QUESTION ONE: Communication Hardware Setup

a) Configuring a Serial Port (10 marks)

Configuring a **serial port** (often designated as a **COM port**) involves ensuring the hardware is recognized and resources are properly allocated in both the system firmware and the operating system.[1]

1. System BIOS/UEFI Configuration

The **BIOS/UEFI** is the firmware that initializes and tests system hardware.[2]

- **Access Firmware: Restart** the workstation and press the designated key (e.g., F2, F10, Del) during startup to enter the BIOS/UEFI Setup Utility.
- **Locate Device Settings:** Navigate to a section dealing with integrated peripherals, I/O ports, or onboard devices.
- **Enable the Port:** Ensure the onboard serial port (typically labeled **Serial Port 1** or **COM1**) is set to **Enabled** or **Auto**. If using a PCI/PCIe serial card, ensure the corresponding slot is enabled.
- **Set Legacy Resources (if applicable):** For very old or specialized legacy hardware, you might need to manually set the **I/O Address** (typically $03F8$h) and the **IRQ** line (typically IRQ 4) to prevent resource conflicts.
- **Save and Exit: Save** the changes and reboot the system.

2. Operating System (OS) Configuration

The OS must recognize and correctly configure the port's communication parameters.

- **Verify Recognition:** Access the **Device Manager** (e.g., in Windows, right-click Start [3]$\rightarrow$ Device Manager) and look under the **Ports (COM & LPT)** section.[4] The serial port should be listed (e.g., Communications Port (COM1)).
- **Configure Port Settings:** Right-click the COM port and select **Properties**.
  - Navigate to the **Port Settings** tab.
  - Adjust the parameters—**Baud Rate**, **Data Bits**, **Parity**, and **Stop Bits**—to **match the specific requirements of the connected serial device** (e.g., 9600, 8, None, 1).[5]
- **Troubleshoot:** If the port shows an error (yellow exclamation mark), try updating the driver or checking for resource conflicts in the port's properties.

---

b) Installing and Configuring a Modem (5 marks)

The procedure depends on the modem type, either **internal** (card) or **external** (USB/Serial box).

1. Installation and Drivers

- Internal Modem:
    1. **Power Down and Insert:** Power off the PC, unplug it, and insert the modem card firmly into an available **PCI** or **PCIe** slot.
    2. **Power On:** Reboot the system. The OS should detect the new hardware.
- External Modem:

    1. **Physical Connection:** Connect the modem to the PC via **USB** or **Serial** cable.
    2. **Phone Line:** Connect the modem's **Line** port to the wall telephone jack using an **RJ-11** cable.[6]
    3. **Power On:** Plug in and power on the external modem.
- **Driver Installation:** Allow the OS to automatically install the driver via Plug and Play. If unsuccessful, manually install the driver using the manufacturer's media or downloaded file via the **Device Manager**.

2. Configuration

- **OS Recognition:** In **Device Manager** or the **Control Panel $\rightarrow$ Phone and Modem** utility, ensure the modem is listed and recognized.
- **Dialing Rules:** Configure **dialing rules** including the **country/region**, **area code**, and any necessary prefixes (e.g., '9' to get an outside line).
- **Create Dial-up Connection:** Use the OS's networking utility (e.g., **Network and Sharing Center** in Windows) to create a new dial-up connection.[7]

    Enter the ISP's **phone number**.

    Enter the provided **Username** and **Password**.

- **Test:** Initiate the connection to verify the modem can successfully dial out and authenticate with the ISP.

c) Configuring a NIC to a Wired LAN (5 marks)

Connecting a **Network Interface Card (NIC)** requires ensuring the hardware is set up for the correct speed and has the appropriate network addressing.

1. Driver and Firmware

- **Driver Check:** Verify in **Device Manager** that the **NIC driver** is correctly installed. Update to the latest version from the manufacturer if performance issues arise.
- **Firmware:** Ensure any NIC **firmware** is current, especially for high-speed or enterprise-grade adapters.

2. Duplex/Speed Settings

- **Access Advanced Settings:** In the NIC's properties (**Device Manager** [8]**$\rightarrow$ NIC** [9]**$\rightarrow$ Properties** [10]**$\rightarrow$ Advanced Tab**).[11]
- **Set Link Speed:** Locate the **Speed & Duplex** setting.
  - The best practice is to set this to **Auto Negotiation** (or **Auto**) so the NIC and the switch can agree on the fastest, most reliable connection (e.g., 1 Gbps Full Duplex).
  - If troubleshooting, you may manually set the speed (e.g., 100 Mbps Full Duplex) to match a fixed setting on the switch.

3. IP Addressing

- **Access TCP/IPv4 Properties:** In the OS's **Network Adapter Settings**, go to the properties of **Internet Protocol Version 4 (TCP/IPv4)**.
- **Dynamic (DHCP):** Select **Obtain an IP address automatically** (recommended for workstations). The network's DHCP server will provide the **IP Address**, **Subnet Mask**, **Default Gateway**, and **DNS Servers**.[12]
- **Static:** If required, select **Use the following IP address** and manually enter a valid, unused IP address, the correct Subnet Mask, the Default Gateway (router's IP), and the DNS server addresses.

QUESTION TWO: Wired and Wireless Network Connectivity

a) Connecting to a Wired Ethernet Network (5 marks)

Connecting a computer to a wired Ethernet network is a fundamental process involving physical connection and software verification.

- **Physical Connection:** Plug one end of a **Cat 5e/6 Ethernet cable** into the workstation's **RJ-45 port** and the other end into an available port on the **network switch** or a corresponding wall jack.
- **Verify Link:** Check the **Link/Activity LED lights** on both the NIC and the switch port. A solid light indicates a good physical connection.
- **Adapter Verification:** Confirm the Ethernet adapter is **Enabled** in the operating system's **Network Adapter Settings**.
- **IP Configuration:** Ensure the adapter's TCP/IPv4 properties are set to **Obtain an IP address automatically (DHCP)**, allowing the router/switch to assign a proper network address.
- **Test Connectivity:** Open the Command Prompt/Terminal and use **ping** to confirm communication, first with the **Default Gateway** (router) and then with an external resource like a public DNS server (e.g., ping 8.8.8.8).[13]

b) Connecting a Device to a Secure Wireless Network (5 marks)

Connecting to a secure wireless network involves discovery, authentication, and IP acquisition.

- **Enable Adapter:** Ensure the device's **Wireless Network Adapter (WLAN)** is turned on (often a physical switch or a function key combination on laptops).
- **Scan and Select SSID:** Use the OS's **Wi-Fi utility** (icon in the system tray) to scan for available networks. Select the correct **Service Set Identifier (SSID)** for the secure office network.
- **Authentication:** The system will prompt for the **security key/passphrase**.
    - The network will typically use a protocol like **WPA2-PSK** or **WPA3-PSK**.
    - Carefully enter the **Wi-Fi Password**, noting that it is case-sensitive.
- **Connect and Acquire IP:** Click **Connect**. If the passphrase is correct, the device will authenticate with the Wireless Access Point and automatically receive an **IP address** from the network's DHCP server.
- **Verify:** Confirm the connection status is **Connected** and that a valid, non-APIPA IP address has been assigned.

  Question 2C

1. No Physical Connection (Wired or Wireless)

This problem occurs when the device fails to establish a link layer connection. For **wired connections**, this is indicated by a **lack of Link/Activity LED lights** on both the Network Interface Card (NIC) and the switch port. For **wireless connections**, the device may not see any available networks or the adapter itself might be disabled.

Troubleshooting Steps:

- **Wired:** The first step is to **check the cable**. Ensure the Ethernet cable is **securely plugged in** at both ends. If the lights remain off, **replace the cable** with a known-good one, or try a **different port** on the network switch.
- **Wireless:** Check the device's settings to ensure the **WLAN adapter is enabled** (some laptops have a physical switch or function key combination that controls this). If the issue persists, **reboot the Wireless Access Point (WAP)** or router.

---

2. DHCP Failure (Limited Connectivity)

This is a common logical failure where the device successfully connects to the network media but fails to obtain a valid IP address from the network's **Dynamic Host Configuration Protocol (DHCP)** server. In Windows, this often results in a **Limited Connectivity** message and the device automatically assigning itself an **APIPA (Automatic Private IP Addressing)** address, typically in the $169.254.x.x$ range.

Troubleshooting Steps:

- **Renew IP Address:** Open the Command Prompt or Terminal and execute the commands **ipconfig /release** followed by **ipconfig /renew** (Windows) or the equivalent commands on other operating systems. This forces the device to try and request a new IP address from the DHCP server.
- **Check DHCP Server:** Verify that the **DHCP service** is active and running correctly on the router or server and that it has an available pool of addresses.
- **Restart Devices:** Power cycle the **router** and the **computer** to resolve temporary glitches in the DHCP process.

3. Authentication Failure (Wireless)

This problem occurs specifically with **secure wireless networks**. The device can see the **Service Set Identifier (SSID)** but cannot join the network because it fails to successfully authenticate. This usually results in the device repeatedly prompting the user to enter the network password.

Troubleshooting Steps:

- **Verify Passphrase:** The most common cause is a typo. **Carefully re-enter the Wi-Fi password/passphrase**, paying close attention to **case sensitivity** (uppercase vs. lowercase letters).
- **Check Security Protocol:** Ensure the device's settings are configured for the correct **security protocol** used by the WAP (e.g., WPA2-PSK or WPA3).
- **MAC Filtering:** If the first two steps fail, check the **Wireless Access Point (WAP) settings** to confirm that a security feature like **MAC address filtering** is not enabled and mistakenly blocking the device's MAC address.