1. In Packet Tracer Simulation Mode, the HTTP request is generated but the web page does not immediately load until Capture/Forward is used. Explain, at the protocol and simulation level, why HTTP communication does not complete instantly in Simulation mode.

In Simulation mode, Packet Tracer pauses time to allow for a step-by-step inspection of **PDUs (Protocol Data Units)**. Unlike Realtime mode, where traffic is processed instantly, Simulation mode requires the user to click **Capture/Forward** to trigger the physical movement of each frame across the media.

2. During the first HTTP event inspection, Layer 4 shows a destination port. Identify which service port the Web Server is listening on, and justify how you concluded this using OSI Layer 4 evidence from the simulation.

The Web Server listens on **Port 80**. This is concluded from Layer 4 of the Outbound PDU details, where the **Dest Port** is explicitly listed as 80, which is the standard well-known port for the HTTP protocol.

3. In the PDU details window, Layer 2 information shows both SRC MAC and DEST MAC fields. Explain why MAC addressing is required even when the destination is identified by an IP address at Layer 3.

IP addresses (Layer 3) are used for logical end-to-end routing, but **MAC addresses (Layer 2)** are required for physical delivery on the local network segment. Without a destination MAC, the network interface card (NIC) cannot determine which specific hardware should "pick up" the frame from the wire.

4. When DNS events are enabled in the simulation filters, DNS traffic appears before HTTP communication fully proceeds. Explain why DNS must occur before HTTP and what failure would occur if DNS resolution did not return an address.

DNS must occur first because HTTP requires a destination IP address to build its packets. If you enter a URL like `www.osi.local`, the PC must first resolve that name to an IP. If DNS fails, the HTTP communication cannot proceed because the **Destination IP field** at Layer 3 would remain empty.

5. In the "View Network Device MAC Addresses" lab, the switch configuration includes the command: no ip domain-lookup Explain why this command is useful in a lab environment and how it prevents specific troubleshooting delays.

This command prevents the switch from trying to resolve a mistyped command as a domain name. In a lab, it prevents long **troubleshooting delays** (often 30+ seconds) where the switch hangs while waiting for a DNS response that will never come.

6.

A MAC address is divided into OUI and serial number components.
Explain how a network administrator can use the OUI portion to identify the manufacturer and why this can be important in network auditing or incident response.

The **OUI (Organizationally Unique Identifier)** consists of the first 3 bytes of a MAC address. Administrators use it to identify the hardware vendor (e.g., Cisco, Intel). In incident response, this helps identify unauthorized devices or rogue hardware plugged into the network.

7.

In the output of show interfaces vlan 1, the MAC address appears twice in the format: address is xxxx.xxxx.xxxx (bia xxxx.xxxx.xxxx)
Explain what BIA means and under what condition the first address might differ from the BIA value.

BIA stands for **Burned-In Address**, the permanent hardware address assigned at the factory. The first address might differ if an administrator has manually configured a **locally administered MAC address** (spoofing or overriding the hardware address) for specific networking requirements.

8.

In the "Switch MAC Address Table" lab, after clearing the MAC table using clear mac address-table dynamic,
some MAC addresses may still remain mapped to the CPU.
Explain why CPU-mapped MAC addresses remain even after clearing the dynamic

table and what type of traffic these addresses usually represent.

These addresses remain because they are **Static**, not Dynamic. They represent the switch's own virtual interfaces and management ports. They handle control plane traffic like **CDP, STP, and VTP**, which the switch CPU must process directly to maintain the network.

9.

In the multi-switch topology, if a switch receives a frame whose destination MAC is unknown, it floods the frame out of all ports except the incoming one.
Explain why flooding is necessary, and analyze the potential security risks this behavior introduces in real enterprise networks.

Flooding is necessary to ensure the frame reaches the intended destination if its location isn't yet known. However, this introduces a **security risk** called "Eavesdropping" or "MAC Flooding Attacks," where a malicious actor can use a packet sniffer to capture sensitive data intended for another device.

10.

After PC-B pings PC-A, S1, and S2, both the ARP cache (arp -a) and the switch MAC address table update.
Explain the relationship between ARP cache entries and switch MAC table entries, and why both are needed for successful end-to-end delivery.

- **ARP Cache (PC)**: Maps an **IP address to a MAC address** so the PC knows what destination MAC to put in the frame.
- **MAC Table (Switch)**: Maps a **MAC address to a physical Port** so the switch knows where to send that frame.

  Both are needed: the PC determines *who* gets the data (MAC), and the switch determines *where* they are plugged in (Port).