module 2 : Installation and Maintenance of Hardware and Its

Section 1: Multiple Choice

1. Which of the following precautions should be taken before working on computer hardware?

-> Wear an anti-static wrist strap to prevent damage from electrostatic discharge.

2. What is the purpose of thermal paste during CPU installation?

-> To improve thermal conductivity between the CPU and the heat sink.

3. Which tool is used to measure the output voltage of a power supply unit (PSU)?

-> Multimeter

4. Which component is responsible for storing BIOS settings, such as date and time, even when the computer is powered off?

-> CMOS battery

Section 2: True or False

5. When installing a new hard drive, it is essential to format it before use.

-> True

6. A POST (Power-On Self-Test) error indicates a problem with the CPU.

-> True

7. It is safe to remove a USB flash drive from a computer without ejecting it first.

-> False

Section 3: Short Answer

8. Explain the difference between a hub and a switch in a computer network.

-> Disconnect and shut down the computer.

-> Take off the side panel of the case.

-> Remove the old graphics card (if applicable) by unscrewing it and releasing the PCIe latch.

-> Insert the new graphics card into the PCIe x16 slot.

-> Secure the card with a screw/attach power cables if necessary.

-> Put the side panel on the case and reconnect the power.

-> Connect the monitor to the new card.

-> Power on the PC and install drivers from the manufacturers website.

9. Describe the process of troubleshooting network connectivity issues.

1 Check the physical connections (cables, router, and modem).

2 Restart all devices (computer, router, and modem).

3 Check your network settings (IP address, Wifi status).

4 Run network diagnostics on the computer.

5 Ping sites or local IPs to see if they connect.

6 Check for driver/firmware updates.

7 Disable firewall, or virus protection for testing.

8 Reset network settings completely if not.

9 Contact your ISP if it continues.

Section 4: Practical Application

10. Demonstrate how to configure a wireless router's security settings to enhance network security.

1. Login into the Router's Admin Panel

Connect your device to the router via Wi-Fi or an Ethernet cable.

Open a web browser and type the router IP address into the URL bar (it will be something like 192.168.0.1 or 192.168.1.1).

Log into the router using the default admin username and password on the router sticker or your credentials.

2. Change the Default Admin Credentials

Find the Administration or System area.

Change the admin username and admin password to something strong and unique!

3. Enable WPA3 or WPA2 Encryption

Find the Wireless Settings or Security area.

Change the security mode to WPA3 (if applicable) or WPA2-PSK [AES].

Avoid WEP or WPA, as they are insecure and out-of-date.

Come up with a strong Wi-Fi password (minimum of 12 characters using letters, numbers, and symbols).

4. Change the SSID (Network Name)

Avoid using something like "TP-Link1234".

Create a custom SSID that does not reveal any private information.

5. Disable WPS (Wi-Fi Protected Setup)

WPS is convenient but allows brute-force attacks on your Wi-Fi key.

Disable WPS under Wi-Fi settings or Advanced settings.

6. Upgrade Firmware

Check for firmware updates under Administration or Maintenance.

Running the latest version will help to resolve security-firmness.

7. Enable Network Firewall

Ensure that the router's firewall is enabled to block unauthorized access.

8. Turn Off Remote Management

Remove access to Remote Management, Remote Web Access or Remote Administration if you have no need for it.

This will help mitigate the risk of hacking attempts from external parties.

9. Limit DHCP or Assign static IPs (optional)

Limit the number of devices that are able to connect automatically.

By assigning static IP addresses to your known devices, you are kept much more in control.

10. Enable MAC Address Filtering (optional)

You may only allow specified devices to connect, by adding those device MAC addresses.

Section 5: Essay

11. Discuss the importance of network documentation and provide examples of information that should be documented.

Network documentation is important for managing, troubleshooting and securing a network. It allows IT staff to quickly troubleshoot issues that arise, plan for upgrades and expansions, demonstrate compliance with regulations, refocus on business priorities in the event of a disaster, and train the new staff.

Examples of documentation includes:

Network topology diagrams

IP addressing and subnets

Device configuration and credentials

Hardware and software inventory

Firewall rules and security settings

Change logs and updates

ISP and vendor contact details