based on their user requirements.

Here is how it is broken down:

- **VOIP LAN (450 Users):**
  To accommodate 450 users, we need at least 512 addresses. This requires a subnet mask of /23 (512 addresses).
  - Network Address: 172.18.10.0
  - Valid Host Range: 172.18.10.1 to 172.18.11.254
  - Broadcast Address: 172.18.11.255
  - Idle IPs: 512 - 450 = 62 idle IPs.
- **Sales LAN (150 Users):**

To accommodate 150 users, we need at least 256 addresses. This requires a subnet mask of /24 (256 addresses).

    - Network Address: 172.18.12.0
    - Valid Host Range: 172.18.12.1 to 172.18.12.254
    - Broadcast Address: 172.18.12.255
    - Idle IPs: 256 - 150 = 106 idle IPs.

- **Finance LAN (125 Users):**
  To accommodate 125 users, we need at least 128 addresses. This requires a subnet mask of /25 (128 addresses).
    - Network Address: 172.18.13.0
    - Valid Host Range: 172.18.13.1 to 172.18.13.126
    - Broadcast Address: 172.18.13.127
    - Idle IPs: 128 - 125 = 3 idle IPs.
- **Staff LAN (50 Users):**
  To accommodate 50 users, we need at least 64 addresses. This requires a subnet mask of /26 (64 addresses).
    - Network Address: 172.18.13.128
    - Valid Host Range: 172.18.13.129 to 172.18.13.190
    - Broadcast Address: 172.18.13.191
    - Idle IPs: 64 - 50 = 14 idle IPs.

---

*4. The IP address 172.18.10. /22 is considered a Private IP address.**

a) Differentiate between Private and Public IP addresses:

- **Private IP addresses** are reserved for use within a private network and cannot be routed on the public internet. They include ranges such as 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8.
- **Public IP addresses** are routable on the internet, meaning they are used for devices that are accessible on the public internet.

b) The choice of a valid Private IP address from Class A, B, or C depends on the number of authorized users. Please provide the list:

- **Class A Private IP range:** 10.0.0.0 – 10.255.255.255 (supports 16,777,214 hosts)

- **Class B Private IP range:** 172.16.0.0 – 172.31.255.255 (supports 1,048,576 hosts)
- **Class C Private IP range:** 192.168.0.0 – 192.168.255.255 (supports 65,536 hosts)

Question 2:

1. Provide two protocols associated with layer 2 (Data Link Layer).

- **Ethernet (IEEE 802.3)**: Ethernet is one of the most widely used protocols at the Data Link Layer, handling communication between devices on the same network segment.
- **PPP (Point-to-Point Protocol)**: PPP is used for direct communication between two network devices, often over serial links such as between routers or modems.

---

2. Explain the purpose and on which layer of the OSI model the following devices operate:

a) Router

- **Layer**: Routers operate on **Layer 3 (Network Layer)** of the OSI model.
- **Purpose**: Routers direct data packets between different networks by analyzing the destination IP address and forwarding them along the most efficient route. They are responsible for inter-network communication and traffic control.

b) Bridge

- **Layer**: Bridges operate on **Layer 2 (Data Link Layer)**.
- **Purpose**: A bridge divides a large network into smaller segments, reducing network traffic. It filters traffic between segments by looking at MAC addresses and deciding whether to forward or block packets.

c) Switch

- **Layer**: Switches operate on **Layer 2 (Data Link Layer)**.
- **Purpose**: A switch connects devices within a single network and forwards data based on MAC addresses, creating a direct connection between sending and receiving devices, improving efficiency compared to hubs.

3. Whenever we issue the `traceroute` command, routers provide the best route based on their routing table:

a) Explain the role of a Router with respect to the `traceroute` command.

- A router plays a key role in providing the path or route taken by a packet to reach its destination when we issue a `traceroute` command. The router sends ICMP packets to trace the hops between the source and destination and returns the response time for each hop.

b) Describe the following command `traceroute 8.8.8.8`.

- This command is used to trace the path from your computer to the Google Public DNS server (IP: 8.8.8.8). It shows the route taken and the round-trip time for each hop along the path.

4. Routers work and store routing tables. Explain why routing tables are important for an efficient packet flow.

- Routing tables store the most efficient paths to reach different networks. They help routers make quick decisions about where to forward packets, ensuring that data is sent along the best route, reducing delays, and improving the overall efficiency of the network.

5. The diagram shows a set of hops from Source router A to Destination router H. The figures between routers refer to its metric:

a) The best route from A to H.

- The best (shortest) route is A -> C -> F -> H, with a metric of 3 + 3 + 2 = 8.

b) The longest route.

- The longest route is A -> D -> E -> G -> H, with a metric of 6 + 5 + 7 + 5 = 23.

Let's go through **Question 3** step by step:

Question 3:

1. What is the full form of SD-WAN?

- **SD-WAN** stands for **Software-Defined Wide Area Network**.

2. Define SD-WAN.

- **SD-WAN** is a virtual WAN architecture that allows enterprises to centrally control and manage their wide-area network (WAN) using software-based technologies. It improves the efficiency and performance of a network by intelligently directing traffic across the most optimal paths, whether through MPLS, broadband, or LTE.

3. Provide two key components to an SD-WAN Solution.

- **Centralized Management:** This component allows network administrators to monitor and manage the WAN through a single interface, improving visibility and control across all branches.
- **Dynamic Path Selection:** SD-WAN can automatically choose the best available path for data packets, improving performance and efficiency. It can reroute traffic in real time based on network conditions such as congestion or link failure.

4. Andrew Lerner mentioned VPNs in 2020 when COVID forced employees to work from home. Explain how VPN technology works with the help of a clearly labeled diagram.

- **VPN (Virtual Private Network)** allows users to securely connect to a remote network over the internet by creating an encrypted "tunnel" for their data. This protects the data from being intercepted by unauthorized users. Employees working from home use VPNs to connect securely to their company's internal network.

Note: The diagram should illustrate a client connecting to the company's network via a VPN server, with encryption shown between the client and the server.

---

5. Describe the VPN technology.

- **VPN technology** creates a secure and encrypted connection between a user's device and a remote server. The encryption ensures that all data transmitted over the VPN cannot be read by third parties, protecting sensitive information. VPNs are often used by employees to securely access company resources remotely.

---

6. With the help of a clearly labeled diagram, describe how a VPN works.

- The diagram should show:
  - **Client (user's device)** -> **VPN Tunnel (encrypted data path)** -> **VPN Server** -> **Company Network**.
  - The client connects to the VPN server, which securely forwards requests to the company network, and any data sent between the client and server is encrypted.

---

7. A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways, and other network parameters to client devices.

a) IP assignment may be done via a DHCP server. What is a DHCP Server?

- **DHCP (Dynamic Host Configuration Protocol) Server** is responsible for automatically assigning IP addresses and other network settings to devices on the network. This eliminates the need for manual configuration of IP settings on each device.

b) Describe the four steps of the DHCP server with the help of a diagram.

The four steps are:

1. **DHCP Discover:** The client broadcasts a request to find available DHCP servers.
2. **DHCP Offer:** The DHCP server responds with an offer, providing an IP address and configuration details.
3. **DHCP Request:** The client accepts the offer by sending a request to the server.
4. **DHCP Acknowledgement:** The server acknowledges the request and finalizes the IP assignment.

Diagram: The diagram should show the interactions between the client and the DHCP server during each of these steps.

Let's go through **Question 4** step by step:

Question 4:

1. Computers need to be protected and made more secure. Describe the following computer security terms:

a) Anti-virus software:

- **Anti-virus software** is a program designed to detect, prevent, and remove malicious software, such as viruses, worms, and Trojans, from a computer. It scans the system, files, and incoming data for known threats.

b) Anti-spyware:

- **Anti-spyware** software is a tool that prevents, detects, and removes spyware, which is a type of malware that secretly gathers information about a person or organization without their knowledge, often for malicious purposes.

c) Access Control List (ACL):

- An **Access Control List (ACL)** is a list of permissions attached to an object (e.g., files, network devices). It specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects (read, write, execute).

d) Pop-up blocker:

- A **Pop-up blocker** is a software feature that prevents unwanted pop-up windows (usually advertisements) from appearing while browsing the internet. It enhances security by blocking malicious pop-ups that may contain harmful scripts.

---

2. Explain the purpose of each of the following commands:

a) FTP (File Transfer Protocol):

- **FTP** is a protocol used to transfer files between computers on a network. It allows users to upload, download, and manage files on a remote server.

b) PING:

- **PING** is a command used to test the connectivity between two network devices by sending ICMP echo request messages. It helps in diagnosing network issues and measuring the round-trip time for packets.

c) Traceroute:

- **Traceroute** is a command that shows the path taken by packets from the source to the destination through various routers. It provides detailed information about each hop and helps in troubleshooting network connectivity issues.

d) Netstat:

- **Netstat** is a command-line tool that displays active network connections, routing tables, and network protocol statistics. It is used to monitor incoming and outgoing network traffic and to troubleshoot network problems.

---

3. Identify the following types of digital communication media, typical transmission speeds, and the medium used to provide a communications link:

The images in the question likely represent different types of network cables. Based on the general descriptions:

a) Rank the media above in terms of its fastest first to slowest:

- Fiber-optic cable (likely represented by one of the images) is the fastest.
- Coaxial cable is typically faster than twisted pair cables.
- Twisted pair cable (Cat5/Cat6) comes after coaxial in terms of speed.
- USB cable (if one of the images represents USB) is typically slower than the other types.

So, the ranking from fastest to slowest could be:
Fiber-optic > Coaxial > Twisted Pair (Cat5/Cat6) > USB

b) Explain which media would be best suited for use in high voltage and electromagnetic environments. Justify your answer.

- Fiber-optic cables are the best-suited medium for high-voltage and electromagnetic environments. This is because they use light to transmit data rather than electrical signals, making them immune to electromagnetic interference (EMI) and capable of operating in environments with high voltage without being affected by the surrounding electrical noise.