**Assignment module 3**

**Understanding and Maintenance of**

**Section 1: Multiple Choice**

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

Ans-(c) Forwarding data packets between networks

1. **What is the purpose of DNS (Domain Name**

**System) in a computer network?**

Ans-(c) Converting domain names to IP addresses

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

Ans-(a) Star

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

Ans-(b) FTP

**Section 2: True or False**

1. 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

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

Ans-False

1. VLANs (Virtual Local Area Networks) enable network segmentation by dividing a single physical network into multiple logical networks.

Ans-True

**Section 3: Short Answer**

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

Ans- Function: A hub is a basic networking device that connects multiple computers in a network and sends data to all devices linked to it. Data Transmission, Efficiency, ntelligence,

Layer: It operates at Layer 1 (Physical Layer) of the OSI model.

1. Describe the process of troubleshooting network connectivity issues.

Ans- process of troubleshooting network connectivity 1st is Identify the Problem, Check Physical Connections, Test Local ,External Connectivity , Check Network Devices, Examine Firewall and Security Settings, Review Logs and System Messages ext, Escalate if Necessary

**Section 4: Practical Application**

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

Ans- To enhance the security of your wireless network, follow these steps to configure your router's security settings:

1. **Access the Router’s Admin Interface**:  
   Connect to your router using a web browser by entering its IP address (commonly 192.168.1.1 or 192.168.0.1). Log in with the default admin credentials.
2. **Change the Admin Username and Password**:  
   Modify the default admin username and password to something unique and strong to prevent unauthorized access to the router's settings.
3. **Set a Strong Wi-Fi Password**:  
   Create a complex Wi-Fi password using a mix of letters, numbers, and special characters. This will help protect your network from unauthorized users.
4. **Change the SSID (Network Name)**:  
   Change the default SSID to a unique name that does not reveal personal information or the router brand, making it harder for attackers to target your network.
5. **Disable WPS (Wi-Fi Protected Setup)**:  
   Turn off WPS, as it can be a security vulnerability that allows easy access to the network through a PIN.
6. **Enable Network Firewall**:  
   Activate the built-in firewall on the router to provide an additional layer of protection against external threats.
7. **Enable MAC Address Filtering**:  
   Configure MAC address filtering to allow only specific devices to connect to your network, adding another layer of security.
8. **Disable Remote Management**:  
   Turn off remote management features to prevent access to the router's settings from outside your local network.
9. **Update Firmware Regularly**:  
   Check for and install firmware updates from the router manufacturer to ensure you have the latest security patches and features.
10. **Create a Guest Network**:  
    Set up a separate guest network for visitors, isolating it from your main network to protect your personal devices and data.

By following these steps, you can significantly enhance the security of your wireless network and protect it from potential threats.

**Section 5: Essay**

1. Discuss the importance of network documentation and provide examples of information that should be documented.
2. Ans **Importance of Network Documentation**
3. Network documentation is essential for the effective management and operation of a network. It serves as a comprehensive reference that aids in various aspects of network administration. Here are some key reasons why network documentation is important:
4. **Efficient Troubleshooting**:  
   Well-documented networks allow administrators to quickly identify and resolve issues, minimizing downtime and improving overall network reliability.
5. **Simplifies Network Maintenance**:  
   Documentation provides a clear overview of the network's structure and components, making routine maintenance tasks easier and more efficient.
6. **Enhances Security**:  
   Keeping detailed records of network configurations and access controls helps identify vulnerabilities and ensures compliance with security policies.
7. **Facilitates Onboarding and Training**:  
   New team members can quickly familiarize themselves with the network setup, reducing the learning curve and improving productivity.
8. **Supports Disaster Recovery**:  
   In the event of a failure, documentation is crucial for restoring systems and configurations, ensuring a quicker recovery process.
9. **Aids in Upgrades and Expansion**:  
   Documentation helps plan and implement network upgrades or expansions by providing a clear understanding of existing resources and configurations.
10. **Examples of Information That Should Be Documented**
11. **Network Topology Diagrams**: Visual representations of the network layout, showing how devices are interconnected.
12. **IP Address Allocation**: A record of assigned IP addresses, including static and dynamic allocations, to avoid conflicts.
13. **Device Inventory**: A list of all network devices, including make, model, serial numbers, and firmware versions.
14. **Configuration Files**: Backup copies of configurations for routers, switches, and firewalls to facilitate recovery and changes.
15. **Network Services Information**: Details about services such as DHCP, DNS, and VPN configurations.
16. **User Access and Permissions**: Documentation of user accounts, roles, and access levels to ensure proper security management.
17. **Cabling and Port Maps**: Information on physical cabling routes and port assignments on switches and patch panels.
18. **Security Policies**: Documentation of firewall rules, encryption methods, and access control measures.
19. **ISP and Vendor Details**: Contact information and service agreements with internet service providers and hardware vendors.
20. **Change Log**: A record of changes made to the network, including updates, modifications, and maintenance activities.
21. By maintaining thorough network documentation, organizations can enhance their operational efficiency, security, and overall network management.