Module:- 3 **Understanding And Maintenance Of Networks**

Section 1: Multiple Choice

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

Answer:- Forwarding data packets between networks

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

Answer:- Converting domain names to IP addresses

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

Answer:- Star

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

Answer:- FTP

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.

Answer:- True

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

Answer:- False

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

Answer:- True

Section 3: Short Answer

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

Answer:-

| **Feature** | **Hub** | **Switch** |
| --- | --- | --- |
| **Function** | Broadcasts data to all connected devices | Sends data only to the specific device (MAC address) |
| **Intelligence** | Not intelligent – doesn't filter data | Intelligent – filters and forwards data intelligently |
| **Data Transmission** | Shared bandwidth; one device at a time | Dedicated bandwidth per port; multiple transfers at once |
| **Security** | Less secure – data visible to all connected devices | More secure – data sent only to intended recipient |
| **Speed & Performance** | Slower due to network collisions | Faster with minimal collisions |
| **Use Case** | Older, simpler networks (rarely used now) | Common in modern networks |

9. Describe the process of troubleshooting network connectivity issues.

Answer:-

Troubleshoot network connectivity issues:

1. **Check physical connections** (cables, power, router/modem).
2. **Verify IP settings** using ipconfig or ifconfig.
3. **Ping** the gateway or external sites to test connection.
4. **Restart devices** like the computer, router, and modem.
5. **Check DNS settings** and try alternate DNS like 8.8.8.8.
6. **Temporarily disable firewall or antivirus** to rule out blocking.
7. **Replace faulty hardware** like cables or network adapters if needed.

Section 4: Practical Application

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

Answer:-

1. **Access the Router Admin Panel:**
   * Connect to the router.
   * Open a browser and enter the IP address (e.g., 192.168.0.1).
   * Login using admin credentials.
2. **Change Default Login Credentials:**
   * Navigate to **Admin Settings**.
   * Change the default username and password to strong, unique ones.
3. **Change the SSID (Wi-Fi Name):**
   * Go to **Wireless Settings**.
   * Change the SSID to a unique name (avoid personal information).
4. **Enable WPA2 or WPA3 Encryption:**
   * Under **Wireless Security**, select **WPA2-PSK** or **WPA3**.
   * Set a strong password (use letters, numbers, and symbols).
5. **Disable WPS (Wi-Fi Protected Setup):**
   * WPS is vulnerable to attacks.
   * Turn it off in WPS settings.
6. **Enable Firewall:**
   * Go to **Security Settings**.
   * Make sure the firewall is enabled to block unauthorized access.
7. **Disable Remote Management:**
   * Prevents external access to router settings.
   * Disable it under **Remote Management/Access** settings.
8. **Update Router Firmware:**
   * Check for firmware updates regularly.
   * Install updates to patch security vulnerabilities.
9. **Enable Guest Network (Optional):**
   * Create a separate Wi-Fi for guests.
   * Limit access to main devices and files.
10. **Use MAC Address Filtering (Optional):**

* Allow only specific device MAC addresses to connect.

Section 5: Essay

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

Answer:-

**Importance of Network Documentation:**

Network documentation is the process of recording detailed information about a computer network’s hardware, software, configurations, and layout. It is **crucial for managing, troubleshooting, upgrading, and securing** the network effectively.

**🔹 Why it is Important:**

1. **Troubleshooting and Maintenance:**
   * Helps network administrators quickly identify and fix problems.
2. **Network Upgrades:**
   * Assists in planning future expansions or changes without disrupting current services.
3. **Security Management:**
   * Identifies vulnerabilities, unused ports, or unauthorized devices.
4. **Consistency and Compliance:**
   * Ensures configuration standards and compliance with IT policies or regulations.
5. **Disaster Recovery:**
   * Makes restoring network infrastructure faster in case of failure.
6. **Training and Handover:**
   * Helps new IT staff understand the network structure quickly.

Examples of Information to be Documented:

| **Category** | **Information to Document** |
| --- | --- |
| **Network Topology** | Diagrams of how devices (routers, switches, servers) are connected |
| **IP Addressing** | IP address ranges, static IP assignments, DHCP settings |
| **Device Inventory** | List of all routers, switches, firewalls, with model, serial number, and location |
| **Configuration Files** | Router/switch configurations, firewall rules |
| **Access Control** | Admin usernames/passwords (stored securely), access rights |
| **Cabling Information** | Cable types, lengths, port numbers |
| **Network Services** | DNS, DHCP, VPN, proxy configurations |
| **Change Logs** | Record of updates, changes, or patches applied to the network |
| **Vendor/Support Info** | Contact details, warranty info, service agreements |