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. 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

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

-->False

7. True or False: 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.

-->Hub:

Broadcasts data to all devices in the network.

Works at Layer 1 (Physical Layer) of the OSI model.

Can cause network congestion due to unnecessary traffic.

Switch:

Forwards data only to the intended recipient based on MAC addresses.

Works at Layer 2 (Data Link Layer) of the OSI model.

More efficient and reduces network collisions.

9. Describe the process of troubleshooting network connectivity issues.

-->Check Physical Connections – Ensure cables are plugged in, and the router/modem is powered on.

Verify Network Settings – Run ipconfig /all (Windows) or ifconfig (Linux/macOS) to check the IP configuration.

Ping the Gateway – Use ping <router_IP> to test connectivity with the router.

Test Internet Access – Ping an external address (ping 8.8.8.8) to check if the internet is reachable.

Check DNS Resolution – If websites aren't loading, try nslookup google.com or ping google.com.

Restart Networking Equipment – Reboot the router, modem, and PC to refresh connections.

Check for Firewall or Security Software Issues – Ensure no security software is blocking network traffic.

Try a Different Network – Connect to another network (e.g., mobile hotspot) to rule out local network issues.

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

enhance network security.

-->Access the Router's Web Interface – Enter the router's IP address (e.g., 192.168.1.1) in a web browser.

Change the Default Admin Password – Use a strong password to prevent unauthorized access.

Enable WPA3 or WPA2 Security – Set the Wi-Fi security mode to WPA3 or WPA2-PSK (avoid WEP, which is outdated).

Use a Strong Wi-Fi Password – Create a secure passphrase to prevent unauthorized access.

Disable WPS (Wi-Fi Protected Setup) – This feature can be a security risk.

Enable MAC Address Filtering (Optional) – Allows only specific devices to connect.

Disable SSID Broadcasting (Optional) – Hides the Wi-Fi name from public view.

Update Firmware – Ensure the router's firmware is up to date for security patches.

Enable a Firewall – Many routers have built-in firewalls that add an extra layer of security.

11. Discuss the importance of network documentation and provide

examples of information that should be documented.

-->Why It's Important:

Helps in troubleshooting and network upgrades.

Improves security by tracking access points.

Provides a reference for future network expansion.

Examples of Network Documentation:

Network Topology Diagrams – Visual representation of devices and connections.

IP Address Allocation – Lists static and dynamic IP addresses.

Device Inventory – Includes routers, switches, and other hardware details.

Configuration Settings – Stores router, switch, and firewall configurations.

Security Policies – Defines access control, encryption settings, and security rules.

Troubleshooting Logs – Records previous network issues and solutions.