A+ - Peripherals And Power Supply
Assignment module 3 : Understanding and Maintenance of Networks
Section 1: Multiple Choice

1. What is the primary function of a router in a computer network?
a) Assigning IP addresses to devices
b) Providing wireless connectivity to devices
c) Forwarding data packets between networks
d) Managing user authentication and access control

2. What is the purpose of DNS (Domain Name System) in a computer network?
a) Encrypting data transmissions for security
b) Assigning IP addresses to devices dynamically
c) Converting domain names to IP addresses Routing data
d) packets between network segments

3. What type of network topology uses a centralized hub or switch to connect all devices?
a) Star
b) Bus
c) Ring
d) Mesh

4. Which network protocol is commonly used for securely accessing and transferring files over a network?
a) HTTP
b) FTP
c) SMTP
d) POP3

Section 2: True or False

5. True or False: A firewall is a hardware or software-based security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. = **Ture**

6. True or False: DHCP (Dynamic Host Configuration Protocol) assigns static IP addresses to network devices automatically. = **False**

7. True or False: VLANs (Virtual Local Area Networks) enable network segmentation by dividing a single physical network into multiple logical networks = **True**

Section 3: Short Answer

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

Hub	Switch
As the hub sends the broadcast to all the device which is been connected to it as they need or not	As the switch forward the respective broadcast to a spective intended device and that specific port
It don't understand the MAC address	It understand MAC address
It create more collision in respective network	It create less collision in respective network
It works on 1st layer of OSI model	It works on 2nd layer of OSI model
It is less secure	It is less secure
It's speed is fast because it had a dedicated bandwidth	It's speed is slow due share bandwidth
It's implementation cost in low	It's implementation cost is high

9. Describe the process of troubleshooting network connectivity issues.

1. Identify and Define the Problem

- Gather information from the user.
- Check what exactly is not working (internet, LAN, specific application, etc.).
- Note any error messages or symptoms.

2. Check Physical Connections

- Ensure cables are properly plugged in.
- Verify that the router, switch, and modem are powered on.
- Check indicator lights (link/activity LEDs) on network devices.
- Test with a different cable or port if needed.

3. Verify IP Address Configuration

- Check if the device has a correct IP address using commands like:
  - Windows: ipconfig
  - Linux/macOS: ifconfig or ip a
- Ensure the device has a valid IP, subnet mask, gateway, and DNS server.

4. Test Connectivity With Ping

- Ping the local host (127.0.0.1) → verifies network adapter.
- Ping the default gateway → checks LAN connection.
- Ping an external site (8.8.8.8) → verifies internet access.
- Ping a domain (google.com) → checks DNS resolution.

5. Use Traceroute/Tracert for Path Testing

- Identifies where packets are failing along the network path.
- Helps locate issues in routers or ISP networks.

6. Check Network Devices

- Restart router/modem/switch.
- Verify DHCP is assigning addresses.
- Ensure firewall settings are not blocking traffic.
- Check for overheating or hardware failure.

7. Review Software and Security Settings

- Disable and re-enable the network adapter.
- Check if antivirus or firewall is blocking connectivity.
- Clear DNS cache (ipconfig /flushdns).
- Verify no VPN is interfering with the network.

8. Replace or Test Hardware

- Try using a different network adapter, cable, switch port, or router.
- Check if other devices on the network face the same issue.

9. Document the Problem and Solution

- Record the cause of the issue.
- Note the steps taken to fix it.
- Helps future troubleshooting and improves network management.

Section 4: Practical Application

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

1. Access the Router’s Web Interface

- Connect to the router via Wi-Fi or Ethernet.
- Open a browser and enter the router’s default IP address, such as:
  - **192.168.0.1**
  - **192.168.1.1**
- Login using the admin username and password.

2. Change the Default Admin Username and Password

- Go to **Administration / System** settings.
- Change the default admin password to a strong password to prevent unauthorized login.

3. Configure Wireless Network Name (SSID)

- Go to **Wireless Settings**.
- Set a unique SSID (network name).
- Avoid using personal details like names or phone numbers.

4. Enable Strong Wireless Encryption

- Under **Wireless Security**, choose:

    - **WPA2-PSK** or **WPA3-PSK** (recommended).
  - Avoid **WEP**, as it is outdated and insecure.
  - Set a strong Wi-Fi password (minimum 12–16 characters with symbols).

5. Disable WPS (Wi-Fi Protected Setup)

- WPS can be exploited by attackers.
- Turn off WPS in security settings to improve protection.

6. Enable MAC Address Filtering (Optional)

- Add the MAC addresses of trusted devices.
- Only these devices will be allowed to connect.

7. Hide SSID (Optional)

- Disable **SSID Broadcast** if you want the network to be hidden.
- Only devices that know the SSID can join the network.

8. Set Up a Guest Network

- Enable a guest Wi-Fi with a separate SSID.
- Keeps visitors away from the main network.
- Apply WPA2/WPA3 security for the guest network too.

9. Update Router Firmware

- Go to **Firmware Update** section.
- Install the latest firmware to fix vulnerabilities and improve security.

10. Save and Reboot

- Save all changes.
- Restart the router for new settings to apply.

Section 5: Essay

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

1. Faster Troubleshooting

When network issues occur, documentation helps administrators quickly identify devices, configurations, and connections, reducing downtime.

2. Easier Maintenance and Upgrades

With proper records of hardware, software versions, and network layout, it becomes easier to update or replace components without confusion.

3. Improved Security

Documentation helps keep track of authorized devices, firewall rules, user accounts, and access controls. This prevents unauthorized changes and security breaches.

4. Better Network Planning

Accurate documents allow administrators to plan expansions, redesign networks, and estimate required resources effectively.

5. Smooth Team Collaboration

Multiple technicians or new employees can understand the network setup easily when proper documentation is available.

6. Compliance and Audits

Organizations often need documentation to meet industry standards, audits, and legal requirements.

Examples of Information That Should Be Documented

Good network documentation includes:

1. Network Topology Diagrams

- Physical topology (cables, switches, routers)
- Logical topology (VLANs, IP schema, subnets)

2. IP Addressing and Subnet Information

- IP address allocation
- DHCP scopes
- Gateway and DNS settings

3. Device Inventory

- Routers, switches, servers, access points
- Model numbers, serial numbers, firmware versions
- Location of each device

4. Configuration Files

- Router and switch configurations
- Firewall rules
- ACLs (Access Control Lists)

5. User Accounts and Permissions

- Administrator accounts
- Access control policies
- Authentication records

6. Security Policies

- Password policies
- Backup procedures
- Incident response plans

7. Backup and Recovery Information

- Backup schedules
- Recovery steps
- Storage locations for backups

8. Change Logs

- Records of updates, patches, and configuration changes
- Who made the change and when