1. What is the primary function of a router in a computer network?
   1. Assigning IP addresses to devices
   2. Providing wireless connectivity to devices
   3. Forwarding data packets between networks



* 1. Managing user authentication and access control

1. What is the purpose of DNS (Domain Name System) in a computer network?
   1. Encrypting data transmissions for security
   2. Assigning IP addresses to devices dynamically
   3. Converting domain names to IP addresses



* 1. Routing data

packets between network segments

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



* 1. Bus
  2. Ring
  3. Mesh

1. Which network protocol is commonly used for securely accessing and transferring files over a network? a) HTTP
   1. FTP



* 1. SMTP
  2. POP3

**Section 2: True or False**

1. 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.   
   **True because**

**a firewall is a security system that can be hardware-based, software-based, or both. It monitors and controls network traffic based on security rules to protect against unauthorized access.**

1. True or False: DHCP (Dynamic Host Configuration Protocol) assigns static IP addresses to network devices automatically.   
     
   **False because DHCP (Dynamic Host Configuration Protocol) automatically assigns dynamic IP addresses, not static ones. Static IP addresses are manually assigned and remain fixed.**

1. True or False: VLANs (Virtual Local Area Networks) enable network segmentation by dividing a single physical network into multiple logical networks.   
     
   **VLANs (Virtual Local Area Networks) enable network segmentation by dividing a single physical network into multiple logical networks, improving performance and security.**

**Section 3: Short Answer**

1. Explain the difference between a hub and a switch in a computer network.   
     
   **Hub:  
     
   Operates at the physical layer (Layer 1) of the OSI model.**

**Broadcasts data to all connected devices, regardless of the intended recipient.**

**Less efficient as it creates unnecessary network traffic and collisions.**

**Cannot differentiate between devices.**

**Switch:**

**Operates at the data link layer (Layer 2) or sometimes Layer 3 for advanced switches.**

**Directs data packets only to the intended recipient using MAC addresses.**

**More efficient as it reduces network traffic and avoids collisions.**

**Supports features like VLANs and full-duplex communication.**

1. Describe the process of troubleshooting network connectivity issues.   
     
   **1. Identify the Problem:**

**Verify the symptoms (e.g., no internet, slow speed, or intermittent connection).**

**Ask users about error messages or when the issue started.**

**2. Check Physical Connections:**

**Ensure cables, ports, and devices are connected securely.**

**Verify that devices like routers, switches, and access points are powered on.**

**3. Verify Network Settings:**

**Check IP configuration using commands like ipconfig (Windows) or ifconfig (Linux).**

**Ensure correct IP, gateway, and DNS settings.**

**4. Test Connectivity:**

**Use ping to test communication with the gateway or another device.**

**Use tracert or traceroute to check the path to a destination.**

**5. Check Network Devices:**

**Restart the router, modem, or switch.**

**Check if the device is functioning properly (e.g., status LEDs).**

**6. Inspect Firewall or Security Software:**

**Ensure firewalls or antivirus software aren’t blocking network traffic.**

**7. Test with Another Device or Network:**

**Use another device to confirm if the issue is device-specific or network-wide.**

**Test the problematic device on a different network.**

**8. Contact ISP or Network Admin:**

**If the issue persists, contact the Internet Service Provider (ISP) or network administrator for assistance.**

**Section 4: Practical Application**

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

**1. Access the Router's Admin Interface**

**Connect to the router using a wired (Ethernet) connection or via Wi-Fi.**

**Open a web browser and enter the router’s IP address in the address bar (common IP addresses: 192.168.1.1 or 192.168.0.1).**

**2. Change the Default Login Credentials**

**For security, change the default admin username and password to something more secure.**

**Look for an option under "Administration" or "System Settings" to change the login credentials.**

**3. Configure Wireless Settings**

**Navigate to the Wireless Settings or Wireless Security section in the router's admin interface.**

**4. Enable WPA3 Encryption (or WPA2)**

**In the Wireless Security section, choose WPA3 (Wi-Fi Protected Access 3), which is the most secure encryption standard.**

**If WPA3 is not available, select WPA2.**

**5. Set a Strong Wi-Fi Password**

**Create a strong Wi-Fi password using a mix of uppercase and lowercase letters, numbers, and special characters.**

**6. Enable MAC Address Filtering (Optional)**

**MAC address filtering allows only devices with specific MAC addresses to connect to the network.**

**7. Disable Remote Management (if not needed)**

**Remote management allows you to configure the router from outside the local network. If you don’t need this feature, disable it to prevent external attacks on the router.**

**Look for the Remote Management option in the router settings and disable it.**

**8. Enable the Router's Firewall**

**Activate the built-in firewall on the router if it's not enabled by default. This helps protect the network from incoming threats.**

**Look for a Firewall or Security section in the router settings and enable the firewall.**

**9. Update Router Firmware**

**Regularly check for firmware updates in the router’s admin interface. Router manufacturers frequently release updates to address security vulnerabilities.**

**Navigate to the Firmware Update section and apply the latest version available.**

**10. Disable WPS (Wi-Fi Protected Setup)**

**WPS is a feature that allows easy Wi-Fi setup by pressing a button or entering a PIN. However, it can be vulnerable to attacks.**

**Disable WPS in the router settings to improve security.**

**11. Reboot the Router**

**After making the changes, reboot the router to ensure the new settings take effect.**

**Section 5: Essay**

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

**Network documentation is critical for the management, troubleshooting, and security of a network. It provides a comprehensive record of the network's architecture, configurations, and devices, enabling efficient operation and quick resolution of issues. Well-documented networks also improve scalability, help in compliance with regulations, and provide a valuable reference for network administrators and IT teams.**

**Key Benefits of Network Documentation:**

**1. Troubleshooting and Maintenance:**

**Helps quickly identify and resolve network issues, as the documentation provides details about network topology, device configurations, and IP addressing.**

**2. Network Planning and Expansion:**

**Assists in planning network upgrades or expansions by having a clear picture of current assets and limitations.**

**3. Security:**

**Documents help ensure that network security measures (such as firewalls, VLANs, and encryption) are properly configured and maintained.**

**4. Compliance and Audits:**

**Network documentation is often required for audits, regulatory compliance, and industry standards.**

**It ensures transparency in the management of data and resources, which is important for meeting legal or corporate policies.**

**5. Employee Onboarding and Knowledge Transfer:**

**Network documentation provides a knowledge base for new network administrators or IT staff, easing onboarding and ensuring continuity of operations.**

**Examples of Information That Should Be Documented:**

**1. Network Topology Diagrams:**

**A visual representation of how all network components (routers, switches, servers, firewalls, etc.) are connected.**

**Should include device names, IP addresses, and how data flows within the network.**

**2. IP Address Scheme:**

**A detailed record of IP address assignments for all network devices.**

**It should document subnetting, ranges of available addresses, static IP addresses, DHCP pools, and reserved addresses.**

**3. Device Inventory:**

**A list of all network devices, including routers, switches, firewalls, servers, and endpoints.**

**For each device, include model numbers, serial numbers, firmware versions, locations, and maintenance schedules.**

**4. Network Configuration Settings:**

**Detailed configurations for network devices (such as routers, switches, and firewalls), including access control lists (ACLs), VLAN configurations, and routing tables.**

**Ensure backup configurations are included for easy recovery after failures.**

**5. Wi-Fi Configuration:**

**Document wireless access points (APs), their locations, SSID settings, encryption methods (WPA2, WPA3), and passwords.**

**Include any roaming configurations or guest network setups.**