

ASSIGNMENT 4

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

c) Forwarding data packets between networks

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

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

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

b) FTP

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 AND A SWITCH ARE BOTH NETWORKING DEVICES USED TO CONNECT MULTIPLE DEVICES WITHIN A LOCAL AREA NETWORK BUT THEY FUNCTION DIFFERENTLY

HUB: OPERATES AT THE PHYSICAL LAYER OF THE OSI MODEL . IT BROADCAST INCOMING DATA PACKETS TO ALL THE PORTS , REGARDLESS OF THE INTENDED RECIPIENT. THIS CAN LEAD TO NETWORK CONGESTION AND COLLISIONS,AS ALL DEVICES RECEIVE THE SAME DATA SIMULTANEOUSLY.

SWITCH : FUNCTIONS AT THE DATA LINK LAYER AND USES MAC ADDRESSES TO FORWARD DATA PACKETS ONLY TO THE PORT CONNECTED TO THE DESTINATION DEVICE.THIS TARGETED DATA TRANSMISSION REDUCES COLLISIONS AND IMPROVES NETWORK EFFICIENCY.

9. Describe the process of troubleshooting network connectivity issues.

To fix network connection problems, start by checking that all cables are plugged in tightly and aren't damaged. Make sure your network devices, like routers and computers, are turned on and working properly. Use the ping command to test if your devices can communicate with each other. Confirm that each device has the correct IP address and subnet mask settings. Check that firewalls or security software aren't blocking your network traffic. Look at system and device logs for any error messages or unusual activity. Finally, restart your devices to clear up any temporary issues.

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

To secure your wireless network, access your router's settings via a web browser by entering its IP address. Log in with your administrator credentials; if unchanged, the default may be "admin" for both username and password. Once logged in, change the default password to a strong, unique one to prevent unauthorized access. Set a distinctive network name (SSID) and choose a strong Wi-Fi password combining letters, numbers, and special characters. Select WPA2 or WPA3 encryption for robust security. Consider disabling Wi-Fi Protected Setup (WPS) due to known vulnerabilities.

Regularly update your router's firmware to patch security vulnerabilities and enhance performance.

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

Network documentation is crucial for maintaining a well-organized, secure, and efficient IT infrastructure. It provides a clear overview of the network's design, configuration, and operation, which helps with troubleshooting, scaling, and ensuring compliance with standards and security policies. Proper documentation allows network administrators to quickly identify and address issues, plan for future growth, and train new staff.

Examples of information that should be documented include network topology diagrams, IP address allocations, hardware inventory, device configurations, VLANs, subnets, routing protocols, security policies, firewall rules, and backup procedures. Additionally, details about software versions, passwords (stored securely), and network performance metrics should be recorded to ensure smooth operations.