**Assignment module 3 : Understanding and Maintenance of**

**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

ANS. **c) Forwarding data packets between networks**

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

d) packets between network segments

ANS. **c) Converting domain names to IP addresses**

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

a) Star

b) Bus

c) Ring

d) Mesh

ANS. **a) Star**

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

a) HTTP

b) FTP

c) SMTP

d) POP3

ANS. **b) 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

ANS. **True**

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

ANS. **False**

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

ANS. **True**

**Section 3: Short Answer**

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

ANS.

|  |  |
| --- | --- |
| Hub | Switch |
| A hub is a basic networking device that broadcasts data to all devices connected to it. | A switch is a more advanced device that forwards data only to the specific device (port) it is intended for. |
| When one device sends data to the hub, the hub copies that data and sends it to every port (regardless of the destination). | The switch keeps a MAC address table and uses it to send data only to the correct recipient. |
| Operates at Layer 1 (Physical Layer) of the OSI model. | Operates at Layer 2 (Data Link Layer), but some switches also work at Layer 3 (Network Layer). |
| Less efficient, because all devices share the same bandwidth, and data collisions are common. | Much more efficient, with less traffic and fewer collisions. |
| Low security, since all data is visible to every device. | More secure, since data is not broadcast to all devices. |

9. Describe the process of troubleshooting network connectivity issues.

ANS. Troubleshooting network connectivity issues involves a systematic approach to identifying and resolving the cause of the problem. The first step is to understand the symptoms, such as whether the issue affects one device or the entire network, and whether the problem is complete disconnection or intermittent connectivity. Next, physical connections should be checked to ensure cables are securely connected and networking hardware like routers, switches, or modems are powered on and functioning.

If using Wi-Fi, ensure the device is within range and connected to the correct network. After that, verifying the device's network configuration is essential—this includes checking for a valid IP address, ensuring that DHCP and DNS settings are correct, and confirming there are no IP conflicts. Various tools like ping, tracert, and ipconfig (or ifconfig on Linux/macOS) can help test connectivity and isolate where the communication is failing. Restarting the device, router, or modem can resolve many temporary issues. It is also important to check router settings, firewall configurations, and any software that might be blocking the connection. Testing with other devices helps determine whether the problem is isolated or widespread.

* Identify the Problem
* Check Physical Connections
* Verify Device Configuration
* Test Network Connectivity
* Restart Devices
* Check Router and Modem
* . Review Network Settings and Firewall
* Test with Different Devices

**Section 4: Practical Application**

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

ANS.To enhance your wireless network security, it's essential to configure your wireless router with strong security settings. Below is a **practical step-by-step demonstration** to help you do that.

**Step-by-Step: Configure Wireless Router Security Settings**

**Step 1: Log in to the Router’s Admin Interface**

1. Connect your computer or phone to the router (via Wi-Fi or Ethernet).
2. Open a web browser, and enter your router’s IP address. Common addresses:
   * 192.168.0.1
   * 192.168.1.1
   * 192.168.1.254
3. **Log in** using the admin username and password.
   * Default login credentials are usually found on a sticker on the router or in its manual.
   * Change these later if still set to default**.**

**Step 2: Change the Default Admin Username and Password**

* Go to the Administration or Management section.
* Change both the **admin username** and **password** to something strong and unique.
  + Example: AdminUsername: myRouter123  
    Password: H@nD#45Tg!q
* Save and reboot if required.

**Step 3: Configure Wireless Network Name (SSID)**

* Navigate to Wireless Settings.
* Change the SSID (Wi-Fi name) to something unique.
  + Avoid using personal info (e.g., your name or address).
  + Example: SecureHomeNet\_5G

**Step 4: Set Strong Wi-Fi Encryption**

* Under Wireless Security or Security Mode, choose:
  + Security Mode: WPA3-Personal (if available)  
    If not, use WPA2-Personal (AES encryption).
* **Set a strong Wi-Fi password**:
  + At least 12 characters with a mix of letters, numbers, and symbols.
  + Example: Mysaf3WiFi@2025!

**Step 5: Disable WPS (Wi-Fi Protected Setup)**

* WPS can be a security risk.
* Find the **WPS** setting and **disable it.**

**Step 6: Enable Network Firewall & Disable Remote Management**

* Go to the **Firewall or Security** section.
* Ensure the **router’s firewall is enabled.**
* Disable any **Remote Management or Remote Access** unless needed.
  + This prevents access to your router settings from outside your network.

**Step 7: Hide SSID Broadcast (Optional)**

* Hiding your SSID won’t stop determined attackers but adds a small layer of obscurity.
* In **Wireless Settings**, find **"Enable SSID Broadcast"** and **disable it** if you want to hide the network.
  + Devices must manually be configured to connect.

**Step 8: Set Up a Guest Network (Optional)**

* If guests frequently use your Wi-Fi, create a **Guest Network:**
  + Enable **Guest Network**.
  + Use a different SSID and password.
  + Restrict access to your main network or local devices.
  + Apply the same strong encryption (WPA2/WPA3).

**Step 9: Save Settings and Reboot**

* Save all changes.
* Restart the router if prompted or if changes don’t take effect immediately.

**Section 5: Essay**

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

Ans. **Importance of Network Documentation**

Network documentation is a critical part of managing and maintaining a reliable, secure, and efficient network infrastructure. It involves recording detailed information about the network’s components, configuration, policies, and procedures. Proper documentation helps IT staff **troubleshoot issues quickly, plan for upgrades, improve security**, and **ensure continuity** when team members change or systems are updated.

Without documentation, network administrators may waste valuable time trying to understand how the network is set up, increasing the risk of errors and downtime. It also serves as a **reference for audits**, **compliance**, and disaster recovery efforts.

1. **Network Topology Diagrams**

* Visual maps of how devices are connected.
* Includes routers, switches, firewalls, servers, and endpoints

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

* List of all assigned IP addresses.
* DHCP scope details and static IP assignments.

3. **Device Inventory**

* Details of all networking equipment:
  + Device name, model, serial number.
  + Firmware/software version.
  + Purchase and warranty information.

4. **Configuration Files**

* Backup configurations of routers, switches, firewalls.
* Settings for access control, routing protocols, VLANs, et

5. **Login Credentials and Access Details**

* Admin usernames and passwords (stored securely).
* SSH keys or management interfaces.
* Role-based access control documentation

6. **Network Services**

* DNS, DHCP, FTP, email servers, etc.
* Configuration and role of each service.

7. **Security Policies**

* Firewall rules.
* VPN setup.
* Port forwarding and access control lists (ACLs).
* Antivirus or IDS/IPS systems.

8. **ISP and Vendor Contact Information**

* Details for internet providers, hardware vendors, and support contacts.

9. **Backup and Recovery Procedures**

* Location of backup files.
* Step-by-step disaster recovery plans.
* Frequency of backups.