Assignment module 3: Understanding and Maintenance of Network Security

**Section 1: Multiple Choice**

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

a) Assigning IP addresses to devices

b) Providing wireless connectivity to devices

c) **Forwarding data packets between networks**

d) Managing user authentication and access control

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

a) Encrypting data transmissions for security

b) Assigning IP addresses to devices dynamically

c) **Converting domain names to IP addresses**

d) Routing data packets between network segments

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

a) **Star**

b) Bus

c) Ring

d) Mesh

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

a) HTTP

b) **FTP**

c) SMTP

d) POP3

**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. **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**

**Section 3: Short Answer Section**

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

**ANS**.

A **hub** is a basic networking device that connects multiple devices in a network by broadcasting data to all ports, regardless of the intended recipient. This can lead to network congestion and collisions.

A **switch**, on the other hand, is more advanced. It intelligently forwards data only to the specific device or port for which the data is intended, reducing collisions and improving overall network efficiency and performance.

9. Describe the process of troubleshooting network connectivity issues.

**ANS**.

1. **Identify the Problem**: Gather details about the issue (single or multiple devices).
2. **Check Physical Connections**: Ensure all cables are secure and undamaged.
3. **Verify Device Status**: Make sure the device is powered on and connected to the network.
4. **Ping Test**: Use the ping command to check connectivity to the router and other devices.
5. **Check IP Configuration**: Verify IP address, subnet mask, and gateway settings using ipconfig (Windows) or ifconfig (Linux/Mac).
6. **Restart Devices**: Reboot the affected device and network equipment (router/switch).
7. **Inspect Network Configuration**: Review router/switch settings, DHCP configurations, and any access control lists (ACLs).
8. **Check Firewall Settings**: Ensure firewalls aren’t blocking the connection.
9. **Use Diagnostic Tools**: Utilize network analysis tools to identify issues.
10. **Test with Alternate Devices**: Connect another device to isolate the problem.

By following these steps, you can effectively troubleshoot and resolve network connectivity issues.

**4: Practical Application Section**

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

**ANS. Done in class**

**5: Essay**

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

**ANS**.

Network documentation is crucial for several reasons:

**Importance of Network Documentation**

1. **Troubleshooting**: Clear documentation helps quickly identify and resolve network issues by providing a reference for configurations and network layouts.
2. **Network Management**: It aids in effective management of the network, allowing administrators to track changes, monitor performance, and plan for upgrades.
3. **Compliance and Security**: Proper documentation ensures compliance with regulations and enhances security by providing a clear understanding of network configurations and access controls.
4. **Training and Onboarding**: New team members can reference documentation to understand the network structure and operations, facilitating quicker onboarding.
5. **Disaster Recovery**: In case of outages or disasters, documentation provides critical information needed to restore services efficiently.

**Examples of Information to Document**

1. **Network Diagrams**: Visual representations of the network layout, including devices, connections, and topology.
2. **IP Addressing Scheme**: A list of assigned IP addresses, subnets, and any static or dynamic assignments.
3. **Device Inventory**: Information on all network devices (routers, switches, firewalls, etc.), including model numbers, locations, and configuration details.
4. **Configuration Files**: Backup copies of device configurations to facilitate recovery and management.
5. **Access Control Lists (ACLs)**: Documentation of user permissions, roles, and access policies to secure the network.
6. **Change Logs**: Records of all changes made to the network, including configurations, device additions, and software updates.
7. **Network Policies**: Guidelines and procedures for network usage, security protocols, and incident response.

By maintaining thorough network documentation, organizations can improve operational efficiency, security, and overall network reliability.