**Assignment module 3 : Understanding and Maintenance**

**Section 1: Multiple Choice**

**1. What is the primary function of a router in a computer network?**

-> Forwarding data packets between networks

**2. What is the purpose of DNS (Domain Name System) in a computer network?**

-> Converting domain names to IP addresses

**3. What type of network topology uses a centralized hub or switch to connect all devices?**

-> Star

**4. Which network protocol is commonly used for securely accessing and transferring files over a network?**

-> FTP

**Section 2: True or False**

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

-> True

**6. DHCP (Dynamic Host Configuration Protocol) assigns static IP addresses to network devices automatically.**

-> False

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

-> True

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

-> A **hub** broadcasts data to **all devices** on a network, regardless of the destination.

-> A **switch** sends data **only to the intended recipient device**, making it more efficient and secure.

**9. Describe the process of troubleshooting network connectivity issues.**

-> **Check physical connections** (cables, power).

-> **Verify device settings** (IP address, Wi-Fi).

-> **Ping other devices** to test connectivity.

-> **Restart network devices** (router, modem).

-> **Check for IP conflicts** or DHCP issues.

-> **Update drivers** and firmware.

-> **Use diagnostic tools** (e.g., ipconfig, tracert, or network troubleshooter).

**Section 4: Practical Application**

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

**Steps to Enhance Wireless Router Security**

1. Access the Router’s Admin Panel

* Connect to your router via Ethernet or Wi-Fi.
* Open a browser and enter the router’s IP (e.g., 192.168.1.1 or 192.168.0.1).
* Log in with the admin credentials (default is often admin/admin—change this later).

2. Change Default Admin Credentials

* Go to **Administration** or **System Settings**.
* Set a **strong username and password** (avoid defaults like admin).

3. Update Router Firmware

* Check for updates in **Administration > Firmware Update**.
* Install the latest security patches.

4. Enable WPA3 Encryption (or WPA2 if WPA3 is unavailable)

* Go to **Wireless > Security**.
* Select **WPA3-Personal** (or **WPA2-PSK AES**).
* Set a **strong passphrase** (12+ characters, mix letters, numbers, symbols).

5. Change the Default SSID (Network Name)

* Navigate to **Wireless > Basic Settings**.
* Rename the SSID (avoid personal info like "John's Wi-Fi").

6. Disable WPS (Wi-Fi Protected Setup)

* WPS is vulnerable to brute-force attacks.
* Disable it in **Wireless > WPS Settings**.

7. Enable Network Firewall

* Go to **Security > Firewall**.
* Enable **SPI (Stateful Packet Inspection)**.

8. Disable Remote Management

* In **Administration > Remote Management**, ensure it’s **disabled**.

9. Enable MAC Address Filtering (Optional)

* Under **Wireless > MAC Filtering**, allow only trusted devices.

10. Reduce Wi-Fi Signal Range (If Needed)

* Adjust **Transmit Power** to "Medium" or "Low" to limit coverage.

11. Disable UPnP (Universal Plug and Play)

* In **Advanced Settings > UPnP**, turn it off to prevent vulnerabilities.

12. Enable Guest Network (Optional)

* Isolate guest traffic in **Wireless > Guest Network**.
* Set a separate password and disable local network access.

Wireless Router

|

(Security Settings)

v

1. Admin Password → Change Default Credentials

2. WPA3 Encryption → Enable Strong Encryption

3. Disable WPS → Prevent Brute-Force Attacks

4. Firewall (SPI) → Block Unauthorized Traffic

5. Firmware Update → Patch Vulnerabilities

6. MAC Filtering → (Optional) Whitelist Devices

|

(Secure Wi-Fi)

v

Protected Devices

**Section 5: Essay**

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

**1. Efficient Troubleshooting and Maintenance**

When network issues arise, well-maintained documentation allows IT teams to quickly identify configurations, IP addresses, and device locations. This reduces downtime and speeds up resolution. For example, if a switch fails, documented port mappings help technicians replace it without guesswork.

**2. Enhanced Security and Compliance**

Documentation helps track security policies, firewall rules, and access controls, ensuring compliance with regulations like **GDPR, HIPAA, or PCI-DSS**. It also aids in auditing by providing a clear record of network changes, reducing vulnerabilities from misconfigurations.

**3. Smooth Knowledge Transfer**

When IT personnel leave or new staff join, documentation ensures continuity. A new administrator can review network diagrams, passwords (securely stored), and device inventories instead of relying on fragmented knowledge.

**4. Scalability and Future Planning**

As networks grow, documentation helps plan expansions logically. Records of IP allocations, subnet structures, and bandwidth usage prevent conflicts and inefficiencies.

**5. Disaster Recovery**

In case of a cyberattack or hardware failure, documented backup procedures, network topology, and device configurations enable faster restoration.

**Key Information to Document**

**1. Network Topology Diagrams**

* Physical and logical layouts of devices (routers, switches, servers).
* Connections between devices (cabling, VLANs, WAN links).

**2. IP Address Management (IPAM)**

* Subnet allocations (e.g., 192.168.1.0/24 for workstations, 10.0.0.0/24 for servers).
* DHCP scopes and static IP assignments.

**3. Device Configurations**

* Router, switch, and firewall settings (exported as backup files).
* Firmware versions and update history.

**4. Security Policies**

* Firewall rules (allowed/denied traffic).
* VPN configurations and access controls.
* Password policies and encryption standards (e.g., WPA3 for Wi-Fi).

**5. User and Access Management**

* Active Directory (AD) or LDAP user roles.
* Privileged account credentials (stored securely in a password manager).

**6. Inventory of Hardware and Software**

* Model numbers, serial numbers, warranty details.
* Installed software licenses and versions.

**7. Backup and Recovery Procedures**

* Schedule of backups (daily, weekly).
* Location of backup files (onsite/cloud).
* Steps to restore services after failure.

**8. Change Logs**

* Records of updates, patches, and configuration changes.
* Who made changes and when (for accountability).